

https://dspace.org/

A critical analysis of the legal framework relating to cybercrime in Uganda

Adesuyi, Daramola

2021
https://hdl.handle.net/10539/33262

Downloaded from a DSpace repository. https://dspace.org/



UNIVERSITY OF THE WITSWATERSTRAND, JOHANNESBURG
SCHOOL OF LAW

A CRITICAL ANALYSIS OF THE LEGAL FRAMEWORK RELATING TO CYBERCRIME IN UGANDA

Submitted in fulfilment of the requirements of the degree of Master of Laws (LL.M) in the Faculty of Commerce, Law and Management at the University of the Witwatersrand, Johannesburg.

By

Daramola Adesuyi

Student No. 2107275

Supervisor: Bernice Welgemoed

Date: December 2020

DECLARATION

I declare that the dissertation, which I hereby submit for the above-mentioned degree at the University of the Witwatersrand, is my own work and has not previously been submitted by me for a degree at another university. Where secondary material is used, this has been carefully acknowledged and referenced in accordance with University requirements. I am aware of University policy and implications regarding plagiarism.

Student: Daramola Adesuyi

Signature: ……A.D……..

ACKNOWLEDGEMENTS

I am most grateful to God, the Lord of great things for his unfailing love, mercy and kindness.

My humble appreciation to my supervisor Bernice Welgemoed, for her enormous guidance, mentorship, ideas, and administrative assistance that have enabled me to accomplish this research work.

My sincere appreciation to my parents, relatives, siblings, and friends for moral, encouragement and spiritual guidance.

ABSTRACT

This dissertation examines the legal framework relating to cybercrime in Uganda and its effect on the enforcement of its terms. Investigating this issue is crucial in the wake of the rise in global interconnectivity as a result of the relative advances in technology, which challenge the application of the old standard of classification and investigation of traditional crimes. Unlike the advanced nations, the current laws regulating criminal conduct in most developing nations today are ill-equipped to cope with these emerging cybercrimes.

Therefore, this dissertation argues that Uganda's extant legal framework is manifestly inadequate to protect individuals from the threats resulting from cybercrime effectively. This view is held based on an analysis of the major procedural challenges and issues in Uganda today and a review of the current legal regime. This dissertation contends that, contrary to the common belief, merely enacting legislation, which is a 'cut and paste' of foreign cyber laws, does not automatically resolve issues related to cybercrimes in Uganda. Furthermore, the dissertation argues that useful lessons can be obtained from an effective legal regime based on insights from the Council of Europe Convention on Cybercrime, and South Africa. Similarly, other pragmatic ways of effective protection against cybercrime in Uganda are suggested to improve awareness and scholarship, strengthen law enforcement agencies and the judiciary, and improve cooperation with international and regional cybercrime regimes.

Keywords: cybercrime, cyber laws, enforcement challenges, Ugandan legislation, Convention on Cybercrime.

ABBREVIATIONS AND ACRONYMS

ABI	Amalgamated Beverage Industries
APA	Anti-Pornography Act
ATA	Anti-Terrorism Act
AU	African Union
AU	African Union
AUCPDP	African Union Convention on Cyber Security and Personal Data Protection
CERT	Computer Emergency Team
CFAA	Computer Fraud and Abuse Act
CMA	Computer Misuse Act
CNRA	Copyright and Neighbouring Rights Act
COE	Council of Europe
CPCA	Criminal Procedure Code Act
CSIRT	Computer Security Incident Response Team
DDoS	Distributed denial of service
DPO	Data Protection Office
DPPA	Data Protection and Privacy Act, 2019
DTPS	Department of Telecommunications and Postal Services
ECTA	Electronic Communications and Transactions Act
ESA	Electronic Signatures Act
ETA	Electronic Transaction Act
EU	European Union
FIUs	Financial Intelligence Units
FNB	First National Bank
GDPR	General Data Protection Regulation
ICT	Information and Communication Technology
IP	Internet Protocol
ISPs	Internet Service Providers
ITU	International Telecommunication Technology
MoICT	Ministry of Information and Telecommunication
NCPF	National Cyber Security Policy Framework
NIST	National Institute of Standards Technology

NITA	National Information Technology Authority
NITA-U	National Information Technology Authority Uganda
NITA-U Act	National Information Technology Authority Act
PKI	Public Key Infrastructure
RICA	Regulation of Interception of Communications Act
SaaS	Software-as-a-Service
SADC	Southern Africa Development Community
SAPS	South African Police Services
SNS	Social Networking Sites
UN	United Nations
UNODC	United Nations Office on Drugs and Crime
UPF	Uganda Police Force

TABLE OF CONTENTS

DECLARATION i
ACKNOWLEDGEMENTS iii
ABSTRACT iv
ABBREVIATIONS AND ACRONYMS v
CHAPTER ONE: INTRODUCTION 1
1.1 Introduction 1
1.2 The cybercrime phenomenon 5
1.3 Problem statement 10
1.4 Objectives of the study 14
1.5 Research questions 14
1.6 Research hypothesis 14
1.7 Significance of the study 15
1.8 Research methodology 15
1.9 Outlining of the remaining chapters 16
CHAPTER TWO: AN EXAMINATION OF REGIONAL EFFORTS TOWARDS CYBERCRIME CONTROL 17
2.1 Introduction 17
2.2 The Council of Europe Convention on Cybercrime 17
2.3 Challenges to the Cybercrime Convention 20
2.3.1 Transborder access 20
2.3.2 Cloud computing 23
2.3.3 Data protection laws 24
2.4 The African Union Convention on Cyber Security and Personal Data Protection 26
2.5 Conclusion 29
CHAPTER THREE: COMPUTER-RELATED OFFENCES IN UGANDAN STATUTES 31
3.1 Introduction 31
3.2 Offences against the State 31
3.2.1 Offences against the Critical National Infrastructure 32
3.2.2 Offences Related to Cyber Terrorism 34

3.3 Offences against confidentiality, integrity and availability of computer data and system 35
3.3.1 Unlawful access to computer and information systems 36
3.3.2 Unauthorised interception 37
3.3.3 Misuse of devices 37
3.3.4 Unlawful interference 38
3.4 Offences against the individual 39
3.4.1 Offences related to child pornography 39
3.4.2 Identity theft offences 41
3.4.3 Cyberstalking offences 42
3.5 Cyberfraud and other related offences 44
3.5.1 Electronic fraud 44
3.5.2 Computer-related forgery 45
3.5.3 Offences relating to copyright and other related rights 46
3.6 Conclusion 47
CHAPTER FOUR: LEGAL FRAMEWORKS FOR COMBATTING CYBERCRIME IN UGANDA 49
4.1 Introduction 49
4.2 Institutional framework of cybercrime in Uganda 50
4.2.1. Financial Intelligence Authority 50
4.2.2 Minister of Information and Communication Technology (MoICT), Uganda 50
4.2.3 Computer Emergency Response Team 51
4.2.4 Uganda Police Force Cybercrime Unit 52
4.2.5 Financial Intelligence Unit ..... **Error! Bookmark not defined.**
4.3 National legislations on cybercrime in Uganda 52
4.3.1 Computer Misuse Act, 2011 52
4.3.2 The Electronic Transaction Act 2011 55
4.3.3 The Electronic Signature Act 2011 57
4.3.4 Data Protection and Privacy Act 2019 58
4.4 Other legislative mechanisms 62
4.4.1 The National Information Technology Authority Act 2009 62
4.4.2 The Regulation of Interception of Communication Act 2010 64
4.5 Emerging issues and challenges in the Arena of Cyberlaw in Uganda 65

4.5.1 Jurisdictional challenge 65
4.5.2 Evidential issues 68
4.5.3 Searches and seizures 71
4.5.4 Extradition and international cooperation 74
4.6 Conclusion 77
CHAPTER FIVE: A COMPARATIVE OVERVIEW OF SOUTH AFRICAN CYBERCRIME LAWS WITH RELEVANT PROVISIONS IN UGANDA 78
5.1 Introduction 78
5.2 National cybercrime legislation in South Africa 78
5.2.1 Electronic Communications and Transactions Act, 2002 78
5.2.2 The Cybercrimes Bill 79
5.2.3 Critical Infrastructure Protection Act, 2019 80
5.2.4 South Africa National Cyber Security Policy Framework (NCPF) 82
5.2.5. Legal position regarding search and seize of electronic evidence in South Africa 83
5.4 How the Cybercrimes Bill has addressed ECTA identified shortcomings 86
5.5 International cooperation and structures 88
5.6 Comparison 89
5.7 Conclusion 93
CHAPTER SIX: CONCLUSIONS AND RECOMMENDATIONS 95
6.1 Introduction 95
6.3 Recommendations 98
6.3.1 Legislative recommendations 98
6.3.2 Ratification and domestication of the Convention on Cybercrime 98
6.3.3 Dedicated structures to manage cybercrime 99
6.3.4. Cybercrime awareness 99
BIBLIOGRAPHY 100

CHAPTER ONE: INTRODUCTION

1.1 Introduction

The arrival of internet technology has revolutionised every aspect of human life. It has changed the way we work and live, and we have come to depend on it in every sphere of our activities. From a population of 16 million connected to the internet in 1995, we now have more than three billion and growing.[1] It is projected that internet connectivity will double in the coming years as a result of some factors: expansion of the internet's generic domain name space and the growing prevalence of tablets and smartphones with internet access. While the benefits of global connectivity have grown exponentially, the internet has also become an irresistible magnet for the preparation and commission of crimes. Cybercrime perpetrators have become innovative and gravitate towards jurisdictions where there is a lack of adequate legislative framework, lack of international cooperation on cybercrime, outdated legal systems, and law enforcement agencies that do not have the skills and resources to investigate, monitor, and prosecute cybercrimes.

The borderless and global nature of the internet facilitates cooperation and coordination among cybercriminals to commit a criminal act in one country and hide behind cyberspace's anonymous nature, thereby frustrating a country's ability to apply its criminal laws against the perpetrator.[2] It has also become possible for an alleged cybercriminal in 'Country A' to commit a criminal act against a victim who is physically situated within the territory of 'Country B' and also hacking into a computer located in 'Country C' without the perpetrator leaving his/her own country.[3] In 2000, 'the Love Bug virus'[4] spread throughout the world estimated to have caused $10 billion in

[1] Available at http://www.internetworldstats.com/emarketing.html accessed 8 April 2020.
[2] J Vogel 'Towards a Global Convention Against Cybercrime, First World Conference on Penal law in Guadalajara, Mexico' (2007) available at http://www.penal.org/sites/default/files/files/Guadalajara-Vogel.pdf, accessed on 25 May 2020.
[3] S W Brenner & B-J Koops 'Approaches to cybercrime jurisdiction' (2004) 4 *J High Tech L* 1.
[4] The source of the virus was eventually traced in the Philippines and with the help of the Federal Bureau of Investigation (FBI), the Philippines' National Bureau of Investigation identified a suspect, one Onel de Guzman, as the person who created the virus and uploaded it on the internet. While there was sufficient evidence against De Guzman, prosecutors for the government faced a serious obstacle before they could file charges against him. It was observed that at the time of the commission of the crime, the Philippines had no laws

damage and affected over 20 countries.[5] At the time, there was no legislation dealing specifically with computer-related crimes in the Philippines, where the offender was located. Charges against the offender were dismissed, as the legal principle of *nullum crimen sine lege*, *nulla poena sine lege* applied. This principle means no punishment for a crime that is not recognised by law.[6]

In as much as various countries must have both substantive and procedural legislation prohibiting cybercrime, it is important to harmonise these different jurisdictional provisions. The need for legislative harmonisation of cybercrime laws was clearly evident in the case of *Yahoo, Inc. v La Ligue Contra Le Racisme et L'Antisemitism*,[7] which also raises important issues in the procedural enforcement of cybercrime legislation such as jurisdiction and international cooperation.

The above case scenario underscores the need for countries to update their individual rules of evidence and other related provisions to cover digitised information, as this would facilitate global cooperation in investigations covering multiple jurisdictions.[8] The need for global collaboration and tackling the increasing rate of cybercrimes led the 43 members of the Council of Europe to draft the first multilateral agreement on cybercrime, which aimed to harmonise both substantive and procedural laws.[9] The

---

criminalising computer hacking. He was, however, charged with credit card theft. As there was no cybercrime law in the Philippines as at the time, he could not be convicted of such.

[5] M D Goodman & S W Brenner 'The emerging consensus on criminal conduct in cyberspace' (2002) 3 *UCLA Journal of Law & Technology* 4-24.

[6] H T Tavani *Controversies, Questions, and Strategies for Ethical Computing* 4 ed (2013) 184.

[7] *Yahoo!, Inc. v La Ligue Contre Le Racisme et L'Antisemitisme*, 169 F. Supp. 2d 1192 (N.D. Cal. 2001) Yahoo! filed an action in the United States District Court for the Northern District of California seeking declaratory relief from the French court's order on the basis that the order (in its entirety) was not enforceable under the United States Constitution. Having concluded that the French order violated Yahoo!'s First Amendment rights, the United States District Court of California stated that such violation no matter how short in duration constituted 'irreparable injury'. The court held that although the French order could regulate speech occurring in France on the basis of content or viewpoint, the French order could not be enforced against the same speech occurring simultaneously in the United States. Enforcement of such an order would impermissibly violate the First Amendment – even if such speech was considered highly offensive. Accordingly, the court refused to enforce the French order prohibiting Yahoo! from displaying or selling Nazi propaganda and artefacts through the use of its web site.

[8] P Williams 'Organized crime and cybercrime: Synergies, trends, and responses' (2001) 6 *An Electronic Journal of the US Department of State* 22-26.

[9] J Clough 'A world of difference: The Budapest Convention on Cybercrime and the challenges of harmonisation (2014) 40 *Monash University Law Review* 698.

multilateral agreement, also referred to as the Convention on Cybercrime, was adopted on 8 November 2001.[10] It was opened for signature in Budapest on 23 November 2001 with the requirement of ratification by five states to enter into force, including at least three member states of the Council of Europe.[11] As of 23 June 2020, the Convention had been ratified by 65 member states.[12] Seven African Union members have signed the Convention on Cybercrime (South Africa, Benin, Cabo Verde, Ghana, Mauritius, Morocco, Nigeria and Senegal),[13] out of which six have ratified except for South Africa.[14] By ratifying this Convention on Cybercrime, member states agree to ensure that their domestic laws will criminalise conduct described in the Convention as crimes. It is pertinent to note that Uganda has not signed, ratified nor adopted the Convention on Cybercrime.

An Additional Protocol to the Convention on Cybercrime was drafted to cover issues such as acts of a racist and xenophobic nature committed through computer systems. The Additional Protocol to the Convention on Cybercrime was opened for signature in Strasbourg on 28 January 2003 and came into force on 1 March 2006.[15] This separate protocol could be interpreted as requiring nations to punish anyone guilty of 'insulting certain groups of people publicly, based on characteristics such as race or ethnic origin through a computer system'.[16] As of 23 June 2017, the Convention had been signed by 38 members states and ratified by 24 members states.[17] Also, Uganda has not signed nor ratified the Additional Protocol to the Convention on Cybercrime.

---

[10] Council of Europe 'Convention on Cybercrime' available at http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=1&DF=&CL=ENG, accessed on 22 May 2020.

[11] L Lloyd *Information Technology Law* 7 ed (2014) 217.

[12] Convention on Cybercrime op cit note 10.

[13] Council of Europe 'Chart of signatures and ratifications of Treaty 185' available at http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/treaty/185/signatures?p_auth=XvRotrxg accessed on 18 October 2020.

[14] Ibid.

[15] Additional Protocol to the Convention on Cybercrime, Concerning Acts of a Racist and Xenophobic Nature Committed through Computer Systems available at http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm, accessed on 22 May 2020.

[16] Ibid.

[17] See, List of Signatories to Additional Protocol to the Convention on Cybercrime, concerning acts of a Racist and Xenophobic Nature Committed through Computer Systems available at http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT-189&CM-4&DF-&CL-ENG, accessed on 23 June 2020.

Encouraged by the Council of Europe's standards, the African Union adopted the African Union Convention on Cyber Security and Personal Data Protection, 2014.[18] This Convention represents the existing commitments of African Union member states at a regional level in building and strengthening their existing legislation on information and communication technologies of member states. As of 23 June 2020, the Convention had been signed by 14 members and ratified by 5 members.[19] Also, Uganda has not signed nor ratified the African Union Convention on Cybersecurity and Personal Data Protection.

Before 2011, there was no specific law on cybercrime in Uganda. The main legislation on criminal matters is the Penal Code Act (the Act).[20] The Act has been amended; however, these amendments do not address issues that pertain to cybercrimes. In 2011, the Computer Misuse Act (CMA) came into force. Before the enactment of the CMA, Uganda was in a similar position to the Philippines', where the suspect of the 'Love Bug virus' could not be effectively prosecuted due to the Philippines' criminal law inadequacies.

However, with the available legal and institutional framework in Uganda, many of the country's citizens would increasingly become victims of cybercrimes.[21] Cybercrimes such as cyberterrorism, intellectual property infringement, internet fraud, online child exploitation and pornography, piracy, hacking all remained a challenge for Uganda.[22] This is yet to include more undiscovered crimes, given the pace at which technology and technological innovations are advancing.[23] Institutions such as the Uganda Police Force and the Ministry of Information and Telecommunication have policy frameworks

[18] On 27 June 2014, at its 23rd Ordinary Session in Malabo.
[19] See, List of African Union Convention on Cyber Security and Personal Data Protection. Available at http://au.int/en/treaties/african-union, accessed on 23 June 2020.
[20] Chapter 120 of the Laws of Uganda 2000 and as amended by the Penal Code (Amendment) Act 8 of 2007.
[21] Ministry of Information and Communications Technology *National Information Security Strategy* (NIIS) (2011) 25.
[22] M Faisal 'Uganda's legal and institutional framework in combating cybercrime: A review of Uganda's ICT law new opportunities in the wake of recent enactments, old challenges as to implementation and sensitisation' Kampala International University available at http:// http://rm.coe.int/16802f2349, accessed on 6 June 2020.
[23] K Mitnick & S L William *The Art of Intrusion, The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers, Hardback* (2005).

designed to address cybercrime. However, the institutions, particularly the Uganda Police Force, lack the expertise in detecting cybercrimes.[24]

Uganda's legal and institutional framework falls short of international standards. The Ugandan Government has acknowledged that it has very weak legislation regulating what occurs in the cyberspace industry[25] and laws pertaining to cybercrimes. Part of the reason is that the laws, which aim at combatting cybercrimes are still in their early stages, resulting in the enforcement of these laws continuously remaining low. With the expanding nature of internet technology, new crimes outside the confines of the statutory provisions continue to present more difficulty for the procedural enforcement of cybercrime laws.[26] By implication, the current laws meant to tackle cybercrime in Uganda could possibly remain inadequate to address these new and evolving forms of crime.[27] Based on the above, it would provide a possible explanation as to why there has been an increase in the cybercrime rates in Uganda.[28]

Today, the number of internet users is growing steadily in Uganda and encompassing 31.3% of the population.[29] The growth in internet users points to an urgent need for the Ugandan Government to regulate the internet. These laws are urgently needed to protect users of internet service providers in Uganda and enhance cybersecurity. It is against this background that this dissertation is written.

1.2 The cybercrime phenomenon

The definition of cybercrime or what constitutes cybercrime is a topic that has generated much debate. Some writers use the terms 'cybercrime,' 'computer crime,' 'network crime,' 'virtual crime,' and 'high-tech crime' interchangeably. Cybercrime refers to a crime related to cyberspace, computers, computer networks, and the

---

[24] F Tushabe *Computer Forensics for Cyberspace Crimes* (unpublished Masters Dissertation, University of Makerere, 2004) 24.
[25] NIIS op cit note 21 at 56.
[26] Y Aslan 'Global nature of computer crimes and the Convention on Cybercrime' (2006) 2 *Ankara LR* 3.
[27] *Uganda vs Dr Aggrey Kiyingi* [2006] UGHC 52.
[28] P Mwaita & M Owor 'Workshop Report on Effective Cybercrime Legislation in Eastern Africa' Dar es Salaam Tanzania (2013) available at http://rm.coe.int/16802f2349, accessed 24 May 2020.
[29] Uganda Communication Commission 'Report on status internet Users March 2017' available at http://www.internetworldstats.com/af/ug.htm, accessed 24 May 2020.

internet. This definition points to three main components of cybercrime, namely, a computer, cyberspace, network, and the internet.
The term “computer” means:

> an electronic, magnetic, optical, electrochemical, data processing device, and a group of such interconnected or related devices performing logical, arithmetic, and storage functions; and includes any data storage facility or communications facility directly related to or operating in conjunction with such a device or group of such interconnected or related devices.[30]

The term ‘Internet’ is defined as:

> a global network wherein devices such as computers, servers, and smart devices are interconnected for data and information exchange. It comprises of public, private, individual and government networks in the domestic and global context, interconnected by a far-reaching array of electronic, wireless, and optical networking technologies.[31]

The term ‘cyberspace’ is used to describe anything related to computer networks or information technology and the internet. It includes the internet, the billions of computers the internet connects, the institutions that enable it, and its experiences.[32] For example, conversations or business transactions taking place on social media platforms such as Twitter, Facebook, or WhatsApp can be said to have been taken place in cyberspace. Richard Clarke explained it clearly when he said:

> Cyberspace is all of the computer networks in the world and everything they connect and control. It’s not just the Internet. Let’s be clear about the difference. The Internet is an open network of networks. From any network on the Internet, you should be able to communicate with any computer connected to any of the Internet’s networks. Cyberspace includes the Internet plus lots of other

[30] Section 1 of the CMA.
[31] IP Location available at http://www.iplocation.net/internet, accessed on 27 May 2020.
[32] K Okafor ‘Legal perspectives to cyber security in Nigeria: Bold Perspectives’ in A Adekunle (ed) *Combatting Cybercrimes in Nigeria: Trends and Issues* (2017) 249.

> networks of computers that are not supposed to be accessible from the Internet. Some of those private networks look just like the Internet, but they are, theoretically at least, separate. Other parts of cyberspace are transactional networks that do things like sending data about money flows, stock market trades, and credit card transactions. Some networks are control systems that just allow machines to speak to other machines, like control panels talking to pumps, elevators, and generators.[33]

Although the term 'cybercrime' is generally used by all, a serious problem that has been encountered by scholars is that there is no universally accepted definition of this term.[34] Although most scholars have found it difficult to identify exactly what aspects are attributable to this term, some researchers have argued that defining the term either too broadly or too narrowly creates the risk of missing the real problem when it comes.[35] Other legal researchers have argued that a broad definition of the term is necessary because of the rapid emergence of new technology-specific criminal behaviours.[36]

Another concern raised by academic scholars and researchers is that it becomes difficult to achieve a global definition for cybercrime, as it is continually changing and evolving. The scope of computer-related crimes and the definition of cybercrimes continue to advance.[37] The expanding nature of computer technology has made cybercriminals more refined in their criminality and broadened their acts towards new computer crimes that fall outside the confines of the statutory definition of cybercrime, thereby making it more difficult for the procedural enforcement of cybercrime laws.[38]

---

[33] R A Clarke & R K Knake 'Cyber War Excerpt' 5 available at https://richardaclarke.net/wp-content/uploads/2019/05/Cyber-War-Excerpt.pdfcontent/uploads/2019/05/Cyber-War-Excerpt.pdf, accessed 6 June 2020.
[34] International Telecommunication Union 'Understanding Cybercrime: A Guide for Developing Countries' (2011); Explanatory Report to the Council of Europe Cybercrime Convention, ETS No. Criminal Policy and Research, 10(1) 27-37.
[35] C J Franklin *The Investigator's Guide to Computer Crime* (2006) 7.
[36] R M Kadir 'The scope and the nature of computer crime statutes: A comparative study' (2010) 11 *German LJ* 614.
[37] S Gordon & R Ford 'On the definition and classification of cybercrime' (2006) 2 *Journal of Computer Virology* 13-20.
[38] Aslan op cit note 26 at 3.

It is surprising that the CMA and the African Union Convention, contain no definition of cybercrime. The fact that prior to the enactment of the CMA and subsequent adoption of the African Union Convention, there had been diverse connotations of what acts amount to cybercrimes. It would have been expected that such pieces of legislation would at least include a workable definition of cybercrime. The absence of a definition of cybercrime in the statute book creates difficulty in establishing what exactly can be attributed to this term.

The Council of Europe Convention on Cybercrime[39] defines cybercrime as a range of malicious activities that fall into four broad categories of computer-related crimes:

1. Security breaches such as hacking, illegal data interception, and system interferences that compromise network integrity and availability
2. Fraud and forgery
3. Child pornography
4. Copyright infringements.

The United Kingdom Home Office, in their Serious and Organised Crime Strategy, published in October 2013, tried to provide a more functional definition of cybercrime[40] and resorted to using an umbrella term to describe two distinct but closely related criminal activities – cyber-dependent crime and cyber-enabled crime.[41] As defined by the United Kingdom Home Office,[42] cyber-enabled crimes are traditional crimes that can be increased in scale or reach by using a computer, computer networks, or other forms of information communication technology (ICT). These acts include hacking,

[39] A copy of the Convention is available at http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm, accessed 24 May 2020.
[40] The strategy is available at http://www.gov.uk/government/publications/serious-organised-crime-strategy, accessed on 23 June 2020.
[41] It states that cyber-dependent crimes are crimes that can be committed only through the use of Information and Communications Technology (ICT) devices are both the tools for committing the crime, and the target of the crime eg developing and propagating malware for financial gains, hacking to steal, damage, and network or activity, while defining cyber-enabled crimes as crimes that can be conducted on or offline, but online may take place at unprecedented scale and speed, for example, data theft and cyber-enabled fraud.
[42] M McGuire & S Dowling 'Cybercrime: A review of the evidence'- Summary of key findings and implications (2013) Home Office Research report 75 available at http://www.justiceacademy.org/ishare/Library-UK/horr75-chap1.pdf accessed on 23 June 2020.

distributed denial of service (DDoS) attacks, and the spread of viruses.[43] It should be noted that the definition appreciates the fact that cybercrimes are not only committed online but could start online while ending up offline. However, there might be differences between cybercrimes and cyber-enabled crimes.

The definition of cybercrime as applicable in the United States takes a relatively broader view of the behavioural constituents of crime committed through the computer and cyberspace. The United States Computer Fraud and Abuse Act (CFAA) criminalises various conducts relating to the use of computers in criminal behaviours. These criminalised acts include acts such as the conduct relating to the obtaining and communicating of restricted information; the unauthorised accessing of information from financial institutions, the United States government, and 'protected computer'; the unauthorised accessing of government computers; fraud; the damaging of a protected computer resulting in certain types of specified harm; trafficking in passwords; and extortionate threats to cause damage to a 'protected computer'.[44] This broad approach adopted by the CFAA can be ascribed to the fact that the United States is one of the signatories to the Council of Europe Convention on Cybercrime. The United States Department of Justice classifies Cybercrime into three subgroups, namely:[45]

1. Existing offences in which the computer is used as a criminal instrument. For example, e-commerce fraud, criminal intellectual property infringement, and illegal interception.
2. Crimes where the computer or computer network is the target. For instance, DoS or DDoS attack,[46] hacking (gain access to a computer system without

[43] G Kirwan *The Psychology of Cybercrime: Concepts and Principles* (2011) 45.
[44] Computer Fraud and Abuse Act 18 U.S.C. 1030.
[45] S Morris 'The Future of Net-crime Now: Part 1 – Threats and Challenges', Home office Online Report 62/04, available at http://www.globalinitiative.net/download/cybercrime/europe-russia/Home%20Office%20-%20The%20future%20of%20netcrime%20now%20-%20Part%201%20%E2%80%93%20threats%20and%20challenge.pdf, accessed on 7 June 2020.
[46] DoS attack (denial-of-service attack) or DDoS attack (distributed denial-of-service attack) is an attempt to make a machine or network resource unavailable to intended users. See, http://en.wikipedia.org/wiki/Denial-of-serviceattack, accessed on 7 June 2020.

authorisation), and aggravated hacking (gain access to a computer system without authorisation to commit other crimes).

3. Crimes in which the use of the computer is an incidental aspect of the commission of the crime but may afford evidence of the crime. For example, phone records of conversations between offender and victim before a homicide. In such cases, the computer is more a source of evidence.[47]

The South African Electronic Communications Amendment Act 1 of 2014 defines cybercrime as any criminal or other offence facilitated by or involves the use of electronic communications or information systems, including any device or the Internet or any one or more of them.[48] This definition seems to be an all-encompassing approach from the South African Act, as it tends to group every offence as cybercrime as far as it has been committed through the use of a computer device.[49] This methodology could also be ascribed to the fact that South Africa is one of the African signatories to the Council of Europe Convention on Cybercrime.[50]

1.3 Problem statement

Article 28(7) and (12) of the Constitution of Uganda prohibits persons from being criminally prosecuted for an act that was not considered a crime at the time of commission or omission. A person may only be criminally prosecuted for an act or omission that constituted a criminal offence at the time of commission or omission, which has been defined under the law and where punishment is prescribed. These constitutional rights aim at preventing persons from the retroactive application of laws, whereby a person may be tried, convicted, and sentenced under an unwritten law.[51]

---

[47] Susan W. Brenner 'U.S. Cybercrime Law: Defining Offences', *Information Systems Frontiers*, (2004) 6 at 116-117.

[48] 'Overview of the Electronic Communications Amendment' Available at http://www.ellipsis.co.za/wp-content/uploads/2014/04/Overview-of-the-Electronic-CommunicationsAmendment-Act-1-of-2014.pdf accessed 27 May 2020.

[49] D van der Merwe 'A comparative overview of the (sometimes uneasy) relationship between digital information and certain legal fields in South Africa and Uganda' (2014) 17 *Potchefstroom Electronic Law Journal* 289-612.

[50] The second and third signatory to the COE Convention is Senegal and Rwanda.

[51] Constitutional Reference No 04/11 at 4.

The criminal law principle of *nullum crimen sine lege*[52] and *nulla poena sine lege*[53] curtail efforts to investigate and prosecute Cybercrimes due to the continuous rise in the techniques used to commit Cybercrime. These new techniques are considered "new crimes", which are not found in existing legislation. Before considering the effectiveness of Ugandan legislation, this research will aim to address the issue of whether cybercrime is in fact an entirely new category of offence without involvement with its offline counterpart. This category of cybercrimes as the 'genuine cybercrime' refers to entirely new crimes and includes the security of computers and data. The interests endangered by this category are not protected under existing criminal law. Second, whether cybercrime is merely a conventional crime committed in new ways. The category speaks to whether 'traditional crimes, which already exist in current legislation, which are facilitated in a novel manner with the use of a computer'. The interests endangered by this category are already protected under existing criminal laws. It is on this basis that this research will determine the effectiveness of Ugandan laws.

The emergence of the internet and the increase in online crimes have triggered fundamental evidentiary issues, especially concerning the proof required for offences committed in cyberspace. It should be noted that section 8(4) of the Electronic Transactions Act, 2011 requires the court to take into account the reliability in how the electronic records are generated, stored, or communicated. However, serious issues have been raised in the digital world due to malpractices such as falsification of information and impersonation, in relation to the authenticity of information relied upon as evidence.[54] This raises queries as to how it is possible to prove the creation and transmission of electronic communication by one party when the party's name as the author of the post could have been inserted by another.[55] Notwithstanding challenges concerning the admissibility and appreciation of electronic evidence, Uganda still has a long way to go in keeping pace with global developments. Although section 8 of the

[52] This means that an individual cannot face criminal liability except for an act that was criminalised by law before they performed the act.
[53] This principle means that a person cannot be punished for doing something that is not prohibited by law.
[54] Vastina Rukimirana Nsaza presentation By Uganda Law Reform Commission on the Law of Evidence ALRAESA conference on 29th – 30th June 2017.
[55] Ibid.

ETA provides clarity with regard to admissibility and weight of evidence of electronic data, they cannot be said to be without limitations. It is clear that Uganda has yet to devise a mechanism for ensuring the veracity of contents of electronic records, which are open to manipulation by any party by obtaining access to the server or space where it is stored. In addition, there is a scarcity of technical skills of stakeholders in the criminal justice system to handle computer and electronic devices that store and process data electronically and digitally.[56] This task requires expertise in information and communication technology. Judges, lawyers and prosecutors need to have extensive computer skills to be able to form independent opinions and understanding of electronic evidence presented to them to satisfy the requirement of section 8 of the ETA and relevant provisions of the CMA. Currently, there are acute shortages of experts and professionals in information and communication technology among lawyers, judges and law enforcement personnel for the successful enforcement of the CMA.[57]

Also, the collection of data outside the territorial boundaries have proven to be one of the most critical challenges to affect cybercrime investigation and prosecution.[58] Although cooperation between Uganda and other countries in the fight against cybercrime is encouraged by the CMA,[59] the requirement for international cooperation by the CMA is not binding on other countries. In essence, other countries are not bound to cooperate with Uganda or render mutual assistance in issues pertaining to cybercrimes if there are no bilateral treaties amongst the participating parties and as enshrined in each state's national legislation.[60] Besides the issue of which country has jurisdiction over the prosecution of the offender, the other question remains, which country has primacy to prosecute if more than one country claims jurisdiction. Both

---

[56] C Emmanuel *An analysis of the adequacy of the Electronic Transactions Act, 2011 in governing e-commerce in Uganda: A case study of online motor vehicle trade in Uganda'* (unpublished LLM dissertation, Uganda Christian University, 2016) 64.
[57] Ibid.
[58] A Singh Poonia, A Bhardwaj & G S Dangayach 'Cyber Crime: Practices and Policies for Its Prevention' (2011) In the First International Conference on Interdisciplinary Research and Development, Special No. of the International Journal of the Computer, the Internet and Management vol 19, available at https://www.academia.edu/41411512/Meaning_and_Nature_of_Cyber_Crime, accessed on 7 June 2020.
[59] Section 30(1) of the CMA.
[60] S D Bedi *Extradition in international law and practice* (1966) 69.

these questions present major challenges. The primary legislation on extradition in Uganda is the Extradition Act, 1964. The Act provides that there is no general obligation to surrender a person who is within its territory unless it had signed bilateral or multilateral[61] extradition treaties agreeing to transfer the 'fugitive offenders'.[62] The nature of cybercrime offences makes them one of the exceptional cases where the fugitive criminal could commit the offence while still being physically present in the extraditing country's territory. The foundation on which extradition is usually established is on the principle of 'dual criminality,' which means that before a criminal can be validly extradited, the alleged offence must be a crime, which is punishable in the jurisdiction seeking extradition; without satisfying this requirement, the criminal may not be extradited. It should be noted that the inability of the extradition law to respond quickly to computer related crimes, present significant challenges to current law enforcement resources and skills in combating cybercrime.[63]

As a result of the gaps discussed above, cybercrime continues to be a challenge in Uganda.[64] The Uganda government does not prioritise funding for cybersecurity infrastructure and does not allocate sufficient funds to pay for solutions, even after identifying security breaches in sensitive government and financial systems.[65] This has negatively affected the Ugandan Government's efforts in combatting cybercrime.[66] This presents difficulty in determining how many offences have been committed and against who, as well as the damage resulting from these offences.

The development of the internet and the proliferation of computer technology have created new opportunities for those who would engage in illegal activities.[67] The rise of technology and online communication has not only produced an exponential

[61] Section 2 of the Extradition Act of 1964 (Application of the Act to Commonwealth countries).
[62] M Kassim-Momodu 'Extradition of fugitives by Nigeria' (1986) 3 *International and Comparative Law Quarterly* 512-530.
[63] Ibid
[64] Uganda 2020 Crime & Safety Report available at https://www.osac.gov/Country/Uganda/Content/Detail/Report/972253e2-8a5b-4164-b3c5-18824394519c, accessed May 4 2021.
[65] Ibid.
[66] J M Kizza *Ethical and Social Issues in the Information Age* (2003) 18.
[67] Mcafee Inc 'A Good Decade for Cybercrime' (2013) available at http://www.biz-file.com, accessed 2 October 2020.

increase in the incidence of criminal activity, but it has also resulted in the emergence of what appears to be some new varieties of illegal activity.

The existing laws on cybercrime in Uganda are inadequate. The result of the inadequacies and the ineffectiveness of the law enforcement officers have led to an increase in cybercrime involving huge financial losses to both individuals and the country. The existing cybercrime legislation leaves the victims with no possibility of relief. The extent to which efforts are being made internationally to combat cybercrime will form the fulcrum of this study, bearing in mind the provisions of the Council of Europe Convention on Cybercrime.

1.4 Objectives of the study

The study has two main objectives:

- This study's main objective is to critically examine both the legal and institutional frameworks relating to cybercrime in Uganda against established international and regional standards.
- The study further aims at analysing the legal issues and problems that arise in dealing with cybercrimes.

1.5 Research questions

This research study seeks to answer the following questions:

- What are the various forms of cybercrimes in the cyber legal framework of Uganda?
- What is the practicability of the existing Ugandan legislation relating to cybercrime and the effect these laws have on their enforcement?
- What lessons can be learnt from South Africa and compliance with the Council of Europe Convention on Cybercrime?

1.6 Research hypothesis

The hypothesis guides this study that the provisions of Uganda's cyber legal framework on cybercrimes fall short of the established international standards, thereby facilitating advanced cyber insecurity.

1.7 Significance of the study

There are but a few writings regarding cybercrime in Uganda, especially critical analyses of the existing laws. This study contributes to bridging the gap in knowledge regarding cybercrime laws in Uganda regarding international and regional standards.

The Council of Europe Convention on Cybercrime is the most comprehensive treaty on cybercrime to date, not only in terms of its substantive law but also in its procedural law. The full implementation of this treaty will facilitate the gathering of electronic evidence, facilitate the investigation of cyber laundering, cyber terrorism and ensure the harmonisation and compatibility of criminal law provisions on cybercrime with those of other countries.

1.8 Research methodology

Examining cybercrime legislation in the selected legal regimes and analysing how they have been pragmatic in judicial practice; doctrinal research will be adopted. Doctrinal analysis can be explained as 'research which asks what the law is in a particular area'.[68] This method is frequently used when a researcher intends to investigate and analyse a body of law, including case law and relevant legislation. To this end, international and local authors' work on cybercrime, its challenges, and international efforts in combatting this menace have been consulted. The success achieved so far by the Council of Europe Convention on Cybercrime in enhancing international cooperation against cybercrime will also be studied.

This research will also adopt a qualitative analysis of the primary and secondary sources of law relevant to the study. Secondary sources to be consulted include materials from the internet, textbooks, articles, and other relevant documents. All sources consulted for information are acknowledged. The legal position in these sources will be critically analysed, the defects therein identified, and suggestions to improve Ugandan's current position on the subject matter. A reflective discussion on the literature and the literature review findings will be embedded throughout the main body of the research rather than summarised in a separate literature review chapter.

[68] M McConville & W Hong Chui *Research Methods for Law* (2007) 18-19.

1.9 Outlining of the remaining chapters

This research is divided into six chapters with subheadings discussed thereunder.

Chapter two: As shown above, cybercrime is an issue within national laws and has international influence. For this reason, this chapter presents an examination of the Convention on Cybercrime, as the most influential international legal instrument on cybercrime.

It should be noted that the Convention on Cybercrime is used as a model law in this dissertation since it contains comprehensive descriptions of the guidelines about cyber offences.

Chapter three provides an analysis of cybercrime offences recognised by the Uganda legal system. This chapter is divided into three segments: offences against the State; offences against the critical national infrastructure; and other related cyber offences against persons. References will be made to various regional and international instruments on cybercrime control.

Chapter four provides an analysis of both the legal and institutional frameworks relevant for combatting cybercrime in Uganda. This chapter further analyses the emerging issues and challenges in the arena of cyber law in Uganda, which are: jurisdictional issues; evidential issues; search and seizures; and extradition and international cooperation. The chapter forms the gist of the study.

Chapter five provides a comprehensive overview of South African cybercrime laws with relevant provisions in Uganda. The similarity between the Convention on Cybercrime and the South African legal system is one of the main reasons for choosing South Africa as a comparison subject. In this regard, South Africa's experiences and discussions may be more relevant than those of Uganda.

Chapter six provides findings, conclusions, and recommendations.

CHAPTER TWO: AN EXAMINATION OF REGIONAL EFFORTS TOWARDS CYBERCRIME CONTROL

2.1 Introduction

Before looking at the position regarding cyber laws in Uganda and the criticisms thereon, it is important to briefly discuss the reasons for the establishment of such legislation. As shown in the previous chapter, cybercrimes certainly have a transnational aspect. The transnational aspect of cybercrimes might arise from the nationality of the offender or the offender's geographic location and offence; it is also likely that a criminal investigation will involve more than one country. The aspect regarding jurisdiction becomes a problem in that laws are sometimes conflicting, especially considering situations where cybercrimes are committed in another country.[69] Therefore, countries that wish to effectively address cybercrime causes and protect themselves against its future impact need to reappraise their laws in line with international standards.[70]

This chapter will examine regional conventions put in place by the Council of Europe and the African Union. Each Convention will be assessed to understand law enforcement's powers in gathering evidence across borders to tackle cybercrimes and the challenges with regional agreements.

2.2 The Council of Europe Convention on Cybercrime

The Council of Europe Convention on Cybercrime, also known as the 'Cybercrime Convention', was adopted in Budapest in 2001 by the European Committee on Crime Problems.[71] The Cybercrime Convention is open to all member states of the Council of Europe and non-members (including countries outsides Europe, such as South Africa).[72] Currently, the Convention has been ratified by 65 member states.[73]

---

[69] F Cassim 'Addressing the spectre of terrorism: a comparative perspective' (2012) 15 *PELJ* 381.

[70] International Telecommunications Union 'Understanding cybercrime: Phenomenon, challenges and legal response', ITU Telecommunications Development Sector (September 2012) 104.

[71] N E Marion 'The Convention on Cybercrime Treaty: An exercise in symbolic legislation' (2010) 4 *International Journal of Cyber Criminology* 701.

[72] Article 36 (1) of the Cybercrime Convention

[73] Council of Europe Convention on Cybercrime available at http://coe.int/en/web/convention/ETSNO.185 accessed on 23 June 2020.

The Cybercrime Convention sets the standards for which domestic laws need to comply with and makes provision for international cooperation administration.[74] The Convention on Cybercrime has four major parts, encompassing both substantive and procedural issues.

Articles 2 to 10 of the Convention requires member states to criminalise certain conduct committed through, against, or related to computer systems, domestically, if they have not already done so. Cybercrime Convention has included these substantive crimes: offences against the 'confidentiality, integrity and availability' of computer data and systems: illegal access (Article 2), illegal interception (Article 3), data interference (Article 4), system interference (Article 5), and misuse of devices (Article 6). The offences included in the Cybercrime Convention also included offences that involve the use of computer systems to engage in conduct that has been criminalised outside the cyber-realm. These offences are computer-related forgery (Article 7), computer-related fraud (Article 8), offences related to child pornography (Article 9), and offences related to infringements of copyright and related rights (Article 10).[75]

In addition, the Convention on Cybercrime also made references to criminal procedures issues which Member State need to comply with. For instance, article 19 of the Cybercrime Convention regulates law enforcement's powers to search and seize computer data that is to be used as evidence.[76] The Cybercrime Convention also regulates mutual legal assistance agreements between member states regarding access to stored computer data,[77] and regulations regarding transborder access to stored computer data[78] to aid a member state in gathering evidence. Evidence in this context refers to evidence in the form of digital data stored on a device such as a hard drive, flash drive, or in cyberspace, connected either to cybercrime or to a traditional crime. Article 19 obliges member states to adopt such legislative and other measures, as may be necessary to empower its competent authorities to search:

[74] Explanatory Report to the Convention on Cybercrime European Treaty Series No. 185.
[75] The Council of Europe, Convention on Cybercrime, European Treaty Series No. 185. The next chapter will discuss how Uganda has criminalised these offences.
[76] Article 19 of the Cybercrime Convention.
[77] Articles 31 of the Cybercrime Convention.
[78] Article 32 of the Cybercrime Convention.

a. a computer system or part of it and computer data stored therein; and
b. a computer-data storage medium in which computer data may be stored.[79]

Furthermore, in the securing of the data, article 19 obliges member states to adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data, including the power to:

a. seize or similarly secure a computer system or part of it or a computer-data storage medium;
b. make and retain a copy of those computer data;
c. maintain the integrity of the relevant stored computer data;
d. render inaccessible or remove those computer data in the accessed computer system.'[80]

Article 31 of the Cybercrime Convention provides for mutual assistance regarding the accessing of stored computer data. This provision stipulates that a state party to the Convention can request another state party to the Convention to search and seize computer data within that second state's domestic territory. According to the domestic laws on search and seizures of that state.[81]

Article 27 of the Cybercrime Convention establishes procedures for a Member State to render mutual assistance requests to another Member State where there are no existing international agreements on mutual assistance and extradition. Article 32 of the Cybercrime Convention further provides for transborder access to stored computer data without seeking mutual legal assistance. However, the adoption of the Cybercrime Convention would not be without some challenges. These challenges will be discussed in the next section.[82]

---

[79] Article 19(1) of the Cybercrime Convention.
[80] Article 19(3) of the Cybercrime Convention.
[81] Article 31 of the Cybercrime Convention.
[82] These reports include the 'T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime' and the 'T-CY Guidance Note # 3 Transborder access to data (Article 32)'.
'Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY: Final report of the T-CY Cloud Evidence Group', and the open

2.3 Challenges to the Cybercrime Convention

The Cybercrime Convention was drafted approximately 20 years ago. The treaty focused on harmonising laws and increasing cooperation across borders to ensure that perpetrators could be prosecuted in multiple affected countries. The Cybercrime Convention was drafted before the exponential growth of internet usage, the development of cloud computing, and the digitalisation of almost all kinds of online interaction. These changes have created enormous challenges for law enforcement, given the global nature of the internet. In response, the Council of Europe's Cybercrime Convention Committee, also referred to as the 'T-CY,' proposed an additional protocol to the Cybercrime Convention designed, among other things, to address these challenges. In 2014, the T-CY offered an overview of its cybercrime efforts during the 12th Plenary of the Cybercrime Convention Committee. The T-CY agenda reflected ongoing discussions on several significant issues pertaining to transborder access, spam, rules on obtaining subscribers' information, and mutual legal assistance.[83] T-CY is a platform for periodic consultation between the representatives of the member states to the Cybercrime Convention.

Nevertheless, over the years, problems curtailing the rapid changes in technology have emerged, thus challenging the existing legal regime's adequacy. For purposes of this research, the issues identified by the T-CY will be discussed under three headings: transborder access, cloud computing, and data protection laws. However, there is no adequate solution to these issues at the moment.

2.3.1 Transborder access

Article 32(b) regulates transborder access to stored computer data without the authorisation of the state party in whose territory the evidence is located. Article 32(b) states that:

> A party may, without the authorisation of another party access or receive, through a computer system in its territory, stored computer data located in

letter of the Article 29 Working Party on the issue of direct access by third countries' law enforcement authorities to data stored in other jurisdiction.

[83] Council of Europe 'T-CY Committee: Guidance Notes' https://www.coe.int/en/web/cybercrime/guidancenotes, accessed on 8 February 2018.

> another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

The provision of this article is intentionally vague and left open to different interpretations by the different state parties, as can be read in the Explanatory Report on Article 32:

> The drafters ultimately determined that it was not yet possible to prepare a comprehensive, legally binding regime regulating this area. In part, this was due to a lack of concrete experience with such situations to date; and, in part, this was due to an understanding that the proper solution often turned on the precise circumstances of the individual case, thereby making it difficult to formulate general rules.[84]

The Explanatory Report goes further to provide that when a person is 'lawfully authorised' to disclose data, such authority may vary depending on the circumstances, the nature of the person, and the domestic laws.[85] It has been agreed that the suspect may consent to disclose the data and that a state may give another state consent to access the data. The T-CY has stated that 'service providers are unlikely to be able to consent validly and voluntarily to the disclosure of their user's data under Article 32'.[86] Although 'service providers are only holders of such data; they do not control nor own the data, and they will, therefore, not be in a position to validly consent.'[87]

In 2011, the T-CY set up an ad-hoc sub-group on jurisdiction and transborder access to data and data flows, resulting in a proposal on draft elements of an additional protocol to the Cybercrime Convention regarding transborder access to data in

---

[84] Council of Europe 'Explanatory Report to the Convention on Cybercrime' (Budapest, 23 November 2001) https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cc e5b, accessed on 8 February 2018, para 293.
[85] Ibid para 294.
[86] T-CY Guidance Note # 3 op cit note 14.
[87] Ibid.

2013.[88] However, nothing seems to have been done with these proposals. Again, in December 2014, the T-CY set up the Cloud Evidence Group to 'explore solutions for access to evidence in the cloud for criminal justice purposes'.[89] The Cloud Evidence Group has noted a lack of clear and efficient international frameworks regarding transborder data searches, which has resulted in states increasingly pursuing unilateral solutions in practice.[90] The T-CY stated that an international solution is required, which provides a framework for lawful transborder access to data.[91] In its plenary in June 2017, the T-CY approved the terms of reference to prepare a Draft 2nd Additional Protocol to the Cybercrime Convention, which was expected by December 2019.[92] Due to the COVID-19 pandemic, the Cybercrime Convention Committee has extended the negotiations of the protocol to December 2020.[93]

As of now, the Additional Protocol focuses on five major provisions: the language of request (Article 1), videoconferencing (Article 2), emergency mutual legal assistance (Article 3), direct disclosure of subscriber information (Article 4), giving effect to foreign orders for the expedited production of data (Article 5).[94]

[88] Cybercrime Convention Committee '(Draft) elements of an additional protocol to the Budapest Convention on Cybercrime regarding transborder access to data: Proposal prepared by the Ad-hoc Subgroup on Transborder Access and Jurisdiction available at https://rm.coe.int/cybercrime-convention-committee-t-cy-transborder-access-to-data-and-ju/168073dc0b, accessed 10 May 2021.

[89] Cybercrime Convention Committee, 'Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY: Final report of the T-CY Cloud Evidence Group' 16 September 2016 available at http://rm.coe.int/16806s495e, accessed 27 October 2020.

[90] Ibid para 45.

[91] Ibid.

[92] Cybercrime Convention Committee 'Terms of Reference for the Preparation of a Draft 2nd Additional Protocol to the Budapest Convention on Cybercrime' Strasbourg, 9 June 2017 available at http://rm.coe.int/terms-ofreference-for-the-preparation-of-a-draft-2nd-additional-proto/168072362b, accessed 27 October 2020.

[93] Available at http://rm.coe.int/summary-towards-a-protocol-to-the-budapest-convention/1680972d07, accessed 11 November 2020.

[94] Provisional Text of Provisions, Preparation of a 2nd Additional Protocol to the Budapest Convention on Cybercrime, Cybercrime Convention Committee (T-CY), Council of Europe (1 October 2019) available at http://rm.coe.int/provisional-text-of-provisions-2nd-protocol-/168097fe64, accessed 11 November 2020.

2.3.2 Cloud computing

The advent of cloud computing is one of the main challenges for the Cybercrime Convention. At that time, the Cybercrime Convention was being drafted; the drafters did not envisage cloud computing possibilities. Cloud computing is 'a way of delivering computing resources as a utility service via a network, typically the Internet, scalable up and down according to user requirements'.[95] There are different types of cloud computing, but this study will only be restricted to, Software-as-a-Service (SaaS) because this is where most of the cyberattacks occur. According to the National Institute of Standards Technology definition, SaaS provides the consumer with:

> [t]he capability…to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser, or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.[96]

Examples of SaaS include webmail services such as Gmail and Hotmail and storage services such as iCloud and Dropbox. These services' unique nature is that the data is not stored on one device but can be accessed from all mobile devices with internet access such as laptops, tablets, and smartphones. The data in a cloud can be stored and moved around in different servers in different jurisdictions,[97] which raises the question of which jurisdiction the data falls. It is complicated for an internet user to tell where the exact data is being stored when accessing the cloud data.[98] Even where the server's location on which the data is stored is known, it might still not be clear which state may exercise exclusive jurisdiction. It may be argued that the location of

---

[95] W Kuan Hon & C Millard 'Cloud technologies and services' in C Millard (ed) *Cloud Computing Law* (2013), 3.
[96] P Mell & T Grance *The NIST Definition of Cloud Computing* (2011).
[97] Cybercrime Convention Committee 'Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY: Final report of the T-CY Cloud Evidence Group 16 September 2016 available at http://rm.coe.int/16806a495e, accessed on 27 October 2020.
[98] J Spoenle 'Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal?' (Council of Europe, Strasbourg, 31 August 2010) 4-5.

the headquarters of the service provider, or of its subsidiary, or the location of the data and server, or the law of the State where the suspect has subscribed to a service or the location or citizenship of the suspect may determine jurisdiction.'[99]

Unlike data stored on a computer, data stored via cloud computing presents challenges in the transborder access to stored computer data. In instances where the location of the data is unknown, the implication is that a state requesting mutual legal assistance in accordance with Article 31 of the Cybercrime Convention will amount to an effort in futility. It is also pertinent to note that time is essential when requesting mutual legal assistance as the data is being moved around servers, thus being moved between many different countries. By the time the mutual legal assistance request is answered, the data may have already moved to a server in another country.

2.3.3 Data protection laws

The right to protect personal data forms part of the right to privacy and is enshrined in Article 12 of the Universal Declaration of Human Rights,[100] Article 8 of the CoE's European Convention on Human Rights,[101] and Article 8 of the European Union Charter of Fundamental Rights.[102] The General Data Protection Regulation (GDPR) is the primary regulation in Europe governing data protection.[103] The GDPR is only applicable to member states of the European Union; thus, not all state parties to the Cybercrime Convention are subjected to their provisions.

European Union data protection laws are said to have an extraterritorial effect.[104] An example of the extraterritorial effect is where non-European union states have adapted their data protection law to ensure adequate protection compared to the European

[99] Cybercrime Convention Committee 'Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY: Final report of the T-CY Cloud Evidence Group' (16 September 2016) https://rm.coe.int/16806a495e, accessed on 8 February 2018, 5.

[100] (adopted 10 December 1948) UNGA Res 217 (III).

[101] Council of Europe, European Convention on Human Rights, CETS No. 005, 1950.

[102] Charter of Fundamental Rights of the European Union, OJ C/2007 C 303/1.

[103] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

[104] C Kuner, 'Extraterritoriality and regulation of international data transfers in EU data protection law' (2015) 5 *International Data Privacy Law* 235.

Union's data protection laws.[105] Law enforcement in the European Union member states can only transfer personal data in criminal investigations to a non-European Union member state based on the derogations listed in the applicable European Union legislation.[106]

Non-European Union data protection laws can make mutual legal assistance procedures and transborder access under Article 32(b) of the Convention problematic, especially in cases where evidence comprises partially of personal data.

In 2013, the EU's advisory organ on data protection sent an open letter to the Director-General of Human Rights and Rule of Law of the CoE's Data Protection and Cybercrime Division and the President of the Convention's Committee. The letter addressed the clashes between EU data protection laws and the transborder access to stored data regime of Article 32(b) of the Cybercrime Convention.[107] Article 29 of the Data Protection Working Party notes that personal data can only be disclosed where the data subject's consent is given freely. Private entities might be allowed to disclose personal data in a police or criminal investigation.[108] However, under EU data protection laws, the private sector can only disclose personal data if the data is necessary and proportionate to the purpose pursued, that is, upon initial presentation of a warrant or any document justifying the need to access the data in accordance with the requested Party's law.[109] Article 29 of the Data Protection Working Party states that 'direct access to personal data by law enforcement authorities of third party countries is not compatible with the data controllers' obligations according to Directive 95/46/EC.'[110]

---

[105] Article 45 of the GDRP.
[106] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89, Articles 35-38.
[107] Article 29 Data Protection Working Party 'Subject: Article 29 Working Party's comments on the issue of direct access by third countries' law enforcement authorities to data stored in other jurisdiction, as proposed in the draft elements for an additional protocol to the Budapest Convention on Cybercrime' (5 December 2013) Ref. A Res (2013) 3645289 – 05-12-2013.
[108] Ibid at 2-3.
[109] Ibid at 4.
[110] Ibid.

As shown above, the Cybercrime Convention sets a normative standard within the international legal framework, acknowledging the need to pursue a criminal policy and procedural law in relation to cybercrime. However, the Cybercrime Convention's enforcement is limited, based on the challenges discussed in the previous paragraphs. Case law demonstrates a trend on issues arising from the Cybercrime Convention, especially on the challenges to its implementation. For instance, in the case of *Ahmet Yildrim v Turkey*[111] the European Court of Human Rights held that Turkey violated Article 10 of the European Convention on Human Rights when it blocked access to all Google sites because of one Internet site facing criminal proceedings for insulting the memory of a former Turkish president. The court wrote that the right to freedom of expression is two-fold, encompassing not only the right to transmit but also to receive information, and that although Article 10 does not afford absolute protection against prior restraint, restrictions on freedom of expression do require strict judicial scrutiny.

At this juncture, another issue to consider is whether the African Union Convention on Cyber Security and Personal Data Protection provides a broader framework to facilitate mutual assistance and international cooperation, which will be discussed in the next section.

2.4 The African Union Convention on Cyber Security and Personal Data Protection

The African Union Convention on Cyber Security and Personal Data Protection was drafted in 2011 and adopted in July 2014. The Convention[112] aims to harmonise the laws of African States on electronic-commerce, data protection, cybersecurity promotion, and cybercrime control. As of 23 June 2020, the Convention has been signed by 14 member states and ratified by 5 member states.[113] The Convention recognises that cybercrime 'constitutes a real threat to the security of computer networks and the development of the Information Society in Africa'.[114] Furthermore,

[111] *Ahmet Yildirim v Turkey* (Application No. 3111/10) 18 December 2012.
[112] See African Union (AU) Convention on Cyber Security and Personal Data Protection EX.CL/846(XXV).
[113] See list of African Union Convention on Cybersecurity and Personal Data Protection available at http://au.int/en/treaties/african-union, accessed 7 October 2020.
[114] See Preamble to the AU Convention on Cyber Security

the Convention adopts a holistic approach to cybersecurity governance by imposing obligations on member states to establish and implement national laws, policies, and institutional governance mechanisms on cybersecurity.[115] Article 28 of the AU Convention on Cyber Security and Personal Data Protection urges AU member states to use existing international cooperation channels (including intergovernmental or regional or private and public partnerships arrangements) to promote cybersecurity and tackle cyber threats.[116] The Convention emphasises the need for States to adopt the principle of dual criminality[117] when rendering cross-border assistance on cybersecurity issues. The AU Convention on Cyber Security and Personal Data Protection aims to do so without member states having to fulfil extradition and mutual assistance requests in the absence of an extradition treaty based on dual criminality. Article 28(1) of the Convention provides that: 'State parties shall ensure that the legislative measures and/or regulations adopted to fight against cybercrime will strengthen the possibility of regional harmonisation of these measures and respect the principle of double criminal liability'.[118] The application of the dual criminality principle also emphasised in Article 28(2) of the Convention, which provides that:

> State parties that do not have agreements on mutual assistance in cybercrimes shall undertake to encourage the signing of agreements on mutual legal assistance in conformity with the principle of double criminality liability, while promoting the exchange of information as well as the efficient sharing of data between the organizations of State Parties on a bilateral and multilateral basis.[119]

---

[115] U J Orji 'Examining Missing Cybersecurity Governance Mechanism in African Union Convention on Cybersecurity and Personal Data Protection', (2014) 5 *Computer Law Review International* 131-132.

[116] Article 28(4) AU Convention on Cyber Security.

[117] 'Dual criminality' exists where a conduct in issue have been criminalised in the laws of both the State requesting for assistance or extradition and the State from whom such assistance or extradition is requested. Under this principle, an extradition request can only be granted in accordance with an extradition treaty between two countries where both countries have criminalized the criminal conduct for which an extradition request is sought. See *ITU Global Cyber-Security Agenda (GCA) High Level Experts Group [HLEG] Global Strategic Report* (2008) 14 and 56.

[118] Article 28(1) of the AU Convention on Cyber Security.

[119] Ibid.

Orji[120] writes that the Convention on Cyber Security and Personal Data Protection appears to establish a requirement for applying the double criminality principle between member states when rendering cross-border assistance on cybersecurity issues. He further argues that the AU Convention made no legal basis for extradition proceedings in the absence of a treaty on extradition. Thus, an extradition request may not be successful between the two member states to the Convention even where the requirements of the principle of dual criminality have been fulfilled.[121]

Thus, a member state that does not have an extradition treaty with another AU Member State may technically provide a safe haven for cybercriminals since an extradition request cannot be successfully made to such Member State from another Member State. The position is quite different under the Council of Europe Convention on Cybercrime, which establishes very elaborate procedures to facilitate international cooperation amongst member states. Article 24(1) of the Council of Europe Convention on Cybercrime provides that extradition arrangements between member states shall be based on the principles of 'dual criminality'. Member states are, however, allowed to adopt the Convention as a legal basis for extradition proceedings in the absence of a treaty on extradition. It is arguable that these provisions create forum shopping opportunities for cybercriminals within Africa. The position is quite different under the Council of Europe Convention on Cybercrime, which establishes very elaborate procedures to facilitate international cooperation amongst member states. Article 24(1) of the Council of Europe Convention on Cybercrime provides that extradition arrangements between member states shall be based on the principles of "dual criminality". Member states are, however, allowed to adopt the Convention as a legal basis for extradition proceedings in the absence of a treaty on extradition. This aims to recognise that extradition treaties may not exist between all member states to the Convention. Thus, the African Union Convention can learn or implement the provisions of the Council of Europe on Cybercrime in this regard.

In addition to this, the AU Convention does not create a regional Computer Emergency Team (CERT) to further facilitate cybersecurity efforts and coordinate responses to

[120] Orji op cit note 48 at 108.
[121] Ibid.

cybersecurity incidents at a regional level. Instead, Article 28(3) of the Convention imposes obligations on member states to 'encourage the establishment of institutions that exchange information on cyber threats and vulnerability assessment such as the CERT or the Computer Security Incident Response Teams (CSIRTs)'.[122] However, the need to establish a CERT and CSIRT is essential. Its absence may result in poor coordination of Africa's cybersecurity efforts and responses to cyber threats at a regional level.[123]

In light of the above, the AU Convention on Cyber Security and Personal Data Protection does not provide an adequate international cooperation framework amongst the African States. The Convention emphasises the use of existing channels of cooperation or bilateral agreements where there are no multilateral agreements between AU Member State.

It is pertinent to note at this point that Uganda has not signed nor ratified the Convention. This research has discussed some of the conventions' limitations; another issue for consideration is whether the ratification of the Convention would provide Uganda with the necessary guidance to implement these laws. This will be considered in the following chapter.

2.5 Conclusion

In summary, while not all international and regional agreements are covered in this chapter, some of the most significant regional agreements regarding cybercrime have been examined. These agreements acknowledge the transnational nature of cybercrimes and the need for global cooperation to tackle the problem; however, each exhibits limitations in their efforts towards cybercrime control.

As shown above, the Council of Europe Convention on Cybercrime remains the most comprehensive international instrument in this area. It is accompanied by a range of regional and national initiatives. The Cybercrime Convention remains an essential

[122] Article 28(3) of the African Union Convention on Cyber Security and Personal Data Protection.
[123] Orji op cit note 48 at 115.

framework against which national efforts may be measured.[124] The following chapter will provide a collective analysis of the computer-related offences under the various Uganda statutes, to determine whether it conforms to the Cybercrime Convention.

[124] J Clough 'A world of difference: The Budapest Convention on Cybercrime and the challenges of harmonisation' (2014) 40 *Monash University law review* 698.

CHAPTER THREE: COMPUTER-RELATED OFFENCES IN UGANDAN STATUTES

3.1 Introduction

In the previous chapter, emphasis was given to the legal provisions enshrined in the Cybercrime Convention to combat cybercrime. However, since the Council of Europe Convention on Cybercrime contains detailed and comprehensive descriptions of and guidelines about cyber offences and had a significant impact on the state's law-making, it is used as a comparative sample and as a criterion for evaluating the computer-related offences under the various Ugandan statutes. This will aid in understanding the existing gap between the legal provisions and computer-related crimes in Uganda. For purposes of this research, these computer-related offences will be analysed under four headings: offences against the state; offences against the confidentiality, integrity, and availability of computer data and system; offences against the individual; and other related offences.

3.2 Offences against the State

The growth of internet technology has ushered in a new era of cybercriminal activities where potential attacks can be launched against national security, economic security, public health, safety, or any combination of those matters, which could be deemed as offences against the state.[125] Before the enactment of the CMA, treasonable offences were punishable under the Penal Code Act. Section 23(1)(a) of the Penal Code Act states that: 'any person who levies war against the Republic of Uganda State is guilty of treason and is liable to the punishment of death'.[126] To further buttress this, Onyeozil[127] argues that levying of war does not mean that to further buttress this, Onyeozil[128] argues that levying of war does not mean that the accused person/s must be members of the military force or even trained in using arms, and the weapons used to wage war is immaterial. Therefore, an attack against the infrastructures of the State,

[125] O Pollicino 'The new relationship between national and the European Courts after the enlargement of Europe: Towards a unitary theory of jurisprudential supranational law?' (2010) 29 *Yearbook of European Law* 65-111.
[126] Section 23(1)(a) of the Penal Code Act 120 of 1950.
[127] E C Onyeozili 'Obstacles to effective policing in Nigeria' (2005) 1 *African Journal of Criminology and Justice Studies* 32-54.
[128] Ibid at 32-54.

can be considered treasonable offences. In *Hofni Topacho Ongiretho v Uganda*[129] it was held that an overt act is an intention to affect any purpose which can be called an element of the offence, every act in furtherance of the commission of the offence, or every act of conspiring with any person to effect that purpose and every act done in furtherance of the purpose by any persons conspiring, shall be deemed to be an overt act manifesting the intention. These offences will be discussed under two subheadings; namely, offences against critical national infrastructure and offences related to Cyber Terrorism.

3.2.1 Offences against the Critical National Infrastructure

The Government of Uganda has been channelling a lot of resources in capacity building for e-Governance. For example, with the Chinese government's support, the Government of Uganda embarked on laying the National Data Transmission Backbone Infrastructure (a fibre optic cable network).[130] Today, different sectors of the Ugandan economy are heavily dependent on information and computer technology because of its contribution to the economy's growth. Therefore, it becomes imperative to protect these sectors from cyber threats.[131] The concept of Critical Infrastructure encompasses:

> Energy (including oil, natural gas, and electric power); banking and finance; transportation (including air, surface, and water transportation); information and communications technology networks; water systems; and government and private emergency services.[132]

Cyberattacks on infrastructure include disrupting power grids, halting trains, and grounding aircraft.[133] The significant increase in these attacks and the exposure of

---

[129] *Hofni Topacho Ongiretho v Uganda* (Criminal Appeal – 1993/1) (1994) UGSC 9 (03 March 1994).
[130] Business Vision Huawei delivers Uganda fibre internet backbone. *The New Vision* available at http://www.newvision.co.ug/newa/18322-huawei-delivers-uganda-fiber-internet-backbone.html, accessed 18 September 2020.
[131] United States The White House, National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, Washington, DC 2003, 6, 47-79 available at http://www.whitehouse.gov/pcipb/physical.html, accessed on 7 June 2020.
[132] T Stevens *Cyber Security and the Politics of Time* (2016) 163.
[133] Ibid.

these infrastructural networks has propelled governments to recognise the seriousness of the issue, resulting in a push for increasing mandated cybersecurity covering both government and private networks; and enacting specific legislation to protect them.[134]

The CMA is silent on what amounts to 'key public infrastructure'. Such *lacuna* creates an ambiguity in the law and is likely to be used by cybercriminals in perpetrating more cyberattacks. The Anti-Terrorism Act, 2002 deals with some of the deficiencies, at least as far as 'key public infrastructure' is concerned. The Anti-Terrorism Act defines a state or government facility as:

> Any permanent or temporary facility, and conveyance used or occupied by state representatives, government officials, the members of parliament, the judiciary, and employees of a public authority.[135]

This dissertation argues that the definitional approach taken by the Anti-Terrorism Act, did not specifically designate the area of the national computers, computer systems, and networks as part of the critical national infrastructure. Although Section 14(1) of the CMA criminalises unauthorised modification of computer material; this section provides that the requisite intent for this offence as:

> Intent to cause a modification of the contents of any computer and in so doing impairs the operation of any computer or computer programme, hinder access to any programme, and data held in any computer.[136]

However, CMA seems to have also left this at the discretion of the courts for interpretation. Although it is arguable that any interference with public infrastructure, as defined in section 14 of the CMA, is considered unauthorised modification, which is a criminal offence.

---

[134] J A Lewis Assessing the risks of cyber terrorism, cyber war and other threats. (Centre for Strategic & International Studies, 2002) available at http://csis.org/files/media/csis/pubs/021101_risks-of_cyberterror.pdf, accessed on 7 June 2020.
[135] Section 2 of the Anti-Terrorism Act of 2002.
[136] Section 14(1) of the CMA.

3.2.2 Offences Related to Cyber Terrorism

The advancement in internet technology has brought about significant changes in global terrorism.[137] Today it is known that terrorists use ICTs and the Internet for propaganda; information; gathering; preparation of real-world attacks; publication of training materials; communication; terrorist financing; and attacks against critical infrastructures.[138] This shift in the activities of terrorists via the Internet has had a positive effect on terrorism, as it highlights areas of terrorist activities that were unknown before. Before one can discuss Cyber terrorism, it is essential to understand the concept of terrorism. These terms have frequently been used interchangeably, despite their evident differences. The International Convention for the Suppression of the Financing of Terrorism 1999 defines terrorism as:

> any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organisation to do or abstain from doing any act.[139]

The above definition has been implemented into Uganda's Anti-Terrorism Act, 2002 (as amended) (ATA). Section 7(1) of the ATA states:

> A person commits an act of terrorism who –
>
> a. Carries out or perpetrates any act, whether occurring in Uganda or elsewhere, that constitutes a crime in accordance with agreements, protocols and treaties described in the annex to the International Convention for the Suppression of the Financing of Terrorism, 1999 or;

[137] International Telecommunication Union Cybercrime Legislation Resources *Understanding cybercrime: A guide for developing countries* (2009) 48.
[138] W Dunlevy 'Intelligence analysis for internet security' Carnegie Mellon Software Engineering Institute, and CERT Coordination Centre (2005).
[139] International Convention for the Suppression of the Financing of Terrorism, 1999 available at http://www.un.org/law/cod/finterr.htm, accessed 18 September 2020.

b. travels outside Uganda for the purpose of the perpetration, planning, or preparation of, or participation in terrorist acts or the providing or receiving of terrorist training.[140]

On the other hand, the term 'Cyber terrorism' is a term that lacks a universally accepted definition. Some scholars have used the term to illustrate criminal acts like stealing data and hacking into a computer system,[141] planning terrorist attacks,[142] causing violence,[143] or an attack on information systems.[144] Other scholars have used the term 'Cyber terrorism' to denote actions such as data theft, hacking, and attacks on information systems.[145]

Although the CMA provides for the classifications of computer systems and networks that form part of the critical national infrastructure, the CMA does not make provision for cyber terrorism offences.

3.3 Offences against confidentiality, integrity and availability of computer data and system

This section will analyse cybercrime offences against the confidentiality, integrity, and availability of computer data and systems found in Uganda's national legislation. Provisions within Uganda's national legislation intends to protect the confidentiality, integrity, and availability of computer systems or data. The offences created in these pieces of legislation can be described as the fulcrum of computer-related offences. They form the basis upon which other additional cyber offences are committed.[146] The ability to access information contained in computer systems regardless of

---

[140] Section 7(1)(a)(b) of the Anti-Terrorism Act of 2002.
[141] A Embar-Seddon 'Cyberterrorism: are we under siege?' (2002) 45 *American Behavioural Scientist* 1033-1044.
[142] K C Desuoza & T Hensgen 'Semiotic emergent framework to address the reality of cyberterrorism' (2003) 70 Technological Forecasting and Social Change at 385-396.
[143] M M Pollitt 'Cyberterrorism – fact or fancy?' in E V Linden (ed) *Focus on Terrorism* (2001) 69.
[144] D Denning 'Statement of Dorothy E. Denning before the United State Congress's House Armed Service Committee' (2000) available at http://www.house.gov/hasc/testimony/106thcongress/00-05-23denning.htm, accessed on 7 June 2020.
[145] M Chawki, A Darwish, A M Khan & S Tyagi *Cybercrime, Digital Forensic and Jurisdiction* (2015) 39.
[146] I Walden *Computer Crimes and Digital Investigation* 3 ed (2007) 250.

geographical distances has led to the rapid growth in the amount of information available. Gregor[147] contends that the user's connectivity to these sophisticated computer systems and networks may be the subject of misuse by offenders who commit cybercrime offences against users who use a computer system or networks for legitimate purposes. This section will analyse the following offences: unlawful access, unauthorised interception, unlawful data interference, and misuse of devices.

3.3.1 Unlawful access to computer and information systems

Unlawful access occurs when a user gains illicit access to a computer network without the owner's authorisation.[148] Access could be as simple as the attacker gaining control of a computer system.[149] The object of most unauthorised access incidents is to gain 'root'[150] control over a system, thereby granting the attacker unhindered access to the computer or network and all of its content. With 'root' access, the attacker has the same privileges as an administrator of the system and may add, modify, delete, or copy at will.

Section 15(1) of the CMA prohibits unauthorised access to computer materials and states that a person will be guilty of an offence where he/she causes a computer to perform any function to gain access to any program or data held in any computer without the requisite authorisation to do so. For this offence to be established, it only needs to be proven that the offender did not have the required authorisation to access the said information. Section 9 of the CMA stipulates the punishment for the offence of unauthorised access to computer material would be six months imprisonment.

---

[147] G Urbas & T Krone 'Mobile and Wireless Technologies: Security and Risk Factors' (2006) *Australian Institute of Criminology*, available at http://www.aic.gov.au/publications/tandi2/tandi329t.html, accessed 18 September 2020.

[148] N A Biegel 'Modern stalking laws: A survey of state anti-stalking statutes considering modern mediums and constitutional challenges' (2001) 14 *Chapman Law Review* at 20.

[149] C Barry 'The Future of Cyber Terrorism, Crime and Justice International' (1997) 13 *Crime and Justice International Journal* 20 and 24.

[150] Root access grants the user administrator privileges allowing full access to the systems files and the ability to change settings on other users or delete and moderate their profiles. In UNIX based systems the user with root privileges is called 'root' while in Windows based system the user is called 'administrator'.

3.3.2 Unauthorised interception

The Council of Europe Convention on Cybercrime recognises the destructive nature of unauthorised interception and requires member states to enact legislation that prohibits all forms of unlawful electronic data transfer, whether by telephone, email, or file transfer, without the consent of the authorised owner. This provision aims to prevent the violation of the right to privacy, where data communication is concerned, and its transmission to a network.[151] Although Uganda is not a signatory to the Council of Europe Convention on Cybercrime, this provision has now been implemented in Uganda's CMA in section 15(1)(b), which criminalises the:

> unauthorised interception and unlawful aiding of interception directly or indirectly of a computer or computer network by means of an electro-magnetic, acoustic, mechanical or other device irrespective of similarity.[152]

Noticeably, the CMA clearly defines unlawful interception as 'non-public' transmission of computer data. By implication, this limits the object of the offence to 'private' transmission.[153] The effect of this is that it is likely to result in attacks on private users more than those that work in public institutions.

3.3.3 Misuse of devices

Article 6 of the Council of Europe Convention on Cybercrime establishes offences relating to the misuse of devices to gain illegal access or interception or committing data and system interference. It criminalises offences like the intentional production, selling, import, or distribution of devices to interfere with the computer system.[154] It should be noted that section 12(1) of the CMA, which criminalises offences such as intentional production, sale, import, or distribution of devices to interfere with the

---

[151] S M Bellovin, M Blaze, S Clark & S Landau 'Security implications of applying the communications assistance to Law Enforcement Act to voice over IP' (2006). Available at http://www.itaa.org/news/docs/CALEAVOIPreport.pdf, accessed on 7 June 2020.
[152] Section 15 (1) (b) of the CMA.
[153] Development of surveillance technology and risk of abuse of economic information, 2.4 available at http://cryptome.org/stoa-r3-5.htm, accessed on 7 June 2020.
[154] Information Security: Computer Controls over Key Treasury Internet Payment System, GAO-03-837 (U.S. Government Printing Office, 2003).

system aligns with Article 6 of the Council of Europe Convention on Cybercrime. According to section 12(1) of the CMA:

> A person who unlawfully produces, sells, offers to sell, procures for use, designs, adapts for use, distributes or possesses a device, a computer programme or a component designed primarily to overcome security measures for the protection of data, and performs any of those acts with regard to a passcode or related type of data commits an offence.[155]

Section 12(3) of the CMA also prohibits the misuse of a computer or computer programmes aimed at destroying computer security components, as well as hindering access to computer data and systems.

3.3.4 Unlawful interference

The CMA describes an information system as a system used for generating, sending, receiving, storing, displaying, and processing data messages.[156] It also establishes a category of criminal activity that involves intentional damaging, deletion, alteration, destruction, and suppression of data.[157] This enactment aims to protect sensitive computer data and programmes from being exposed to potential perpetrators. Section 12(5) of the CMA provides that:

> A person who accesses an information system to constitute a denial of service to legitimate users, whether fully or partially, commits an offence.[158]

The requisite *mens rea* needed to prove the offence is that there was interference with the computer system, irrespective of whether the offence is directed at a particular programme or data within a specific computer.[159]

---

[155] Section 12(1) of the CMA.
[156] Section 2 of the CMA.
[157] Section 9 of the CMA.
[158] Section 12 (5) of the CMA.
[159] R Power 'CSI/FBI Computer Crime and Security Survey' (2002) 17 *Computer Security Journal* 2-29.

3.4 Offences against the individual

Traditionally an offence against the individual is a crime that is committed where direct physical harm or force is applied to another person.[160] The CMA contains variant provisions on cybercrime offences against the individual and includes any harm that the offence intended to cause or might have foreseeably caused.

In the paragraphs below, this research will analyse the following categories of cyber offences and xenophobic offences, and cyberstalking offences.

3.4.1 Offences related to child pornography

The growth of internet technology has enlarged the avenue that offenders use to access, create or distribute child pornography across Social Networking Sites (SNSs).[161] SNSs are one of the most remarkable technological phenomena of the 21st century.[162] These SNSs mostly have private meeting rooms which make monitoring of paedophilic activities difficult.[163] The popularity of these SNSs has increased over the past five years, attracting a large number of users, of which significant proportions are teenagers.[164] In Uganda, the protection of children from pornography is mandated by the constitution. Citizens have a duty to protect children from any form of abuse, harassment, or ill-treatment.[165] The United Nations Optional Protocol on Child Pornography,[166] to which Uganda is a party, requires states to take all necessary steps to strengthen international cooperation in the prevention, detection, investigation, prosecution, and punishment of those responsible for acts involving child pornography.[167]

---

[160] R Card *Criminal Law* 21 ed (2014) 2.
[161] M McGuire *Hypercrime: The New Geometry of Harm* (2007).
[162] M Chawki & Y el Shazly 'Online sexual harassment: Issues and solutions' (2013) 4 *JIPITEC* 2.
[163] Ibid.
[164] See ENISA Position Paper No.1 'Security Issues and Recommendations for Online Social Network' 2007 available at http://www.enisa.europa.eu, accessed 2 December 2020.
[165] Article 17(1)(c) of the Constitution of the Republic of Uganda 1995.
[166] Uganda acceded to the United Nations' Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography 2002 on 30 November 2001 available at http://indicators.ohchr.org, accessed 27 October 2020.
[167] Article 10(1) of the United Nations Optional Protocol to the Convention on the Rights of the Child on the State of Children, Child Prostitution and Child Pornography 2002.

Section 23(3) of the CMA defines child pornography as including pornographic material that depicts a child, a person appearing to be a child, and realistic images representing children engaged in sexually suggestive or explicit conduct. The Anti-Pornography Act, 2014 (APA), which was passed after CMA defines child pornography as any representation through publication, exhibition, cinematography, indecent show, information technology or by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child primarily for sexual enjoyment.[168]

Section 23(1)(a) to (e) of the CMA prohibits child pornography by imposing a fine of 7,200 000 Uganda shillings and or imprisonment for 15 years. The provision was restricted to child pornography to provide continuous protection to children, even if the laws against adult pornography were ever to be relaxed.[169]

This provision in the CMA compliments a number of other obscenity laws in the country, such as the Anti-Pornography Act, 2014. Section 14(1) of the APA criminalises acts of child pornography; it provides that:

> A Person shall not produce, traffic in, publish, broadcast, procure, import, export, sell or abet any form of pornography.[170]

The Anti-Pornography Act provides a fine not exceeding Ugandan shilling 750,000 or imprisonment not exceeding 15 years or both as the punishment for the said offence. Section 3 of the Prevention of Trafficking in Person Act[171] provides that anyone who recruits a person in pornography commits an offence.[172]

[168] Sections 14(2) and 2 of the Anti-Pornography Act 2014.
[169] Parliament Hansard Tuesday, 29 June 2010. At the time Act was passed, adult pornography was and still is illegal in Uganda.
[170] Section 14(1) of the Anti-Pornography Act of 2014.
[171] Prevention of Trafficking in Persons Act 7 of 2009.
[172] Section 3(4) of the Prevention of Trafficking in Persons Act 7 of 2009.

3.4.2 Identity theft offences

Identity theft has grown to be a significant problem for the global economy.[173] Uganda recorded an enormous loss of 610,000,000 Ugandan shillings in 2019 due to identity crimes.[174] The dynamic nature of these offences has contributed to the lack of uniformity in their definition. Terms such as 'identity crime,' 'identity fraud,' and 'identity theft' are often used interchangeably.[175] However, there are usually two aspects involved in this type of offence: theft and fraud.[176]

The term identity theft describes the criminal act of fraudulently obtaining and using another person's identity.[177] A person could be found liable where the person falsely makes representation intending to cause loss to another to make a material gain or to expose another to the risk of loss.[178] An example of this offence is phishing, where a person attempts to use electronic communication such as emails, text messages, or Facebook to acquire information such as usernames, passwords, and credit card details by presenting themselves as an honest service provider.

Identity fraud occurs when the offender uses the stolen identity to commit further criminal activities to obtain goods or services by deception.[179] A person could be liable for the commission of offence where the person uses their victim's stolen identity details to open bank accounts, obtain credit card loans;[180] order goods in the victims' names, and take over their victims' existing accounts.[181] 'Online impersonation' is an example of impersonation enhanced by technology. This can be described as creating

---

[173] CIFAS identity fraud report is available at https://www.cifas.org.uk/identity_fraud accessed on the 8 June 2020.
[174] Available at http://www.independent.co.ug accessed on 9 June 2020.
[175] K M Finklea *Identity theft: Trends and issues* (2010) 2.
[176] European Commission Directorate-General, Joint Research Centre. Available at http://primeproject.eu/community/furtherreading/studies/IDTheftFIN.pdf, accessed on 8 June 2020.
[177] A N Ayofe 'Towards ameliorating cybercrime and cybersecurity' (2009) 3 *International Journal of Computer Science and Information Security* 1-11.
[178] J Scannell 'The 419 scam: An unacceptable power of the false?' (2014) 11 *PORTAL Journal of Multidisciplinary International Studies* 11.
[179] A brief study of the EU, the UK, France, Germany and the Netherlands' (2006) Perpetuity Research & Consultancy International, Leicester.
[180] V Lynne, H Copes & I Birch 'Identity theft' (204) In *Encyclopaedia of Criminology and Criminal Justice* 2419-2429.
[181] S Byers 'Internet: Privacy Lost, Identities Stolen' (2001) 40 *The Brandeis LJ* 141.

a web page, a social media network, sending an email or an instant message on the internet using the name or any other personal data of another person with the intent to harm, defraud, intimidate or threaten another person or persons.[182]

However, a more deceptive form of identity 'theft' involves 'botnets'. In this case, internet protocols (IP) have been infected by remote administration tools (malware).[183] Botnets have increased the power of cybercrime perpetrators. They have transformed the operational nature of criminal activities in cyberspace by increasing the number of computers infected by malicious software or viruses.[184] Based on the above, the CMA provisions are unclear concerning the problems associated with identity theft and impersonation.

3.4.3 Cyberstalking offences

The Council of Europe Convention on Prevention and Combating Violence Against Women and Domestic Violence (Istanbul Convention)[185], defines stalking as 'repeatedly engaging in threatening conduct directed at another person, causing her or him to fear for his or her safety'.[186] Goodno[187] contends that cyberstalking is synonymous with traditional offline stalking because of the similarities in content and intent. This research does not subscribe to these opinions that seek to combine cyberstalking with offline stalking.[188] Although there are similarities between the two, such as the desire to exert control over the victim, and, much like offline stalking, cyberstalking involves 'the repeated use of the internet, email, or related digital electronic communication devices to annoy, alarm, or threaten a specific individual or

[182] Ibid.
[183] V Jignesh, A Meniya & HB Jethva 'A review on botnet and detection technique' (2003) 4 *International Journal of Computer Trends and Technology* 23-29.
[184] Ibid.
[185] Available at http://www.coe.int/t/dghl/standardsetting/convention-violence/thematic_factsheets/Stalking_EN.pdf, accessed on 9 June 2020.
[186] Article 34 of the Council of Europe Convention.
[187] N Goodno 'Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws' (2007) 12 *Missouri Law Review* available at http://scholarship.law.missouri.edu/cgi/viewcontent.cgi?article=3985&context=mlr, accessed on 9 June 2020.
[188] R A Bonanno & S Hymel 'Cyber bullying and internalizing difficulties: Above and beyond the impact of tradition forms of bullying' (2013) 45 *Journal of Youth and Adolescence* 685-697.

group of individuals'.[189] While trying to describe offline stalking, Pittaro[190] contends that 'in offline stalking, although the offender may harass the victim by repeatedly telephoning him/her, every telephone call is a single event that requires the stalker's action and time, and involves only the victim and offender'. This differs in cyberstalking cases where the involvement of blogs, websites, and social network sites such as Facebook, Twitter, and LinkedIn have complicated issues surrounding cyberstalking.[191] Cyberstalking takes on many forms, such as defamation or libel, falsification, fraud, intimidation, offensive comments, personal attacks, graphic violence, and privacy rights violations.[192] However, there are numerous acts associated with cyberstalking. Such acts include threats, false accusations, insults, network attacks, unlawful spying, impersonation, and online harassment.

Section 24 of the CMA criminalises cyber harassment. The punishment for cyber harassment is a fine of 1,440,000 Uganda shillings or imprisonment not exceeding three years or both. Section 25 of the CMA regards offensive communications as a misdemeanour; an accused is liable to a fine not exceeding 480,000 Uganda shillings or imprisonment not exceeding one year or both. Section 26 of the CMA criminalises cyberstalking. The crime attracts a punishment of 2,400,000 Uganda shillings or imprisonment not exceeding five years or both. The Ugandan cases of *Uganda v Stella Nyanzi*;[193] *Uganda v Nsubuga*;[194] *Hesse v Senyonga;*[195] *Uganda v Ssentongo*;[196] and *Uganda v Sserunkuma*[197] reveal that the defendants were charged under the CMA provisions on cyber harassment and offensive communication.

[189] D Robert & J Doyle 'Study on cyberstalking: Understanding investigative hurdles' (2003) 72 *FBI Law Enforcement Bulletin* 10-17.
[190] M L Pittaro 'Cyber stalking: An analysis of online harassment and intimidation' (2007) 2 *International Journal of Cyber Criminology* 180-197.
[191] J C Merschman 'Dark side of the web: Cyberstalking and the need for contemporary legislation' (2001) 24 *The Harvard Women's LJ* 255.
[192] K Clark et al 'A Dutch approach to cybersecurity through participation' (2014) 5 *Security & Privacy, IEEE* 27.
[193] *Uganda v Stella Nyanzi* (Criminal Appeal-2019/) [2020] UGHCCRD 2 (20 February 2020).
[194] *Uganda v Nsubuga* (HCT-00-AC-SC-2012/84) [2013] UGHCACD 12 (03 April 2013).
[195] *Hesse v Senyonga* (Civil Suit-2014/612) [2015] UGCommC 90 (25 June 2015).
[196] *Uganda v Ssentongo* (Criminal Session Case-2012/123) [2017] UGHCACD 1 (14 February 2017).
[197] *Uganda v Sserunkuma* (HCT-00-CR-SC-2013/15) [2015] UGHCACD 4 (27 April 2015).

3.5 Cyberfraud and other related offences

With the reliance on computers and computer-related networks, there has been a rapid change from the phase of computer-related crimes to the recent phase of cybercrime, which occurs within cyberspace. Cyberspace is an ideal environment for the commission of several varying and modern crimes such as computer-related fraud and other related offences, like forgery.[198] New and emerging risks are therefore born with the continuing advent of these new technologies.[199] Provisions on computer-related fraud and forgery protect interests in property, financial assets, and documents' authenticity.[200] These offences are analysed under three subheadings: electronic fraud, computer-related forgery, and offences relating to intellectual property rights.

3.5.1 Electronic fraud

Electronic fraud is one of the most prevalent crimes on the internet in Uganda as it enables the offender to use automation and software tools to mask criminals' identities.[201] For instance, in the Ugandan cases of *Hesse Brian v Senyonga Patrick,*[202] *Uganda v Nsubuga*[203] and, *Uganda v Ssentongo*,[204] reveal the seriousness of the need for security of systems and electronic platforms for electronic transactions in Uganda. Section 20 of the CMA defines electronic fraud as:

> deception deliberately performed with the intention of securing an unfair or unlawful gain where part of a communication is sent through a computer

---

[198] E A Glyn 'Computer abuse: The emerging crime and the need for legislation' (1983) 12 *Fordham Urban Law Journal* 73-101.

[199] United Nations Statistical Commission, 2012. National Institute of Statistics and Geography of Mexico Report on Crime Statistics: Note by the Secretary General E/CN.3/2012/3, 6 December 2011.

[200] U Sieber 'Legal Aspects of Computer-Related Crime in the Information Society' (1998) COMCRIME Study, available at http://www.edc.uoc.gr/~panas/PATRA/sieber.pdf, accessed on 9 June 2015.

[201] PWC's Global Economic Crime and Fraud Survey 2020 available at http://pwc.com/gx/en/services/advisory/forensics/economic-crime-survey.html, accessed on 30 June 2020.

[202] Op cit note 147 at 21

[203] HCT-00-AC-SC-0084-2012[2013]UGHCCRD 13 (3 April 2013, available at http://www.ulili.org/ug/judgement/high-court-criminal-divison/2013/13-0, accessed 7 May 2021.

[204] *Ssentongo* supra note 72.

network or any other communication and another part through the action of the victim of the offence or the action is performed through a computer network or both.[205]

This act is referred to as a crime as, in most cases, a computer is the only medium, which establishes a link between the unsuspecting or gullible victims and offender/s. Furthermore, automation enables offenders to make large profits from several acts.[206] The fraud may be committed entirely within the computer network. Section 19(1) of the CMA criminalises electronic fraud.[207] The CMA imposes a fine not exceeding 360 currency points or imprisonment not exceeding 15 years or both upon a conviction for this offence.

Section 26(3) of the Electronic Transaction Act, 2011 extends the scope of electronic fraud to acts that companies often commit, such as telecommunication companies, which charge customers for unsolicited messages and calls. This offence involves a person sending messages not sanctioned by the receiver. The punishment for this offence is a fine of 152 currency points or imprisonment not exceeding five years or both.[208]

3.5.2 Computer-related forgery

Article 7 of the Council of Europe Convention on cybercrime urges member states to criminalise all forms of computer-related forgery. Computer-related forgery is the 'intentional … input, alteration, deletion, or suppression of data resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if were authentic.' It should be noted that section 12(1) of the CMA also aligns with Article 7 of the Council of Europe Convention on Cybercrime. According to section 12(1) of the CMA:

[205] Section 19 of the CMA.
[206] International Telecommunication Union Cybercrime Legislation Resources *Understanding cybercrime: A guide for developing countries* (2009).
[207] Section 19 (2) of the CMA.
[208] Section 26 (4) of the Electronic Transactions Act.

> A person who unlawfully produces, sells, offers to sell, procures for use, designs, adapts for use, distributes or possesses a device, a computer programme or a component designed primarily to overcome security measures for the protection of data, and performs any of those acts with regard to a passcode or related type of data commits an offence.[209]

Furthermore, the evolution of smartphones and computers makes it easy to manipulate electronic documents and digital information. This is attributed to the fact that digital information can be copied, resized, and easily manipulated with and efficiently passing it off as real documents.[210] However, there are no guidelines that highlight key principles for determining the reliability of electronic evidence. The Electronic Transactions Act relates electronic evidence to electronic transactions but does not give the use of electronic evidence general application.[211]

3.5.3 Offences relating to copyright and other related rights

The innovation of technology in the reproduction and dissemination of information has created a favourable tool for the infringement of intellectual property rights, particularly copyright issues. In addition, the production of fake, sub-standard, and unlicensed products has become very frequent.[212] Article 10 of the Council of Europe Convention urges member states to adopt legislative measures as may be necessary to establish the infringement of copyright as criminal offences under their domestic law.

The Ugandan Copyright and Neighbouring Rights Act, 2006 (CNRA) contains provisions prohibiting unlawful dealing with works or performances of an individual; without authorisation by the *bona fide* owner of the rights; and in excess of or contrary to the nature of the authorisation granted to a person by the entitled person.[213] Section 5(1)(e) of the CNRA identifies computer programmes, electronic data banks, and other accompanying materials as items eligible for copyright. Section 13(6) of the CNRA

[209] Section 12 (1) of the CMA.
[210] J A Redi, W Taktak & J-L Dugelay 'Digital image forensics: A Booklet for Beginners' (2011) 51 *Multimed Tools Appl* 133-162.
[211] Vastina Rukimirana Nsaza op cit note 54 at 7
[212] S M Besen & L J Raskind 'An introduction to the law and economics of intellectual property' (1991) *The Journal of Economics Perspective* 3-27.
[213] Section 47 of the CNRA.

protects the economic rights of authors of computer programmes for a period of 50 years, from the date on which the programme was made available to the public. Section 46 of the CNRA provides for the various forms of copyright infringement. The authorisation to use or alter copyright may be obtained through transfer, licensing, assignment, and any other form recognised under Uganda's laws. This authorisation ought to be express and clear.[214] This implies that unlawful usage of a person's copyrightable material through a cyber network constitutes a computer-related offence.

Further, section 47(7)(a) and (b) of the CNRA criminalises illegal removal or alteration of any electronic moral rights information. This offence extends to availing performances, copies of a sound recording, and audio-visual fixation to the public with prior knowledge by the perpetrator of its unauthorised alteration.[43]

It should be noted that the CMA makes no reference to/or draw penalties for offences such as copyright and trademark infringement. This is rather an unfortunate situation, and one would have thought the legislature ought to have used the provisions within the CMA to correct the anomalies and the obvious *lacunas* in the CNRA regarding infringements of copyright rights and related rights by means of a computer system. These are situations that call for the ratification of the Convention on Cybercrime. In particular, the infringement of intellectual property rights related to copyright is the most commonly committed offences on the Internet, causing concern to copyright holders. The reproduction and dissemination on the Internet of protected works without the authorisation of the copyright holder have become extremely normal.[215]

3.6 Conclusion

This chapter has discussed the various computer-related offences listed under the various Ugandan statutes that seek to criminalise access to any computer or any device without authorisation. In this regard it was established that the CMA fails in legislating exact offences, and other broadly drafted offences to cater for crimes using

[214] Section 46(1) of the CNRA.
[215] Besen & Raskind op cit note 91 at 3-27.

cryptocurrency. It is submitted that the CMA is not forward looking, in that it has stuck to traditional crimes.

As discussed earlier in this chapter, some elements of online behaviour may be similar to behaviour already criminalised under existing laws. For example, data theft could be compared to traditional forms of theft as this act satisfies the elements of the offence under the criminal justice system (Penal Code Act). However, the offender's anonymity ensures that sufficient differences exist to justify laws that specifically target online offences. Therefore, while existing laws may appear superficially adequate to address online offences, the differences in how these offences are committed require new laws and not just the amendment of laws already enacted. The limited literature in Uganda suggests that the existing laws are inadequate to address the threat of cybercrime. It is necessary to enact specific legislation uniting existing provisions under one piece of specific cybercrime legislation.

After reviewing the relevant legal provisions regarding cybercrime in Uganda, Uganda's laws fall short of the international standards. The writer's opinion is that they are not drafted in a manner that is effective in practice for prosecuting cybercrime. It is pertinent to note that the ever-changing nature of technology also requires that the act be drafted broadly to cater for new crimes. It will be argued in this dissertation that this analysis is justified and that the provisions of the Convention on Cybercrime[216] should be fully implemented to ensure that the growing problem is adequately addressed. The next chapter will examine the legislative responses to emerging issues and challenges in the arena of cybercrime in Uganda, to determine whether it conforms to the international standard.

[216] Council of Europe Convention on Cybercrime ETS. 185, (Budapest, 2001).

CHAPTER FOUR: LEGAL FRAMEWORKS FOR COMBATTING CYBERCRIME IN UGANDA

4.1 Introduction

Cyberlaw deals with codified rules that govern the exchange of communication and information to protect intellectual property rights, freedom of speech, and public access to information in Cyberspace.[217] In Uganda, the CMA, promulgated in 2011, regulates online offences. Before the commencement of the CMA, most of the traditional crimes such as theft, obtaining goods by false pretence, malicious injury to property, housebreaking, rape, and murder originate from the Penal Code Act. These traditional crimes deal only with physical evidence of a tangible nature relating directly to the crime. Tangible evidence simply refers to evidence that can be treated as real or capable of being touched—for instance, a gun, knife, blood, fingerprints, etc. Tangible evidence must be scientifically evaluated, and the results interpreted to be useful.[218] Scientific evaluation increases the reliability of the evidence. The Penal Code Act cannot effectively deal with cybercrimes that produce evidence of an intangible nature. Zittrain[219] argues that the advanced nature of interconnectivity between numerous forms of communication and services on the internet has altered the scope of global criminal law and criminal procedure. Many developing countries are neither adequately protected by legislation nor properly aware in the event of a Cyberattack on a national level.[220] Therefore, it is important not only for criminal laws to keep abreast of these diverse and novel criminal activities but also for criminal procedural law[221] and investigative techniques to be so compliant.[222]

---

[217] N O Umejiaku & M I Anyaegbu 'Legal framework for the enforcement of cyber law and cyber ethics in Nigeria (2016) 15 *International Journal of Computer & Technology* 1.
[218] Available at http://wwwlaw.jrank.org/pages/i656/Police-criminal-investigation, accessed 2 October 2020.
[219] J Zittrain *The future of the internet and how to stop it* (2008) 19.
[220] Ibid.
[221] Section 4.5 below will discuss the challenges in the arena of criminal procedural law in Uganda.
[222] M Gercke 'Challenges in developing a legal response to terrorist use of the internet' (2010) *Gabor IKLODY* 37, available at http://www.tmmm.tsk.tr/publication/datr/volumes/datr6.pdf#page=42, accessed on 29 July 2020.

This chapter will examine the legal and institutional framework which regulate cybercrimes in Uganda. This chapter will also examine the emerging issues and challenges in the arena of cybercrime legislation in Uganda.

4.2 Institutional framework of cybercrime in Uganda

4.2.1. Financial Intelligence Authority

Uganda's Financial Intelligence Authority (FIA), was established on 1 July 2014, following the enactment of the Anti-Money Laundering Act in November 2013. The FIA's mandate is to safeguard the Ugandan Financial system and contribute to the global fight against money laundering, terrorism financing, and related crimes through the provision of credible financial intelligence. The FIA has coordinated the National Risk Assessment exercise which assessed the money laundering and terrorist financing risks that the country faces.[223] The FIA has also signed memoranda of understanding with 15 other Financial Intelligence Units (FIUs) and 9 local authorities; and, as of November 2017, the process is underway to submit the application to join the EGMONT Group of FIUs.[224] The Ugandan cases of *Health Marketing Group v Financial Intelligence Authority*;[225] *Sundus Exchange & Money Transfer v Financial Intelligence Authority*[226] among others reveal the seriousness of the FIU in combatting financial crimes involving electronic transactions in Uganda.

4.2.2 Minister of Information and Communication Technology (MoICT), Uganda

The Ministry of Information and Communications Technology was established in June 2006 with a mandate of providing strategic and technical leadership, overall coordination, support, and advocacy on all matters of policy, laws, regulations, and strategy for the ICT sector.[227] The MoICT has also shown a level of interest in

[223] Effective Inter-Agency Co-Operation in Fighting Tax Crimes and Other Financial Crimes 3 ed (2017) available at https://www.oecd.org/tax/crime/effective-inter-agency-co-operation-in-fighting-tax-crimes-and-other-financial-crimes-third-edition.pdf, accessed 4 May 2021.
[224] Ibid.
[225] Health Marketing Group v Financial Intelligence Authority (Miscellaneous Cause-2019/178) [2019] UGHCCD 215 (01 November 2019).
[226] Sundus Exchange & Money Transfer v Financial Intelligence Authority (Miscellaneous Cause-2018/154) [2018] UGHCCD 100 (27 August 2018).
[227] The Ministry of Information and Communications Technology (2011), National Information Security Strategy (NIIS) Final Draft, 2011 available at http://www.nationalsecuritystrategy.org, accessed on 18 September 2020.

developing and protecting technology abuse. The Ministry has proposed strategies to establish a national computer incident response team with a 24/7 call centre, computer incident response teams, a watch and alert centre, and reporting mechanisms.[228]

Despite this interest, the ministry still faces challenges with ICT development and implementation. Some of the identified challenges facing the ICT sector include low levels of digital literacy and general apprehension with respect to ICTs; inadequate complementary infrastructure for effective roll out of ICT facilities; vandalism of ICT infrastructure; onerous taxation regimes for the sector; and fragmented ICT initiatives across government due to disparate mandates.[229] Worse still, individuals with technical knowledge of networks and networking devices continue to steal sensitive information and money through online access to bank accounts and credit card numbers used by online retailers. This includes conducting a host of juvenile pranks like erasing backup files, raising the buildings' temperature, and turning off phones and traffic systems.[230] In the case of *Uganda v Garuhanga and Mugerwa*[231] computer data was manipulated, resulting in the loss of 3,800,000,000 Ugandan shillings for Shell Uganda Ltd. The accused persons were charged with embezzlement and false accounting as there was no enabling law for charges of computer forgery and computer fraud at that time. These challenges facing the country need to be addressed to harness the opportunities arising from the development of the sector.

4.2.3 Computer Emergency Response Team

Computer Emergency Response Team (CERT-UG) is the national Computer Emergency Response Team for Uganda, operating Under the National Information Technology Authority of Uganda (NITA-U). CERT-UG is the first official National Computer Security Incident Response Team to be launched in Uganda. Its establishment helps to ensure the protection of the nation's critical information infrastructures, assist in drafting the overall plan on the country's approach to cybersecurity-related issues. It can serve as a focal point for further building and

[228] Ibid.
[229] 'The State of ICT in Uganda' (2019) available at https://researchictafrica.net/wp/wp-content/uploads/2019/05/2019_After-Access-The-State-of-ICT-in-Uganda.pdf, accessed on 18 September 2020.
[230] NIIS Final Draft op cit note 11.
[231] CR 17 of 2004.

implementing the National Culture of Cybersecurity.[232] There is a collaboration with threat-intelligence agencies,[233] and in addition, private sectors share information with CERT-UG and the Communication Sector CERT.[234] The establishment of CERT to facilitate cybersecurity efforts in Uganda is therefore in line with the international best practice.

4.2.4 Uganda Police Force Cybercrime Unit

The Ugandan Police Force has established a Cybercrime Unit, which is mandated to detect and investigate crimes that are electronically or computer-generated; these are crimes committed using online platforms like Facebook, WhatsApp, Twitter, etc. Generally, the Police Cybercrime Unit has the power to enforce the CMA with its subsidiary legislations. These subsidiary legislations will be discussed below.

4.3 National legislations on cybercrime in Uganda

4.3.1 Computer Misuse Act, 2011

The CMA is the first Act enacted in Uganda to prevent abuse and misuse of information systems by regulating the conduct of electronic transactions and the safety and security of information transmitted electronically.[235] The Act was passed into law by Parliament on 14 February 2011. The Act contains 32 sections, five parts, and one schedule.

Part 1 of the Act contains definitions and interpretation of terms used in the Act. Part II of the Act includes provisions that further explain the meanings assigned to crucial terms used in the Act, particularly those concerning how data is accessed or modified on a computer.[236] Part III of the Act is what this chapter will focus on as it captures the procedural-law section of the CMA. Part III provides three orders, which can be issued by the court in relation to data on computers. These are the preservation order, the disclosure of preservation order, and the production order. The preservation order is

[232] 'The role of Computer emergency team' available at http://Ucc.co.ug/cert/, accessed 26 April 2020.
[233] Ibid.
[234] Ibid.
[235] Long Title of the CMA.
[236] Section 2 of the CMA.

issued at the request of an officer investigating the commission of any offence, to access, preserve, or procure any computer data necessary for the investigation. The order is issued where data on a computer is reasonably suspected to be in danger of modification, loss, or damage.[237] The disclosure of preservation order is issued where data has been preserved to be disclosed to an officer investigating the commission of an offence, no matter how or by whom such data was stored or transmitted.[238] Amanya[239] argues that the CMA is silent on the standard of proof required in an expeditious preservation order. He further states that the 'reasonable' ground test is insufficient to apply across all crimes listed in the Act. It poses a significant risk of a preservation order being issued on the basis of mere suspicions, which risk violations of the right to privacy.

Part IV of the Act puts in place punitive measures to punish computer misuse. The first category of offences involves fraud and exploitation through computers, and these are treated as the most serious offences within the Act. It is important to note that where the offence involves 'protected computers', life imprisonment can be imposed.[240] Protected computers are computers used for or in connection with national security and diplomatic relations, financial services or banking, communications infrastructure, public utilities, public safety, and emergency services. Section 20 of the CMA regulates enhanced punishment for offences involving protected computers. This section places the onus on an accused to prove that he or she did not know that the computer concerned was 'protected'. Section 20(2) defines this type of machine as follows:

> a computer is treated as a 'protected computer' if the person committing the offence knows or ought reasonably to have known, that the computer or program or data is used directly in connection with or necessary for –
>
> a. the security, defence or international relations of Uganda;

[237] Section 9 of the CMA.
[238] Section 10 of the CMA.
[239] T Amanya *A Critical Examination of the Law Relating to Cybercrime in Uganda* (unpublished LLM dissertation, University of the Western Cape, 2019) 54.
[240] Section 20 of the CMA.

b. the existence or identity of a confidential source of information relating to the enforcement of a criminal law;
c. the provision of service directly related to communications infrastructure, banking and financial services, public utilities or public key infrastructure; or
d. the protection of public safety including systems related to essential emergency services such as police, civil defence and medical services.[241]

In connection with the onus of proof, section 20(3) provided as follows:

> For the purposes of any prosecution under this section, it shall be presumed, until the contrary is proved, that the accused has the requisite knowledge referred to in subsection (2).[242]

Van der Merwe[243] argues that the above section seems to load the dice too heavily in favour of the State.

Section 28 of the CMA contains provisions on search orders; it provides that a police officer can search and seize any computer system or applications that he/she reasonably believes are concerned in the commission of a crime. Such an officer can demand information from persons in charge of the computer system or compel service providers to provide information within their technical abilities. It is a crime to hinder or prevent the officer from doing his/her work. A person found guilty is liable on conviction to a fine not exceeding 240,000 Uganda shillings or imprisonment not exceeding six months or both.[244] Section 28(7) of the CMA requires that police officers executing such search warrants 'shall have due regard to the rights and interests of a person affected by the seizure to carry on his or her normal activities.' In this respect,

[241] Section 20(2) of the CMA.
[242] Section 20(3) of the CMA.
[243] D van der Merwe 'A comparative overview of the (Sometimes Uneasy) relationship between digital information and certain legal fields in South Africa and Uganda' (2014) 17 *PELJ* 302.
[244] Section 28(7) of the CMA.

Amanya[245] argues that the CMA gives broad and unclear powers to police officers regarding the search and seizure of data or devices based on suspicion of a potential perpetrator's plan to commit a computer-related offence under the Act. This creates a risk of abuse of fundamental human rights since the Act leaves the determination of 'reasonableness' to the assessment of criminal justice officers.[246]

Section 30 of the CMA however bestows on the Magistrate court, the exclusive jurisdiction on offences relating to the Act. It is however notable that the CMA has extraterritorial application, which means that it applies to anyone regardless of their nationality or their presence in Uganda,[247] provided they were in Uganda at the time of the commission of the offence or the program used was based in Uganda.[248] In relation with the Council of Europe Convention on Cybercrime, it should be noted that some of the terms defined by the CMA (for example, 'data', 'program' or 'computer program', 'traffic data'), type of conduct criminalised and the wordings used in some of the offences, and the investigative measures introduced by the Act (for example, preservation order, disclosure of preservation order) has a close resemblance with the wording in the Convention.[249]

Other laws enacted, guide, and regulate the ICT sector to create level ground, and conducive environment for doing business using electronic means in Uganda include the Electronic Transaction Act and the Electronic Signature Act. These laws will be discussed in the subsequent sections.

4.3.2 The Electronic Transaction Act, 2011

The Electronic Transaction Act, 2011 (ETA) was enacted to provide for the use, security, facilitation, and regulation of electronic communications and transactions; and to encourage the use of e-government services and provide for matters connected therewith. The objective of the Act includes:

---

[245] Amanya op cit note 28 at 49.
[246] Ibid.
[247] Section 30(1) of the CMA.
[248] Section 30(2) of the CMA.
[249] The cybercrime legislation of commonwealth states: Use of the Budapest Convention and Commonwealth Model Law available at https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3e4

a. to provide a legal and regulatory framework to enable and facilitate electronic communication and transaction;
b. remove and eliminate the legal and operational barriers to electronic transactions;
c. promote technology neutrality in applying legislation to electronic communication and transactions;
d. provides legal certainty and public confidence in the use of electronic communications and transactions;
e. promote e-Government services through electronic communications and transactions with the Government, public and statutory bodies;
f. ensure that electronic transactions in Uganda conform to the best practices by international standards;
g. encourage investment and innovation in information communications and technology to promote electronic transactions;
h. develops a safe, secure and effective environment for the consumer, business and the Government to conduct and use electronic transactions; and
i. foster economic and social prosperity.[250]

The ETA addresses issues relating to the enforcement and requirements of electronic contracts; the regulation of domain names is now considered a new form of digital property. The ETA aims to ensure privacy protection for consumers and users of electronic media and the establishment of a regulatory framework, which is compliant with the rapid technological changes. The ETA has also imposed several duties on electronic communications service providers, such as telecommunications service providers and internet service providers, to intercept or halt the use of the internet and telecommunications facilities in the perpetration of cybercrime.[251] In this respect, a different argument can be drawn from Copyright legislation, which provides that infringement of copyright and neighbouring rights. Infringement occurs where, without proper authorisation under the Act, a person does or causes or permits another to reproduce, fix, duplicate, or extract copyright material other than for his or her private

[250] Section 4 of the Electronic Transaction Act.
[251] Section 29 of the Electronic Transaction Act.

use.[252] The interpretation of this provision would mean that where electronic communication service providers permit clients to misuse the internet by carrying out any form of criminality related to copyright infringement, they share the offender's liability.[253] Kakooza[254] contends that the position of 'fair use' of copyright works over the internet is difficult to exercise. He further argues that it is hard for licence holders to access their work over the internet without computer hackers taking advantage of the 'fair use' principle to gain access to the copyrighted works.[255]

It is pertinent to note that, with regard to the evidential value attached to electronic records, section 8(4) of the ETA requires a court to take into account the reliability in how the electronic records are generated, stored, or communicated. In the case of *Hesse Brian v Senyonga Patrick & 12 Others*[256] His Lordship Justice Christopher Madrama buttressed the best evidence rule as applicable in respect of electronic record and that it is fulfilled upon proof of the authenticity of the electronic record system in or by which the data was recorded or stored. He further held that the court has to take into account several matters relating to the reliability of the manner in which the data messages was generated, stored or communicated. It should be noted that the ETA mainly takes care of civil proceedings that relate to an electronic transaction but are not sufficient to take into consideration aspects of electronic evidence of a criminal nature.[257]

4.3.3 The Electronic Signature Act, 2011

The Electronic Signatures Act, 2011 (ESA) was enacted to regulate the use of electronic signatures in Uganda. The ESA's objectives include the modernising and harmonising of laws relating to computer-generated evidence and amendments to the

---

[252] Section 46 of the Copyright and Neighbouring Rights Act.
[253] E Wanyama 'The upsurge of cybercrime in Uganda: where the gaps and loops lies; Analysis of the Need For Legislative and Policy Framework' available at https://www.academia.edu/8949753/The_Upsurge_of_Cyber_Crime_in_Uganda_Where_the_Gaps_and_Loops_lie_Analysis_of_the_Need_for_Legislative_and_Policy_Framework, accessed May 13 2021.
[254] A C Kakooza 'Cybercrime and Social-economic development in Uganda: A legal perspective' available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1715637, accessed 30 September 2020.
[255] Ibid.
[256] Civil Suit No. 612/2014
[257] Vastina Rukimirana Nsaza op cit note 54 at 8

current laws that allow for admissibility and evidential weight of electronic communication. ESA regulates the use of electronic signatures, criminalisation of unauthorised access and modification of electronic signatures, and determination of minimum requirements for the functional equivalence of electronic signatures.[258]

The ESA defines 'electronic signature' as data in electronic form affixed to or logically associated with a data message, which may be used to identify the signatory in relation to the data message and indicate the signatory's approval of the information contained in the data message; and includes an advance electronic signature and the secure signature. Part IV of the ESA further contains provisions that apply to digital signatures or signatures used as the prescribed encryption method in the Public Key Infrastructure (PKI). Van der Merwe[259] contends that the introduction of the PKI-Infrastructure as a prescribed encryption method is a standard that has been accepted worldwide.[260]

Furthermore, the ESA mandates the National Information Technology Authority – Uganda (NITA-U) to manage, monitor and control PKI.[261] In this respect, the investigation powers granted in terms of NITA-U can be abused, especially with regards to the anonymity and privacy of the individuals whose identities are connected to a certificate.[262]

4.3.4 Data Protection and Privacy Act, 2019

On 23 May 2019, the Data Protection and Privacy Act, 2019 (DPPA) came into force in Uganda. The DPPA gives effect to Article 27 of the Constitution of the Republic of Uganda, 1995, that the right to privacy should at all times remain protected in the management of data. The DPPA aims to protect individuals' privacy and personal data by regulating the collection and processing of such personal information. It also seeks to provide for the rights of persons whose data is collected. The DPPA applies to

[258] Section 2 of the Electronic Signature Act.
[259] D van der Merwe 'A comparative overview of the (sometimes uneasy) relationship between digital transformation and certain legal fields in South Africa and Uganda' (2014) 17 *PELJ* 297-326.
[260] Ibid.
[261] Section 22 of the Electronic Signature Act.
[262] Ibid.

collecting, holding, and using personal data within Uganda and data collected outside Uganda relating to Uganda citizens.

The DPPA is divided into eight parts covering data collection and processing principles, data security, data subjects' rights, data protection register, complaints, and offences. Section 2 of the DPPA defines data as information that is processed utilising equipment operating automatically in response to instructions given for that purpose or is recorded to be used or processed.

The DPPA creates a Data Protection Office (DPO) under the National Information Technology Authority (NITA), whose role to oversee the overall enforcement of DPPA. The NITA does not constitute an independent body, NITA-U is given authority and is under the general supervision of the MoICT.[263] The DPO is charged with enforcing the DPPA and specifically to:

a. Oversee the implementation of the DPPA;
b. Promote the protection and observance of the right to privacy and personal data;
c. Monitor, investigate and report on the observance of the right to privacy and personal data;
d. Carry out sensitisation on the DPPA;
e. Investigate cases of violation of data protection and privacy and;
f. Maintain data protection register among other function.

Part II of the DPPA provides for duties and responsibilities that a person or entity holding data shall comply with. The Act further provides that a person holding data, including a data collector, processor, controller, or any person who collects, processes, holds, or uses data shall follow the set principles. The principles of data protection under section 3 include:

1. Accountability to the data subject;

[263] Available at http://Data-Protection-and-Privacy-Law-Analysis, accessed 28 September 2020.

2. Fairness and lawfulness;
3. Adequacy and relevancy of data;
4. Use of data as authorised by law;
5. Ensuring quality of information collected, processed or held;
6. Transparency and participation of data subject;
7. Ensuring safety and security of the data[264]

The principles mentioned above align with the international standards on data reliability and accountability. Furthermore, in relation to section 3(1)(a) of the DPPA, which provides for the accountability principle, a review of the DPPA shows that limited provisions are outlining the requirements of how the data collector, processor, or controller obtained the data in compliance with the law.

The DPPA is silent on areas of what is deemed lawful or unlawful collection of data. Section 3 of the DPPA provides that data must be collected or processed lawfully and fairly. Section 7 requires that consent, as defined as 'freely given, specific, informed and unambiguous', must be obtained from a person before the data is collected. However, section 7(2) provides for exceptions to the general rule of consent. It provides that:

a. Data will be collected without consent where it is required by law;
b. Where the collection of data is necessary for public use;
c. For national security;
d. For prevention, detection, investigation, prosecution or punishment of an offence or breach of the law;
e. For performance of a contract where the data subject is a party;
f. For medical purposes

In light of the above, section 7(2) of the DPPA could be open for abuse. For instance, provisions allowing for the collection of data for medical reasons may be abused to collect all forms of private data without consent from the holder. The law should have provided for such limitations to avoid abuse of such discretion.[265]

[264] Ibid.
[265] Ibid.

Section 8 of the DPPA requires a data controller or processor to seek the parent/legal guardian's consent before dealing with any data relating to a minor. Section 9 of the DPPA prohibits collecting and processing data related to religious, philosophical, political opinion, sexual, financial, health status, or medical records of an individual. The exceptions are if the data is collected or processed by the Uganda Bureau of Statistics, collection mandated by law on an employer. Where data is gathered for these reasons, consent is said to be given freely by the data subject.

Section 10 of the DPPA prohibits collecting or processing personal data in a manner that infringes on a data subject's privacy. The Act has empowered the data subject (the individual in respect of whose personal information is requested, collected, collated, processed, or stored) by providing for rights such as:

a. the right to know the purpose for which the information is collected;
b. the right to consent to the collection (informed consent given freely for a specific purpose); and
c. the right to request for correction by way of updating or ensuring accuracy of the data or deletion of the information.

Section 14 of the DPPA provides that a data controller or processer shall only process necessary or relevant data. Such data shall not be excessive or beyond what is authorised by law. This provision will ensure data is not abused, and the data collected is in line with its purpose and use.

Section 23 of the DPPA makes it mandatory for a data controller or processor who believes that personal data has been accessed or acquired by an unauthorised person to notify the NITA. NITA will, in turn, determine if there is any need to notify the data subjects. Section 24 of the DPPA further confers on a data subject a right of access to information relating to their data. However, the DPPA provides for two exceptions to the principle of access to information. First, where a third party can access information held by a data controller or processor, this happens where the data subject has provided consent to the access of such data. Second, where it is reasonable in

the circumstances to give data to a third party without the consent of the data subject.[266]

Despite the laudable provisions enumerated in the DPPA, the DPPA does not provide for situations where the data subject may withdraw his or her consent to collect and process data in any form.

4.4 Other legislative mechanisms

4.4.1 The National Information Technology Authority Act, 2009

The National Information Technology Authority Act (NITA) establishes the National Information Technology Authority in Uganda (NITA-U), a government agency under the general supervision of the Minister responsible for information technology; to coordinate, supervise and monitor the utilisation of information technology in public and private sectors in the country.[267] Section 5(3) of the NITA Act mandates the NITA-U to coordinate, supervise, and monitor the use of information technology systems. NITA Act is silent on the scope of the supervision and monitoring to be done by NITA-U. Amanya[268] argues that the Act leaves the concept of 'use of information technology system' unexplained, making this provision unclear and ambiguous. Amanya further states that this provision's interpretation could subject persons to illegal cyberattacks and unlawful interceptions of personal data.

The NITA Act mandates NITA-U to regulate and enforce standards for information technology hardware and software equipment procurement in all government sectors, agencies, and parastatals.[269] NITA-U is also obligated to create, design, and maintain a national data system.[270] The NITA Act does not stipulate the nature, mode, and form of data to be stored in the national database. This *lacuna* creates room for illegal interception under the guise of collecting data for the national database. The nature of the database is furthermore unclear and it is therefore submitted that this makes data susceptible to unlawful access by third parties.

[266] Section 24(4)(b) of the Data Protection and Privacy Act.
[267] Section 5(3) of the NITA-U Act.
[268] Amanya op cit note 28 at 42.
[269] Section 5(3) of the NITA-U Act.
[270] Section 5(e) of the NITA-U Act.

The NITA Act mandates NITA-U to establish, maintain, and regulate aspects of technological planning, organisation, delivery, support systems, disposal, database security, policy implementation and disposal systems.[271] Section 5 of the NITA Act confers broad powers to the NITA-U to establish guidelines and regulations regarding information technology systems' utility. The NITA Act does not explain the regulation procedures involved, thereby creating opportunities for unnecessary interceptions with personal data and devices.

Part V of the NITA Act regulates the information technology surveys and powers of NITA-U. An information technology survey is understood as an operation in which enumerations, inspections, studies, examinations, reviews, inquiries, or analyses are carried out to collect or gather information and data on information technology matters. In carrying out such a survey, the NITA-U has the power to collect information and data regarding information technology for the sector specified in the order. It may use summons and search warrants to facilitate the enforcement of such collections of data and information.[272]

Section 20(1) of the NITA Act stipulates that where data or information technology has been collected in accordance with Section 19 of the NITA Act, the Executive Director, an officer of the authority, or an authorised officer, may require any person to supply him or her with any particulars as may be prescribed, or any particulars as the Executive Director may consider necessary or desirable in relation to the collection of the information. Furthermore, a person who is required to give information under subsection (1) shall, to the best of his knowledge and belief, provide all necessary information, in the manner and within the time specified by the Executive Director.[273]

Section 21 of the NITA Act further expands on the powers of the authority. Section 21 provides that the authority's staff or an authorised officer may at all 'reasonable times' enter and inspect any building or place to make such inquiries, as may be necessary for the collection of information and data for a survey to be carried out under Section

[271] Section 5 (6) of the NITA-U Act.
[272] Section 19(3)(a)(b) of the NITA-U Act.
[273] Section 20(2) of the NITA-U Act.

19. The NITA Act is silent on the meaning of 'reasonable times'. Section 38(4) provides that where a person hinders or obstructs the Executive Director, an officer of the authority or an authorised officer in the lawful performance of any duties or in the lawful exercise of any power imposed or conferred on him or her under NITA-U commits an offence. A person who commits such an offence is liable, on conviction, to a fine not exceeding 12 currency points or imprisonment not exceeding 6 months, or both.

Section 34 to 39 of the NITA Act confers unfettered powers to the Minister of Information and Computer Technology to make directives and make regulations necessary for implementing the NITA Act, including declaring acts or offences that amount to a crime under the Act and prescribing punishment for such offences. Amanya asserts that the checks and balances established under the NITA Act are weak and fall short of international standards to enhance a transparent system.

The functions of NITA-U have a crucial role in the fight against cybercrime. NITA-U, as a regulatory agency saddled with the responsibility to coordinate, monitor, and promote the use of information technology in Uganda, they are in a position to recommend enacting regulations that will be useful in combatting cybercrime. If the mandate given to NITA-U is effectively carried out, it will create barriers to engage in computer-related offences.

4.4.2 The Regulation of Interception of Communication Act, 2010

The Regulations of Interception of Communications Act (RICA) came into force on 3 September 2010. Section 3 of RICA provides for the establishment of a monitoring centre to intercept communication under the Act. The Minister of 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 Organization, the Inspector General of Police, or their nominees.[274] A warrant to intercept communications shall be issued by a designated judge upon proof of legitimate interest instead of proof of the existence of substantial grounds.[275] RICA bases the grounds for the application of a warrant of

[274] Section 4(1) of the Regulation of Interception of Communication Act.
[275] Sections 5, 6 and 7 of the Regulation of Interception of Communication Act.

interception on threats to the national economic interest.[276] However, the statute is silent on the meaning of national economic interest.[277]

Section 9 of RICA mandates telecommunications service providers to ensure that subscribers register their SIM cards and provide comprehensive information about, for example, their identity and address.[278] RICA does not provide details relating to maintaining the databases by these firms, which create opportunities for illegal access to personal data of Ugandans by third parties.[279] RICA presents many ambiguous, undefined procedures and terms of reference for the officials involved in its implementation.[280]

4.5 Emerging issues and challenges in the Arena of Cyberlaw in Uganda

4.5.1 Jurisdictional challenge

The existing international law pertaining to a nation's sovereignty also details that a sovereign nation can make laws affecting those people who reside within its territorial boundaries.[281] The Charter of the United Nations also recognises that a state has to be supreme within its borders.[282] However, the Internet is borderless, and it has no geographic boundaries, thereby thwarting the entire jurisdiction issue. Jurisdiction refers to each state's power under international law to prescribe and enforce its national laws concerning those persons and property within its territorial borders. This power can be exercised in three forms, which are generally recognised in international law as the jurisdiction to prescribe, jurisdiction to adjudicate, and jurisdiction to enforce.[283] Prescriptive jurisdiction, also known as legislative jurisdiction, relates to the state legislature's right to create, amend, or repeal legislation.[284] Adjudicative jurisdiction signifies the competence of courts to apply their national laws.[285] Lastly,

---

[276] Section 5 of the Regulation of Interception of Communication Act.
[277] Amanya op cit note 28 at 45.
[278] Section 9 of the Regulation of Interception of Communication Act.
[279] Amanya op cit note 28 at 45.
[280] Ibid.
[281] M N Shaw *International Law* 5 ed (2003) 409.
[282] Article 2(4) and 2(7) of the Charter of the United Nations (adopted 24 October 1945) 1 UNTS XVI.
[283] Ibid at 143.
[284] Ruwanthika Gunaratne and Public International Law available at https://ruwanthikagunaratne.wordpress.com,2008 accessed 27 September 2020.
[285] Ibid.

enforcement jurisdiction refers to a States' ability to enforce its national laws or judicial labour (for example, gathering evidence and imposing sanctions).[286] The above-mentioned types of jurisdiction are often co-dependent and based on similar considerations.

The determination of jurisdiction in respect of cyber-related offences could be cumbersome and most difficult for the courts to determine.[287] Because cybercrime is relatively new, no international norm exists for the punishment of offenders. This has continued to cause confusion and misapplication of legal principles for the enforcement of cybercrime laws. Since cybercrime offences are usually transnational involving multiple jurisdictions, this creates the problem of which state could rightly assume jurisdiction. These problems have necessitated the need for various states to include provisions conferring their national courts with extraterritorial jurisdictions.[288] One of the primary concerns with the assertion of extraterritorial criminal jurisdiction, or even the primary use and application of the old 'Territorial Principle', gives rise to competing claims.[289] The competing jurisdictional claims by various nations were evident in *Yahoo, Inc. v La Ligue Contra Le Racisme et L'Antisemitism*,[290] wherein an action filed in France by the International League against Racism and Anti-Semitism and the Union of Jewish Students against Yahoo. Yahoo! Inc. posted on Yahoo.fr a warning to French citizens that searches might lead them to items that violate French law. Yahoo! Inc. also prohibited the auctioning of items on its website that promoted racist groups, accepting government-issue stamps and coins, and establishing a more

---

[286] I Bantekas & S Nash *International Criminal Law* 2 ed (2003) 143.
[287] A M Weber 'Council of Europe's Convention on Cybercrime' (2003) 18 *Berkeley Tech LJ* 425.
[288] M Hildebrandt 'Extraterritorial jurisdiction to enforce in cyberspace? Bodin, Schmitt, Grotius in cyberspace' (2013) 2 *University of Toronto Law Journal* 196-224.
[289] Ibid.
[290] *Yahoo!, Inc. v La Ligue Contre Le Racisme et L'Antisemitisme*, 169 F. Supp. 2d 1192 (N.D. Cal. 2001) Yahoo! filed an action in a United States court seeking declaratory relief from the French court's order on the basis that the order (in its entirety) was not enforceable under the US Constitution. Having concluded that the French order violated Yahoo!'s First Amendment rights, the United States District Court of California stated that such violation no matter how short in duration constituted 'irreparable injury.' The court held that although the French order could regulate speech occurring in France on the basis of content or viewpoint, the French order could not be enforced against the same speech occurring simultaneously in the United States. Enforcement of such an order would impermissibly violate the First Amendment-even if such speech was considered highly offensive. Accordingly, the court refused to enforce the French order prohibiting Yahoo! from displaying or selling Nazi propaganda and artefacts through the use of its web site.

permissive stance on items of personal expressions, such as books or films. Yahoo! did include infrastructure on their space domain to prevent French citizens from accessing websites auctioning any such items.

Nevertheless, the French court ordered the items to be removed from the American site, arguing that French restrictions on free speech applied to any website viewable in France. On the other hand, Yahoo! argued that it is a company incorporated in the United States of America and is not bound by French Laws. On 22 May 2000, the French court determined that Yahoo!'s yahoo.com website, which offered certain items of Nazi propaganda and artefacts, violated a French criminal code provision that prohibited the display or sale of such items. Significantly, the French court further ordered Yahoo! to 'take all necessary measures to dissuade and render impossible any access via Yahoo.com to the Nazi artefact auction service and to any other site or service that may be construed as constituting an apology for Nazism or a contesting of Nazi crimes'.[291]

The Ugandan approach to deal with jurisdiction is arguably not well developed. However, the Ugandan law enforcement agencies are currently developing their practices and procedures relating to cyber-investigation. When one examines the provision of the CMA, one realises that on paper, the law has granted extraterritorial jurisdiction concerning cybercrime cases; in reality, it is not applied beyond the territorial boundaries of Uganda. This is due to these provisions directly conflicting with foreign governments' exercise of sovereignty within their national boundaries.

This is also exemplified by the case of Andrew Zzimwe Kasagga with two Congolese wanted by Interpol (Kenya) for being involved in a multi-million-dollar scam.[292] They were accused of fraudulent intranet bank transfers between Standard Charted Bank, Nairobi, and Barclays Bank Kampala. The Kenyan Standard Chartered Bank staff wired $5 million in three instalments 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

[291] Ibid
[292] S I Nganda & H Abdallah 'Interpol pursues Zzimwe fraud case' *The Weekly Observer*, 13 January 2015.

intercepted at Crane Bank. It had allegedly been sent to another suspect. While further investigations and trials were being conducted, another $3 million was swindled from Kenya; this transaction was detected before it was sent to the Forex Bureaux via the Development Finance Company of Uganda Group, commonly referred to as the 'DFCU' bank in Kampala.[293] To complicate the matter further, these organisations that used cyberspace services also lack sufficient information on security controls.[294] Therefore, in this scenario, it becomes an increasingly futile exercise to register any cybercrime case wherein the perpetrator of the cybercrime is physically located outside Uganda's territorial boundaries.

There is a need for the Ugandan authorities to assume enabling jurisdiction over data and information impacting Uganda more comprehensively than is currently provided for under current laws. There is a complete lack of case law on this issue of cybercrime jurisdiction in Uganda. The fact that Uganda is not a signatory to the Convention on Cybercrime is one of the challenges that will be encountered in an attempt to enforce the laws outside the jurisdiction of the Ugandan Police force. Until such time Ugandan law in this regard needs to be amended to comply with international practices; it would be prudent for Ugandan law enforcement agencies to detect, investigate, and prosecute cybercrimes within the ambit of existing principles of law.

4.5.2 Evidential issues

Evidence plays an important role in the administration of justice. According to Watney:

> when a crime is committed, one of the parties in the subsequent criminal proceedings may wish to rely on information generated, distributed or stored on electronic devices such as emails, text messages, database, and spread sheets. Electronic information is often relevant in proving or disapproving a fact or a point in question relating to the guilty or innocence of the accused and as

[293] P Maguta & C Ipu 'Effects of Cybercrime on State Security: Types, Impact and Mitigations with the Fiber Optic Deployment in Kenya' *Journal of information Assurance & Cybersecurity* Vol. 2011 at 6 available at http://www.ibimapublishing.com/journals/JIACS/jiacs.html accessed May 13 2021.
[294] F Tushabe *Computer Forensics for Cyberspace Crimes* (unpublished Masters Dissertation, University of Makerere, 2004) 25.

such the information forms part of the totality of evidence before the court. This information constitutes electronic evidence and the rule of law of evidence are applicable thereto in deciding its admissibility.[295]

This explains why the Evidence Act remains relevant in determining the type of facts that can be admissible as evidence. The Evidence Act, Cap 6 was enacted in 1909 and has not undergone major reform despite the numerous developments, such as technological developments and the changing nature of information. Section 60,[296] 61[297] and 63[298] of the Uganda's Evidence Act emphasises the 'Best Evidence Rule' which requires that only original documents in its written form are admissible in a court of law, in case of dispute, the admissibility and weight of this kind of evidence can be a challenge. While many Ugandans having adopted the use of technology, reliance on the 'Best Evidence Rule' as provided under the Evidence Act can pose challenges for admissibility of electronic evidence.

Over the years, efforts have been made through promulgation of a statute to ensure admissibility of electronic or digital evidence in Uganda. The Judicature (Visual-Audio Link) Rules, 2016 makes it more affordable to use technology to conduct proceedings in courts of law, these aims to provide for the taking of evidence in court by visual-audio link and to make it easier for witnesses to give evidence without physically appearing in court and their evidence does not constitute electronic evidence. However, the use of a Visual-Audio Link is merely an administrative channel for expeditious determination of disputes and does not constitute electronic evidence. Also, the Constitution (integration of ICT into the Adjudication process for courts of judicature) (Practice Directions), 2019 provides for electronic service of court documents, providing for electronic versions of documents including pleadings, emphasising use of technology.

[295] Admissibility of Electronic evidence in criminal proceedings. An outline of the South African legal position.
[296] Section 60 of Evidence Act, 1990 states that *'[t]he contents of documents may be proved either by primary or secondary evidence'.*
[297] That primary evidence means the document itself produced for inspection of the court.
[298] Documents must be proved by primary evidence except in cases mentioned under s 64.

As far as admissibility and weight of evidence of electronic data is concerned, section 8 of the Electronic Transactions Act, 2011 provides that rules of evidence shall not be applied to deny admissibility on the ground that it is merely a data message or electronic record where it is the best evidence that the person adducing the evidence could reasonably be expected to obtain or on the ground that it is not in the original form. It should be noted that, just like any other evidence, the proponent of electronic evidence must lay the proper foundation which makes the evidence reliable. Also, electronic evidence can also be relied on if the party who alleges has *inter alia* established its authenticity and the opposite party has not produced any proof of tampering. In the case of *Uganda v Ssrunkuma*[299] the court held that "the authenticity and integrity of electronic evidence is not in question until party suggesting otherwise can produce evidence to say so." However, the provisions on admissibility and evidential weight of a data message or electronic record under the Electronic Transaction Act of 2011, mainly takes care of civil proceedings that relate to an electronic transactions, but are not sufficient to take into consideration aspects of electronic evidence of a criminal nature.[300]

As shown above, it is clear that there is an improvement in the admissibility of electronic or digital evidence. However, serious issues have been raised in the digital world due to malpractices such as falsification of information and impersonation, in relation to the authenticity of information relied upon as evidence. It raises queries as to how it is possible to prove the creation and transmission of electronic communication by one party when the party's name as the author of the post could have been inserted by another. The challenges with respect to the admissibility and appreciation of electronic evidence, Uganda still has a long way to go in keeping pace with the developments globally. Although, section 8 of the ETA provides clarity with regard to the admissibility and weight of evidence of electronic data, they cannot be said to be without limitations. It is clear that Uganda has yet to devise a mechanism for ensuring the veracity of contents of electronic records, which are open to manipulation by any party by obtaining access to the server or space where it is stored.

[299] HC CR SC 15/2013.
[300] Vastina Rukimirana Nsaza op cit note 54 at 8.

However, time will determine how the courts will decide on cases where there has been a violation of the CMA and section 8 of the ETA to see whether there will be the need for amendment on the provision dealing with the admissibility of electronically generated evidence. In addition, there is a scarcity of technical skills of stakeholders in the criminal justice system to manage computer and electronic devices that store and process data electronically and digitally.[301] This task requires expertise in information and communication technology. Judges, lawyers and prosecutors need to have extensive computer skills to be able to form independent opinions and understanding of electronic evidence presented to them to satisfy the requirement of section 8 of the ETA and relevant provisions of the CMA. The computer knowledge will also give them the ability to verify the authenticity and certification of electronic evidence at their disposal to arrive at fair and just decisions. Currently, there are acute shortages of experts and professionals in information and communication technology among lawyers, judges and law enforcement personnel for the successful enforcement of the CMA.

4.5.3 Searches and seizures

This study also focuses on the search and seizure of electronic evidence in Uganda in the context of cybercrime. The primary legislative mechanisms that currently regulate search and seizure of electronic evidence in Uganda is the Criminal Procedure Code Act of 1950 (CPCA) (provides search and seizure procedures) and the CMA (which provides police officers with additional powers of search and seizure). With cybercrimes being committed in a different environment than a physical crime, the type of evidence differs too, requiring a change in legal procedures and ICT forensics.[302] In the physical world, searching for evidence at a crime scene would include fingerprints, DNA, gunpowder residue etc. However, the search for electronic evidence includes artefacts and electronic equipment that would indicate the use, ownership, or possession of electronic evidence.[303]

---

[301] C Emmanuel *'An Analysis of the Adequacy of the Electronic Transactions Act, 2011 In Governing E-Commerce in Uganda: A case study of online motor vehicle trade in Uganda'* (unpublished LLM dissertation, Uganda Christian University, 2016) 64.
[302] D P Van der Merwe et al *Information and Communications Technology Law* 2 ed (2016) 63.
[303] S C McQuade *Encyclopaedia of Cybercrime* (2009) 29.

Therefore, it is clear that the foundation of search and seizure of evidence shifts from the 'material world to the virtual world of cyberspace.'[304] As opposed to tangible evidence, digital evidence[305] can be found, for example, on electronic devices left behind at the scene of a crime, and to successfully arrest and prosecute criminals, consistent and clearly defined forensic procedures need to be followed by investigators.[306] Consequently, the field of ICT forensics[307] aims to preserve, collect, identify, analyse, and interpret electronic evidence derived from electronic sources to present this evidence before a court of law.[308] It is worthy to mention that Uganda has digital forensic laboratories in place, but despite the digital era, most laboratories are not equipped with the capabilities to conduct their own investigation.[309]

It is critical to acknowledge that the provisions of the CPCA that apply to search or seizure during investigation has not been reviewed since it came to force. This can be attributed to the limited knowledge of the criminal trial process by law enforcement officers.[310] The CPCA provides that a police officer may search any person who has been arrested and may take possession of anything found on the person, which might reasonably be used as evidence in any criminal proceedings.[311] As stated earlier, the CPCA was enacted in a time where data messages were not fully envisaged, and the only need was for search and seizure of tangible evidence and not electronic evidence. However, the issue for consideration is the applicability of the CPCA to electronic evidence with regards to cyber-specific terminology and procedures. Currently, the CPCA is being applied to matters that include the element of electronic evidence, providing for search warrants, searches and seizures without a warrant, the

---

[304] GP Bouwer 'Search and seizure of electronic evidence: Division of the traditional one-step process into a new two-step process in a South African context' (2014) 2 *SACJ* 156.
[305] Digital evidence and electronic evidence will be used interchangeably in this dissertation.
[306] M Reith et al 'An Examination of Digital Forensic Models' (2002) 1 *International Journal of Digital Evidence* 2.
[307] ICT Forensics is a separate complex topic that requires far more in-depth discussion which is not included in this paper however it is worth mentioning as the practical implementation of the search and seizure of electronic evidence requires the application of techniques that are foundational to ICT forensics.
[308] V Baryamureeba & F Tushabe 'The enhanced digital investigation process model' (2004) *The Digital Forensic Research Conference* 4.
[309] Available at http://www.forensicinstitute.org/forensicinvestigationinUganda accessed 12 December 2020.
[310] Ibid.
[311] Section 6 of the CPCA.

entering of premises, and the forfeiture and disposal of property connected with offences. [312] The CPCA further provides the mode of search and seizure procedures with a search warrant[313] and the authority to enter into premises. It should be noted that the right to a fair trial can be infringed by search and seizure procedures at the pre-trial stage.[314] Accused persons have the right to privacy[315] and the privilege against self-incrimination.[316]

The CMA further makes provision for powers to search and seize, obtain a warrant, and preserve confidentiality by the police. The police can access information or enter any premises in the furtherance of an investigation into alleged cybercrime.[317] As a result of the police's defunct position, the CPCA is relied upon in the regulation of the search and seizure of electronic evidence. Therefore, the provisions of section 28 of the CMA is expected to enable the authorising officer to extend their search to the external systems or servers, and information in the cloud, often referred to as 'cloud computing' if at any time during their investigation, they discover that the required information or evidence is stored in another computer system or network.[318] However, the CMA is silent in this regard.

Concerning the search of external servers and information in the cloud by an authorising officer, one of the problems that are usually envisaged is that the authorising officers may be liable for actions against third parties in cases where the required information is being held in the custody of an external server that is jointly shared by others. This is because it might be difficult to decrypt the actual information relevant to the case and the suspect in question.

---

[312] Currently electronic evidence is accepted under the definition of 'document' in s 221(5) of the CPCA.
[313] Section 6(2) of the CPCA states that '[n]otwithstanding subsection (1), a police officer may search any person who has been arrested and may take possession of anything found on the person which might reasonably be used as evidence in any criminal proceedings.'
[314] Article 28 of the Ugandan Constitution.
[315] Article 27 of the Ugandan Constitution.
[316] Article 28(11) of the Constitution.
[317] Sections 28 and 29 of the CMA.
[318] J Dykstra 'Seizing electronic evidence from cloud computing environments' (2013) Available at http://www.csee.umbc.edu/-dykstra/Seeizing-Electronic-Evidence-from-Cloud-Computing-Environments.pdf, accessed on 7 June 2020.

Another relevant issue for consideration is whether an order of court must first be obtained before any search is made? To answer this question, section 28(3) of the CMA provides that 'A computer system referred to in subsection (2) may be seized or samples or copies of applications or data may be taken, only by virtue of a search warrant'. Invariably, the provision of section 28(3) of the CMA empowers the law enforcement officer to search and seize any computer evidence or data with a warrant.

Several jurisdictions have adopted practices to improve the criminal trial process in line with technological developments and international standards. As discussed in chapter two, the Ugandan CMA does not align with the international best practices with regards to search. Article 19(2) of the Council of Europe Convention on Cybercrime urges member states to adopt legislative and other measures to ensure that where its authorities search or similarly access a specific computer system or part of it and have grounds to believe that data sought is stored in another computer system or part of it; authorities shall be able to expeditiously extend the search or similar accessing to the other system.[319]

Based on the above, there is no doubt that cloud computing's introduction raises serious challenges to enforcement agencies' powers to search and seizes computer evidence relating to cybercrime cases and will most likely infringe on citizens' privacy rights.

4.5.4 Extradition and international cooperation

Extradition is the formal procedure for requesting the surrender of persons from one territory to another for the following purposes: prosecuting the offender, sentencing the offender after conviction of the offence, or carrying out a sentence that has already been imposed against the offender.[320] Generally, extradition happens between two countries and is mostly supported by bilateral treaties amongst the participating parties

[319] Ibid.

[320] Z Deen-Racsmány *Active personality and non-extradition of nationals in international criminal law at the dawn of the twenty-first century: Adapting key functions of nationality to the requirements of International Criminal Justice* (unpublished Doctoral dissertation, EM Meijers Institute of Legal Studies, Faculty of Law, Leiden University, 2007). Available at http://openaccess.leidennuniv.nl/bitstream/hamdle/1887/12098/Chapter+4.pdf?sequence=10&origin=publication accessed on 7 June 2020.

and as enshrined in each state's national legislation.[321] There are three main parties in extradition: the country which has made the extradition request (the 'requesting' State); the country which has been asked to extradite a person in their territory (the 'requested' State); and the person whose extradition is sought (the 'subject').[322]

The primary legislation on extradition in Uganda is the Extradition Act, 1964. The Act provides that there is no general obligation to surrender a person who is within its territory unless it had signed bilateral or multilateral[323] extradition treaties agreeing to transfer the 'fugitive offenders'.[324] The nature of cybercrime offences makes them one of the exceptional cases where the fugitive criminal could commit the offence while still being physically present in the extraditing country's territory. The foundation on which extradition is usually established is on the principle of 'dual criminality,' which means that before a criminal can be validly extradited, the alleged offence must be a crime, which is punishable in the jurisdiction seeking extradition; without satisfying this requirement, the criminal may not be extradited. The difficulties presented by this requirement is well illustrated in the 'Love Bug' case. The Love Bug virus destroyed many files, stole passwords, and then spread rapidly throughout the world, and forced the shutdown of computers at large corporations such as Ford Motor Company and Dow Chemical Company and the computer system at the House of Lords.[325] It was estimated to have affected over 45 million users in more than 20 countries, causing billions of dollars in damage. However, investigators determined that the person responsible was a former computer science student in the Philippines. At the time, the Philippines had no applicable law punishing such conduct. The accused could not be extradited to the United States due to the lack of dual criminality, as no cybercrime laws existed in the Philippines at the time.[326]

---

[321] S Deva Bedi *Extradition in International Law and Practice* (1966) 69.
[322] A Babalola 'Extradition under International Law: Tool for Apprehension of Fugitives' (2014) 22 *Journal of Law, Policy and Globalization* 25-35.
[323] Section 2 of the Extradition Act of 1964 (Application of the Act to Commonwealth countries).
[324] M Kassim-Momodu 'Extradition of Fugitives by Nigeria' (1986) 3 *International and Comparative Law Quarterly*, 512-530.
[325] S W Brenner 'Cybercrime Investigation and Prosecution: The Role of Penal and Procedural Law' available athttp://unpan1.un.org/intradoc/group/public/documents/APCITY/UNPAN003073.pdf, accessed on 7 June 2020.
[326] N K Katyal 'Criminal law in cyberspace' (2001) *University of Pennsylvania Law Review,* 1003-1114.

By their nature, cybercrime offences are transnational and go across territorial boundaries and geographical limitations, and therefore require international cooperation between countries to ensure successful investigation and prosecution.[327] Cybercrime offences are profoundly different from traditional crimes, and therefore their investigations require high-level technical expertise and efficient cross-jurisdictional investigations.[328]

The CMA makes no provision or reference to international cooperation whether or not any bilateral or multilateral agreements exist between Uganda and the requested or requesting country. The Act, therefore, creates administrative and legislative bottlenecks that are encountered in cybercrime prosecutions. In extradition proceedings, issues regarding the principle of 'dual criminality' will continue to hinder international cooperation in respect of cybercrime offences in developing countries like Uganda. There is a lack of counterpart capacity both in human resources and technical capabilities.[329] Computer systems and computer networks work on diverse operating systems that, in turn, are composed of millions of codes that require outstanding technological know-how to configure how these systems work and the level of their interconnections to the various networks.[330] Investigations into these areas require extensive investment in the requisite human resources, which are often far beyond a developing nations' budget where these cybercriminals usually thrive.[331] There is no doubt that cybercriminals take advantage of these *lacunas* in the laws in perpetuating their nefarious acts against computer systems. It is not enough to merely provide for international cooperation without going through the essentials of how this should be achieved. Lastly, because these offences are of a cross-border nature,

---

[327] M Keyser 'Council of Europe Convention on Cybercrime' (2002) *J Transnat'l L & Pol'y* 12, 287.

[328] R Broadhurst 'Developments in the global law enforcement of cyber-crime' (2006) 3 *Policing: An International Journal of Police Strategies & Management* 408-433.

[329] S W Brenner & J J Schwerha IV 'Transnational evidence gathering and local prosecution of international cybercrime' (2001) 20 *J Marshall J Computer & Info L* 347.

[330] B Shavers 'Cybercrime investigation case studies: An excerpt from placing the suspect behind the keyboard' (Newnes, 2012); A O Nkechi 'Effective strategies for the improvement of human and material resources management in the Nigerian local government system' (2014) 3 *International Review of Management and Business Research* 1264.

[331] G Lovet 'Fighting cybercrime: Technical, juridical and ethical challenges' (2009) In Virus Bulletin 67-70.

there are limited extents that law enforcement officers would need to take to locate evidence abroad, not to mention suspects. The issue of jurisdiction is always guided by individual law enforcement officers, thereby making it difficult for the other agencies to investigate beyond their own boundaries.

4.6 Conclusion

This chapter has discussed the various existing legal and institutional frameworks applied to prosecuting digital crimes in Uganda. Some of these prosecution cases have been based on the CMA, the Electronic Signature Act, and the Electronic Transaction Act, and applied as 'Cyber laws'. It is pertinent to note that the punishment for the crimes mentioned above is not a major legal problem. The cyber-related laws adopted already target such acts and determine the appropriate punishments. However, the real problem lies in the difficulty of proving the elements of these crimes and prosecuting the perpetrators. The intangible nature of the internet, its international nature, and the differences between Uganda and other countries' laws have been a major limitation in the prosecution of cybercrimes.

In light of the above, the difficulty of applying the current laws that are not adequate to the new nature of cybercrime is problematic. Some of the key procedural issues in the regime of cyberlaw include jurisdictions, search and seizures, evidential issues, and extradition and international cooperation. These issues have been a significant limitation on the prosecution, investigation, and enforcement of cybercrime laws in Uganda.

The next chapter will examine the measures taken by South Africa to address cybercrimes and the key procedural issues in the regime of cyber law.

CHAPTER FIVE: A COMPARATIVE OVERVIEW OF SOUTH AFRICAN CYBERCRIME LAWS WITH RELEVANT PROVISIONS IN UGANDA

5.1 Introduction

South Africa was the first African country to adopt comprehensive cybercrime legislation as far back as 2002.[332] Since then, it has developed a national cybersecurity strategy and has embarked on a process of implementing it. It has also coordinated cybersecurity efforts, as well as a number of laws to protect personal data, including the Electronic Communications and Transaction Act (2002), Cyber Security Policy Framework (2012), Protection of Personal Information Act (2013), Critical Infrastructure Protection Bill (2019), the Cybercrimes Bill (2020), and the National Cybersecurity Policy Framework. Notably, the government also works with civil society to educate and raise public awareness of cyber risk.[333] These measures include comprehensive data protection laws, a national cyber policy, data privacy regulators, and the establishment of a focal point to champion these processes and work with the public. Therefore, this chapter will conduct a comparative study on how the South African legal system has responded to cybercrime and what lessons Uganda can learn.

5.2 National cybercrime legislation in South Africa

5.2.1 Electronic Communications and Transactions Act, 2002

The ineffectiveness of the common law to deal with and combat cybercrime led to the promulgation of the ECTA in 2002. The ECTA has as its objective the facilitation and regulation of electronic communications and transactions. The ECTA deals with cybercrime in Chapter XIII, in which several new cybercrime-related offences were created. These new offences include obtaining unauthorised access to, interception of or interference with data, computer-related extortion, fraud and forgery; and attempt, and aiding and abetting regarding the aforementioned offences.[334]

---

[332] Available at http://www.itweb.co.za/historyofSouthAfricanCyberlegislation, accessed 12 December 2020.
[333] N Kortjan 'A cyber security awareness and education framework for South Africa (unpublished Masters dissertation, Nelson Mandela Metropolitan University, 2013) 166.
[334] Sections 37(3), 40(2), 58(2), 82(2), 86(1), (2), (3) of the ECTA.

The ECTA also created the "cyber inspector" who may "enter any premises or access any information that has a bearing on an investigation" into a cybercrime.[335] The arrival of the ECTA was applauded, as it was an attempt made by the South African legislature to address and improve cybersecurity and to create and prosecute new cybercrimes. However, the ECTA received some criticism and it is generally accepted that there is still room for improvement.[336]

It is argued that the penalties for engaging in cybercrime, as stipulated in section 89 of the ECTA, are not severe enough.[337] This is because it is argued, a person convicted of certain offences in the ECTA can, at most, be liable for a fine or be imprisoned for a period of one year.

For other offences in the ECTA, a person can be liable for a fine or be imprisoned for, at the most, a period not exceeding five years. It is argued that these punishments are not enough of a deterrent to prevent the commission of cybercrimes and that the ECTA should be amended to included harsher penalties.

5.2.2 The Cybercrimes Bill

The Cybercrimes Bill seeks to amend the ECTA to bring it in line with the international community.[338] The Bill aims to align the ECTA with current legislation trends, such as the Protection of Personal Information Act 4 of 2013 and the Consumer Protection Act 68 of 2008. The National Council of Provinces on 1 July 2020 approved the changes in the Bill and now awaiting a signature from the President for it to become law.[339] As set out in the long title, the purpose of the Bill is:

- To create offences which have a bearing on cybercrimes;
- To criminalise the distribution of data messages which are harmful;

---

[335] Section 82(1) of the ECTA.
[336] D van der Merwe D et al *Information Communications and Technology Law* 2 ed (2016) 80-81.
[337] F Cassim 'Addressing the growing spectre of cybercrime in Africa evaluating measures adopted by South Africa and other regional role players' (2011) 44 *CILSA* 123 at 127.
[338] C Schultz Cybercrime: An Analysis of current legislation in South Africa (unpublished LLM, University of Pretoria, 2016) 31.
[339] The Cybercrimes Bill is one step away from becoming law, available at http://www.clifffedekkerhofmeyr.com accessed 7 October 2020.

- To regulate jurisdiction in respect of cybercrimes;
- To regulate the powers to investigate cybercrimes;
- To regulate aspects relating to mutual assistance in respect of the investigation of cybercrimes;
- To provide for capacity building; and
- To provide that the executive may enter into agreements with foreign states to promote measures aimed at the detection, prevention, mitigation, and investigation of cybercrimes.

Part II of Chapter 2 of the Bill deals with malicious communications. Specifically, it addresses the dissemination of data messages that incite damage to property or violence; the distribution of data messages that threaten persons with damage to property or violence; and the non-consensual sharing of intimate images.

The Cybercrimes Bill, however, imposes harsh penalties, for an offence that is committed. The penalties range from a fine with a minimum amount of R5 million to a maximum of R10 million. The period for imprisonment provided for is a minimum of five years to a maximum of ten years.[340] In this regard, it is pertinent to note that the Cybercrimes Bill has provided for harsher fines and more extended periods of imprisonment, which is considered a substantial improvement from the ECTA.

Furthermore, sections 50 to 57 of the Cybercrimes Bill provide the structures which deal with cybersecurity. These include the Cyber Response Committee, Cybersecurity Centre, Government Security Incident Response Team, the National Cybersecurity Centre, Cyber Command, Security Hub, and Private Sector Security Incident Response Teams.[341] These provisions in the Bill create new state institutions to counter cybercrime and cyber-terrorism.

5.2.3 Critical Infrastructure Protection Act, 2019

On 28 November 2019, the President of the Republic assented to the Critical Infrastructure Act 8 of 2019 (the CIP Act). The CIP Act recognises that certain

[340] Chapter 2 of the Cybercrimes Bill.
[341] Section 52 (3) (a) of the Cybercrimes Bill.

infrastructure is critical for public safety, national security, and continuous protection of basic public services. As such, the CIP Act stipulates that adequate measures should be identified and put in place to protect and secure critical infrastructure.

The CIP Act provides that infrastructure is considered critical infrastructure if:

a. the functioning of such infrastructure is essential for the economy, national security, public safety and the continuous provision of basic public services; and
b. the loss, damage, disruption or immobilization of such infrastructure may severely prejudice the functioning or stability of the Republic, the public interest with regard to safety and the maintenance of law and order and national security.

The CIP Act repeals and replaces the National Key Points Act, 1980. Any National Key Point or National Key Point Complex declared under the National Key Points Act must be deemed to be a critical infrastructure until the Minister of Police has decided whether or not to declare it as critical infrastructure in terms of the CIP Act, which must be done within a period of 60 days after coming into operation of CIP Act.

The CIP Act establishes a Critical Infrastructure Council. Their responsibilities include considering and making recommendations in respect of applications to be designated as critical infrastructure, approving various guidelines, and reporting to the Minister of Police in respect of all matters relating to the CIP Act.[342]

The CIP Act further provides that the National Commissioner of the South African Police Service attend to the Act's administration.[343] The CIP Act allows the National Commissioner to appoint police officials as inspectors who have the authority to conduct inspections at critical infrastructure to ensure compliance with the Act.[344] A person in control of infrastructure can apply to have such infrastructure designated as

[342] Section 4 of the CIP Act.
[343] Section 9 of the CIP Act.
[344] Section 10 of the CIP Act.

critical infrastructure.[345] Once designated as critical infrastructure, the owner thereof is required to secure the critical infrastructure, as prescribed, at its own expense. The owner thereof must appoint an employee as a security manager of the critical infrastructure and notify persons who enter the premises that such infrastructure is critical infrastructure.[346] Should an owner fail to secure the critical infrastructure, the Minister of Police may order the owner to do so, failing which the Minister of Police may take steps to secure the critical infrastructure itself and recover any costs in doing so from the owner.[347]

Furthermore, any person who commits an offence in terms of the CIP Act is liable on conviction to a fine or imprisonment not exceeding 3 to 20 years, or both, depending on the offence.[348]

5.2.4 South Africa National Cyber Security Policy Framework (NCPF)

The NCPF was approved in 2012. The NCPF outlined its purpose as being,

> to create a secure, dependable, reliable and trustworthy cyber environment that facilitates the protection of critical information infrastructure while strengthening shared human values and understanding of cybersecurity in support of the nation's security imperatives and the economy.[349]

The NCPF milestones were to establish the CSIRT and the CERT at the end of March 2012. Grobler *et al*[350] argue that this could not be achieved due to political will as there were mandate changes that resulted in the mandate being handed over to the Department of Telecommunications and Postal Services. The mandate was later given to the State Security Service (SSA). The results thereof led to time-delay between policy development and policy implementation, and as a result, some

[345] Section 24 of the CIP Act.
[346] Section 17 of the CIP Act.
[347] Ibid.
[348] Section 26 of the CIP Act.
[349] National Cybersecurity Policy Framework, 201, at 15.
[350] M Grobler & J J van Vuuren 'Combating cyberspace fraud in South Africa (2007) slides from Council for Scientific and Industrial Research.

measures proposed in the NCPF are currently not implemented as originally projected.

5.2.5. Legal position regarding search and seize of electronic evidence in South Africa

The primary legislation on criminal procedure is the Criminal Procedure Act 51 of 1977. However, the ECTA, and the Regulation of Interception of Communications and Provision of Communication-related Information Act[351] have added additional search and seizure rules.

General searches and seizures are carried out under the authority of a warrant as prescribed by section 21 of the CPA. Section 21 of the CPA sets out that articles can be seized by virtue of a lawful search warrant, requiring police officials to seize the article in question and further authorise the police officers to search any person or premises or any person found on the premises identified in the warrant.

In terms of search and seizure, the CPA defines 'premises' as 'including land, any building or structure, or any vehicle, conveyance ship, boat or aircraft'.[352] Bouwer asserts that the search of a computer falls outside the ambit of this definition.[353] By way of illustration, in the case of *Zoeco System Managers CC v Minister of Safety and Security NO,* the applicant sought to set aside a warrant where their computer equipment and other electronic devices were seized.[354] Their application was successful on the grounds that the articles being seized were not described with sufficient particularity; therefore, the applicants could not decipher which articles were susceptible to being searched and seized.[355]

In aid of bringing the CPA in line with the virtual realm, Snail writes that the ECTA provides clarity to the terms 'premises' and 'article' used in the CPA by stating that

---

[351] The Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 (RICA).
[352] G P Bouwer 'Search and Seizure of electronic evidence: Division of the traditional one-step process into a new two-step process in a South African context' (2014) 2 *South African Journal of Criminal Justice* 158.
[353] Ibid.
[354] *Zoeco System Managers CC v Minister of Safety and Security NO* 2013 (2) SACR 545 (GNP).
[355] Ibid.

these terms include information systems and data messages.[356] Therefore, it updates the CPA provisions on search and seizure to include electronic evidence. The ECTA[357] identifies that certain evidence that will be encountered during cybercrime investigation. These include computer systems comprising of hard drives, keyboards, monitors, laptops, servers; traditional telephone systems, the Internet, wireless telecommunication systems, embedded computer systems which include mobile devices, navigation systems, smart cards, sensing, and diagnostic modules, amongst others.[358]

Furthermore, the ECTA introduced a cyber inspector who is an employee of the Department of Communications to search (enter any premises) and seize (access information) that may impact the investigation into cybercrime[359] and further permits the South African Police Services (SAPS) to call upon the cyber inspector for help in the investigation of cybercrime.[360] The ECTA further enables cyber inspectors with more technical search and seizure procedures by affording them the power to monitor and investigate the conduct and activities of cryptography service providers[361] and an authentication service provider[362] and perform an audit on a critical database administrator.[363]

The challenge identified is that despite the introduction of the cyber inspectors, none has been appointed in a cyber inspector's capacity who would have the skills to carry out these procedures.[364] It is also pertinent to note that the Act does not clearly specify the type of qualification a cyber inspector should possess but instead assigns the onus of appointing a cyber inspector to the Department of Communications Director-

[356] S Papadopoulos & S Snail. *Cyberlaw@SA III The law of the internet in South Africa* 3 ed (2012) 328.
[357] Sections 86 and 87.
[358] E Casey *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* 3 ed (2011) 8.
[359] F Cassim 'Formulating specialised legislation to address the growing spectre of cybercrime: a comparative study' (2009) 12 *PELJ* 59.
[360] Section 81(2) of the ECT Act.
[361] Section 81(1)(b) of the ECT Act.
[362] Section 81(1)(c) of the ECT Act.
[363] Section 81(1)(d) of the ECT Act.
[364] *S v Miller* [2015] 4 All SA 503 (WCC) para 56.

General.[365] Van der Merwe asserts that even though the ECTA aimed to bring new developments to the field of investigation in technology and cybercrime, it did not follow through on the practical application, as no cyber inspectors have been appointed.[366] The effect of this is that the SAPS had no opportunity to seek advanced assistance in the search and seizure of electronic evidence.

The difference between the search and seizure provisions of the CPA and the ECTA with regards to the information in the warrant is that the ECTA does not refer to a peace officer, and the warrant must specify 'the premises or information system' to be searched and seized.[367] Here, the inclusion of 'information system' remedied the uncertainty surrounding whether it was included in the term 'premises' as set out by the CPA.

To further strengthen the surveillance mechanisms used as search and seizure methods, the South African government passed into law the Regulation of Interception of Communications and Provision of Communication-related Information Act (RICA). It is pertinent to note that RICA is the only law in South Africa that governs communications signal interception. RICA establishes the practice of surveillance of direct and indirect communications and the collection of information. This is done by interception, monitoring, data retention, and decryption.[368] It further brought about the prohibition of unlawful data interference or monitoring of data.[369]

Currently, the exceptions to the general prohibition of unlawful interception are, amongst others: a directive being granted permitting the interception; consent being provided; for reasons such as the prevention of serious bodily harm or to determine the location in emergency situations etc. RICA provides for different directions and warrants, namely:

a. interception direction[370]

---

[365] S L Gereda 'The Electronic Communications and Transactions Act' (2006) *Telecommunication Law in South Africa* at 281.
[366] D P Van der Merwe et al *Information and Communications Technology Law* 2 ed (2016) at 86.
[367] Section 83(3)(a) of the ECT Act.
[368] Ibid.
[369] Sections 3 to 11 of RICA.
[370] Section 16 of RICA.

b. real-time communication-related direction[371]
c. archived communication-related direction[372]
d. decryption direction[373]
e. entry warrant.[374]

5.4 How the Cybercrimes Bill has addressed ECTA identified shortcomings

As shown in the ECTA, the concept of electronic evidence was limited to the terms 'data' and 'data message'. The Cybercrimes Bill broadens the foundation set by the ECTA by detailing different types of electronic devices and mediums such as programmes, systems, and storage mediums. The Cybercrimes Bill states that the CPA still applies together with the provisions set out in the Cybercrimes Bill as long as they do not contradict each other.[375] The impact of introducing definitions that cater for electronic devices, in addition to providing consistency and clarity to the existing legal position, is that it educates police officials with the knowledge that there are different types of electronic devices, which can create and store data in electronic form, and such data may constitute evidential material.[376] These examples show that the promulgation of the Cybercrimes Bill will bring about a greater sense of awareness and competency in those that deal with challenges involving technology.

The Cybercrimes Bill also establishes the 24/7 Point of Contact and the Cyber Response Committee.[377] The creation of the 24/7 Point of Contact as envisaged by the Cybercrimes Bill is inspired by the Cybercrime Convention[378] setting out its features to include operating twenty-four hours a day and seven days a week.[379] The objective of this organisation is to ensure that assistance is available with regard to proceedings or investigations of any offence as set out in the Bill.[380] The Cybercrimes Bill establishes the Cyber Response Committee to implement cybersecurity policies

[371] Section 17 of RICA.
[372] Section 19 of RICA.
[373] Section 21 of RICA.
[374] Section 21 of RICA.
[375] Section 27 of the Bill.
[376] S Mason & D Seng *Electronic Evidence* 4 ed (2017) 1.
[377] Section 52 of the Bill.
[378] M A Vatis 'The Council of Europe Convention on Cybercrime' (2010) *Proceedings of a workshop on deterring cyberattacks* 217.
[379] Section 52(3)(a) of the Bill.
[380] Ibid.

created by the Government.[381] The centralisation and proper coordination of these two bodies will ensure effective investigation and regulate cybercrimes.[382]

Further to the above, the Cybercrimes Bill now builds on and works together with RICA by introducing additional directions.[383] The Bill changes the current legal position by setting out specific obligations on all electronic communications service providers.[384] Currently, only fixed-line operators are required to be interceptable and store communication-related information.[385] The Cybercrimes Bill creates three more directions that involve data that is reasonably believed to be involved in the commission of an offence,[386] namely:

a. Expedited preservation of data direction - this direction involves preserving data for a period of 21 days.[387]
b. Preservation of data direction – this direction serves as a less invasive measure than seizure and serves as an alternative means of investigation in instances where seizure of the article in question is not necessary.[388] Under this direction data must be preserved for the period stipulated in the direction which cannot exceed 90 days. [389]
c. Disclosure of data direction[390] – this direction is similar to that of the preservation of data direction in that it acts as an alternative to seizure of an article.[391]

These preservation directions cater for instances whereby the electronic communications service providers are directed to freeze traffic data associated with an identified internet user for a certain period of time for a specific criminal

[381] Ibid.
[382] M Musoni 'Is cyber search and seizure under the Cybercrimes and Cybersecurity Bill consistent with the Protection of Personal Information Act? (2016) 37 *Obiter* 687.
[383] Section 38 of the Bill.
[384] Memorandum on the objects of the Cybercrimes and Cybersecurity Bill (2017) see (note 26 above at 25).
[385] Section 2 of GN 1325 in *GG* 28271 of 28 November 2005.
[386] Memorandum op cit note 53.
[387] Section 41 of the Bill.
[388] Memorandum op cit note 53.
[389] Section 42 of the Bill.
[390] Section 43 of the Bill.
[391] Memorandum op cit note 53.

investigation.[392] Preservation relates to data that has already been stored. It is submitted that these directions are put in place as measures to ensure the availability or integrity of the evidence by preventing deletion, deterioration, or modification.[393] This serves as an enhancement of the current legal position and provides a more effective tool in the search and seizure of electronic evidence.

Based on the above, it is evident that the drafting of the Cybercrimes Bill was influenced by the Cybercrime Convention, in that the Cybercrime Convention provides 'legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.'[394] It is submitted that the standard operating procedures speak to the specific criminal investigations mentioned in the Cybercrime Convention.

5.5 International cooperation and structures

The Council of Europe Convention on Cybercrime was the first international instrument at the international level to provide a comprehensive approach for the essential cross-border law enforcement cooperation in tackling cybercrime It should be noted that South Africa is yet to ratify the Convention.

In March 2012, the SADC adopted the Model Law on Computer Crime and Cybercrime[395] to guide the development of cybersecurity laws in SADC member states. However, it does not impose any obligations on member states to establish cybercrime laws. It does not establish any international cooperation obligations on member states. However, member states that have established cybersecurity laws may rely on the SADC Protocol on Mutual Legal Assistance in Criminal Matters[396] and the Protocol on Extradition[397] to obtain international cooperation from other Members.

---

[392] Papadopoulos & Snail op cit note 41 at 341).
[393] A Nieman *Search and seizure, production and preservation of electronic evidence* (Unpublished LLD, North-West University, 2006) 56.
[394] Article 14 of Council of Europe Convention on Cybercrime European Treaty Series.
[395] See SADC Model Law on Computer Crime and Cybercrime Version 2.0 Adopted on 02 March 2012.
[396] SADC Protocol on Mutual Legal Assistance in Criminal Matters (Luanda, 3 October 2002).
[397] SADC Protocol on Extradition (Luanda, 3 October 2002).

The SADC Protocol on Mutual Assistance requires member states to provide each other with 'the widest possible measures of mutual legal assistance in criminal matters'.[398] The Protocol also requires that such assistance shall be rendered without regard to whether the conduct which is the subject of the mutual assistance request by a Requesting State would constitute an offence under the laws of the Requested States.[399] The Protocol on Extradition requires that SADC States can only obtain cooperation amongst themselves based on 'dual criminality'.[400]

The review of the SADC showed the existence of international cooperation and mutual assistance mechanisms. It is also pertinent to note that the SADC failed to promote the establishment of a national CERT to coordinate responses to cybersecurity incidents at the sub-regional levels.

5.6 Comparison

Internationally, countries have enacted legislation to deal with cybercrimes. From a comparative perspective, the following discussions briefly examine the measures taken by South Africa and how Uganda can benefit from South Africa.

The battle against cybercrime cannot be won without first understanding the phenomenon. Once the lexicon is in place, drafting of the necessary artefacts for the harmonisation of ICT strategy, policy and regulatory frameworks can be undertaken in earnest. The South African Electronic Communications Amendment Bill, defines cybercrime as any criminal or other offence that is facilitated by or involves the use of electronic communications or information systems, including any device or the Internet or any one or more of them.[401] The Cybersecurity Policy Framework for South Africa of 2015 further defines cybercrime as 'illegal acts, the commission of which involves the use of information and communication technologies'.[402] These definitions seem to be an all-encompassing approach from the South African Act, as it tends to group every offence as a cybercrime as long as it has been committed through the use of a

[398] Article 2(1) SADC Protocol on Mutual Legal Assistance in Criminal Matters.
[399] Article 2(4) SADC Protocol on Mutual Legal Assistance in Criminal Matters.
[400] Article 3 SADC Protocol on Extradition.
[401] 'Bill may not be passed. Has laid fallow for six years and due to be replace by Cybercrimes Bill.
[402] National Cybersecurity Policy Framework for South Africa (2015).

computer device.[403] However, there is no definition of cybercrime in the Ugandan CMA.

Furthermore, as information technology develops rapidly around the world, so does cybercrime. To curb the menace, the selected jurisdiction introduced cyber-specific criminal offences. However, the newly introduced criminal offences become insufficient in curbing cybercrime as it keeps developing. Therefore, unlike Uganda, the criminal offences have been reviewed, amended, and expanded in South Africa. Also, drawing comparisons on criminal sanctions between the South African ECTA and the Ugandan CMA, it is pertinent to note that Van der Merwe criticised the criminal sanctions of the ECTA for being too lenient to offenders[404] although this appears to be a different case with Uganda's CMA[405].

Before the promulgation of the specific provisions to combat crime involving a computer, both Uganda and South Africa have tried the existing legal statutes, including applying traditional criminal provisions in cyberspace and applying cybercrime provisions to new forms of crimes. In doing so, judges become the front line of regulating the cybercrimes in question. However, it is not long before judges realise that far-reaching reforms cannot be achieved through judicial interpretations only in this specific field. An example of such a situation is the admissibility of electronic evidence. In South Africa, the ECTA has facilitated the investigation and prosecution of cybercrime and the admission of electronic evidence. For instance, in December 2009, a senior First National Bank employee, Morwesi Theledi, was arrested by the SAPS on allegations that she stole her colleague's PIN and passwords and granted access to Amalgamated Beverage Industries' (ABIs) bank account and carted away, with R27.3 million.[406] The SAPS used section 86(1) of the ECTA to investigate the suspect. Section 86(1) stipulates that a person, who intentionally

---

[403] D van der Merwe 'A comparative overview of the (sometimes uneasy) relationship between digital information and certain legal fields in South Africa and Uganda' (2014) 17 *PELJ* 289-612.

[404] The penalty provisions of the ECT Act – Maximum periods of the imprisonment of one year for most of the crimes prohibited by s 86 of the Act.

[405] The penalty provisions of the CMA – Maximum periods of the imprisonment of fifteen years for the crimes prohibited by s 20 of the CMA.

[406] L B Zomba *Computer Related Crime: A Comparative Analysis of Tanzania and South Africa Frameworks* (unpublished Post Graduate Diploma in Law, University of Cape Town, 2014) 32.

accesses or intercepts any data without authority or permission to do so, is guilty of an offence.

Section 15 of the ECTA provides for the admissibility and evidential weight of a data message as electronic evidence. For instance, in the case of *S v Motata,*[407] the accused was charged with, *inter alia,* driving a motor vehicle while under the influence of alcohol. After the accused allegedly crashed into the boundary wall of a residential property that belonged to the complainant, the complainant made certain audio recordings on his mobile phone and took some photos of the scene of the accident with a digital camera. The audio recording was later transferred from the mobile phone and stored on the complainant's laptop. At the trial, the court found that the audio recording was documentary evidence and ruled them admissible. On subsequent application for review by the applicant, the High Court of South Africa stated that a video film, like a tape recording, 'is real evidence, as distinct from documentary evidence, and provided it is relevant, it may be produced as admissible evidence, subject to any dispute that may arise either as to its authenticity or the interpretation thereof'.[408]

As shown in section 28 of the Ugandan CMA, the concept of electronic evidence was limited to the terms 'data' and 'data message.' Comparing this position with the South Africa legal system on cybercrime, one can notice that under the Cybercrimes Bill, the concept of electronic evidence has been expanded beyond 'data' and 'data message' to include different types of electronic devices and mediums such as programmes, systems, and storage mediums.[409] In this context, Uganda can learn from the South Africa legal regime on cybercrime.

Also, in terms of section 82(1) of the ECTA, unlike Uganda, the law has created a 'cyber inspector' who, with the authority of a warrant, may search any premises or information system if there is reasonable cause to believe that the documents or records have a bearing on an investigation. However, it has been argued that the

[407] Unreported case no. 63/968/07, Johannesburg District Court at 622.
[408] *Motata v Nair* NO 2009 (2) SA 575 B(T) para 21.
[409] Section 43 of the Cybercrimes Bill.

regulation of cyber inspector in practice does not work as well as expected, and very few of them, if any, have been appointed since the inception of the Act.[410]

It is worthy to mention that similar to South Africa, Uganda chooses to adopt territorial jurisdiction. The territorial jurisdiction authorises a country to regulate acts conducted in its territory, as long as the acts took place in the territory of the country in question, even when these acts have been carried out by foreigners.[411] However, this principle of territorial jurisdiction is pointed out to have an extraterritorial jurisdiction effect. The extraterritorial effect, according to section 30 of the CMA, means that it applies to anyone regardless of their nationality or their presence in Uganda,[412] provided they were in Uganda at the time of the commission of the offence or the program used was based in Uganda.[413] As concluded previously, it is noticeable that although Uganda attaches the extraterritorial effect to its jurisdiction principle, many issues still need to be considered, such as the judicial sovereignty of other countries. In this context, Uganda can learn from the South Africa legal regime on cybercrime. This will have a far-reaching effect on the problem of jurisdiction.

Further to the above, the Cybercrimes Bill of South Africa now builds on and works together with RICA by introducing additional directions.[414] The Bill changes the current legal position by setting out specific obligations on all electronic communications service providers.[415] Currently, only fixed-line operators are required to be interceptable and store communication-related information.[416] In this context, Uganda can learn from the South Africa legal regime on cybercrime.

In addition, South Africa has promulgated new legislation to deal with critical infrastructure as observed in the previous paragraph. The Critical Infrastructure Act of 2019 (the CIP Act) recognises that certain infrastructure is critical for public safety,

---

[410] Cassim op cit note 44 at 45.
[411] L Cohen-Tanugi 'The Extraterritorial application of American Law: Myths and Realities', February 2015, available at http://paper.ssrn.com/so13/papers.cfm?abstract_id=2576678 accessed 13 December 2020.
[412] Section 30(1) of the CMA.
[413] Section 30(2) of the CMA.
[414] Section 38 of the Bill.
[415] Memorandum op cit note 53.
[416] Section 2 of GN 1325 in *GG* 28271 of 28 November 2005.

national security, and continuous protection of basic public services. As such, the CIP Act stipulates that adequate measures should be identified and put in place to protect and secure critical infrastructure. In contrast with the legal position in Uganda cyber, there is no specific legislation protecting certain infrastructure. In this context, Uganda can learn from the South Africa legal regime on cybercrime.

5.7 Conclusion

As shown above, this chapter investigated the insights that can be gained from the comparative study of South Africa to combat cybercrime. The analysis was carried out based on the adequacy assessment criteria of the Cybercrime Convention, which focuses on the contents of the substantive and procedural laws and the enforcement mechanism. The analysis was conducted to identify the significant features of the impact of the implementation on the South Africa legal regime on cybercrime and establish what lessons can be drawn by Uganda in developing a framework on cybercrime. Another important issue contained in this chapter is the national implementation of the Cybercrime Convention in South Africa. Discussion of this issue also tried to justify the choice of South Africa for this research. In this regard, it was argued that the legal framework for cybercrime in South Africa had been amended to incorporate a series of crimes, using the Cybercrime Convention's standards as a model.

Consequently, the most innovative aspect of the implementation of this Convention is related to the procedural and international cooperation aspects contained in the treaty. The implementation of the Convention would imply a modernisation in the ways of obtaining digital evidence, which would be applied to the investigation of any crime, not just computer crimes. Likewise, the implementation of the Convention would imply being part of an international cooperation system. This is, indeed, relevant for cybersecurity protection in Uganda.

International best practices are clearly moving forward faster than Ugandan legislative practices in terms of the provision for substantive and procedural criminal law measures for more effective investigation of cybercrime. The Cybercrime Convention

provides a legal framework for international cooperation and instils confidence and trust that such cooperation has a solid foundation in domestic law.

While admitting that no cybercrime regime is perfect, some efforts at legislative reforms of cybercrime laws in South Africa were identified. In this regard, the chapter notes that for cybercrime law to be effective in responding to contemporary challenges, it must be periodically reviewed. On the whole, the comparative study presents a number of useful lessons for Uganda.

CHAPTER SIX: CONCLUSIONS AND RECOMMENDATIONS

6.1 Introduction

As we proceed into the information age, it becomes clearer that every nation must have a comprehensive legal framework to combat cybercrime. A criminal armed with a computer and an internet connection has the capability to access private information and computer systems illegally anywhere in the world.[417] The major challenge is that international cybercrimes have impeded law enforcement efforts in ways never before contemplated.[418]

This dissertation has critically analysed the practicability of the existing Ugandan legislation relating to cybercrime and the effect these laws have on their enforcement. Further, in the introductory chapter, it is explained that there is no uniform definition of cybercrime.

The second chapter of this dissertation examined the regional efforts towards cybercrime control. Aspects of the Council of Europe Convention on Cybercrime and the AU Convention were discussed in this dissertation's second chapter. It was ascertained that the Council of Europe Convention on Cybercrime is a successful convention not only because of the international platform it establishes, it also takes a systematic and consistent approach to cybercrime control. Therefore, if Uganda wants to join the international community and cooperate against cybercrime, it is better to adopt the Council of Europe Convention on Cybercrime.

Chapter three of this dissertation discussed computer-related offences under various Ugandan legislation. The classification of these offences are provided for in the CMA, it is submitted that the CMA does not comply with the international best practices in criminalising certain offences. In relation to the penalties within the CMA, this research has shown that the CMA imposes harsh penalties if offenders are found guilty of committing offences criminalised within the CMA.

[417] D Leslie *Legal Principles for Combating Cyber-Laundering* (2014) 168.
[418] Ibid.

Chapter four of this dissertation discussed the legal frameworks for combatting cybercrime in Uganda. First, it examined institutions such as the Ministry of Information and Telecommunication and the Uganda Police Force (UPF) that both have policy frameworks designed to address cybercrime. The UPF is legally mandated by the Constitution to prevent and detect crime[419] in order to ensure that the rule of law prevails. However, these institutions have little knowledge of computer crimes, especially in detecting cybercrimes.[420] In a fully competitive environment of internet providers in Uganda, there would be a need for adequate cybercrime control regulations. The dynamic competitive role in the information and communications sector and the unsettled issues introduced by new technologies affect the regulatory environment. This prompted the Ministry of Information and Communications Technology to infuse national consciousness for the security ramifications of online activity.[421]

Second, regarding the regulatory frameworks in Uganda, this research has shown that the CMA, Electronic Transaction Act, and the Electronic Signature Act have recently been implemented to protect against cybercrime while promoting a safe and environmentally healthy electronic transacting environment. However, despite the available legal and institutional framework, the country continues to experience increasing cybercrimes.[422] Crimes such as cyber terrorism, intellectual property infringement, internet usage policy abuses, internet fraud, industrial espionage and altering of data, online child exploitation and pornography, illegal goods purchasing, piracy, impersonation, and hacking, remain a challenge.[423] This is yet to involve more undiscovered crimes given the pace of advancing technology, and while the future of technology remains rich with innovations.

The final discussion which was raised within chapter four of this research was about the emerging issues and challenges in the arena of cyber law in Uganda. It is

[419] Article 212(iii) of the Constitution of the Republic of Uganda 1995.
[420] F Tushabe *Computer Forensics for Cyberspace Crimes* (unpublished Masters Dissertation, University of Makerere, 2004).
[421] The Ministry of Information and Communications Technology (2011), National Information Security Strategy (NIIS) Final Draft, 2011.
[422] Ibid.
[423] F Tushabe & V Baryamureeba 'Cyber Crime in Uganda: Myth or Reality? (2005) 8 *Proceedings of the World Academy of Science, Engineering and Technology*.

submitted that there is a need for Uganda to amend the current cyber legislation to bring it in line with international best practices. The Evidence Act governing evidential issues as well as the search and seizure of electronic evidence in terms of the CPCA currently being used to search and seize electronic evidence also need to be urgently reviewed.

Considering the above, applying the current cyber-related legislation is problematic when considering the ever-changing nature of cybercrimes. The international nature of cybercrime raises complex legal issues, such as jurisdiction. Internet technology has resulted in countries being interconnected which also had the unintended consequence of the spread of cybercrime; each of these states has the right to claim jurisdiction in its favour. On the other hand, the issue of international cooperation in the field of judicial adjudication and the implementation of foreign judgements are raised. Enforcing a judgement given by a Ugandan court in relation to cybercrime outside the territory of the country is often not possible because of the absence of an international convention allowing for such cooperation. Therefore, Uganda's legal and institutional framework desires a lot to be done. This research has shown that there is no adequate legislation that contains adequate criminal procedural rules for cybercrime. Cybercrime remains on the increase due to the continuous use of online computer systems, the ability of criminals to hack into the systems, lack of control techniques, in the face of advancing technology.

Chapter five of this dissertation conducted a comparative overview of South African cybercrime laws with relevant provisions in Uganda. The first aspect discussed within the fifth chapter of this dissertation was the ECTA position. It was ascertained that the ECTA was an important step in creating a more secure and legally certain environment for electronic commerce. Furthermore, some shortcomings were identified within the ECTA. These shortcomings are that penalties which are provided for within the ECTA are not stringent enough to deter cybercriminals. A further criticism is that the ECTA provides for a cyber inspector for specialised investigation of cybercrime, and to date, not much has come of this because no cyber inspector has been appointed. To address the identified shortcomings, the Cybercrimes Bill was proposed. The Cybercrimes Bill has successfully addressed the shortcomings of the ECTA by imposing harsher penalties than those contained in the ECTA. The Cybercrimes Bill

also provides for state institutions that are controlled under different State departments to counter cybercrimes and ensure cybersecurity.

6.3 Recommendations

From the above assessment of the previous comparison and conclusion, this part addresses Uganda specifically on how Uganda can benefit from this research. The following recommendations are proposed:

6.3.1 Legislative recommendations

This recommendation is premised on the need to bridge the gaps disclosed by this study. The amendments are necessary at a national level to create an environment for the full enjoyment of cyber freedoms. The concept of electronic evidence should be defined and standardised amongst all areas of law to provide clarity and consistency on how the law interacts with this type of evidence.

Learning from the experience of South Africa, the need for the Ugandan CMA to have clear duties and boundaries of all law enforcement agencies; provisions encouraging mutual cooperation among law enforcement agencies and private bodies in the fight against cybercrime; clear definitions and scope of cybercrime; transparent procedures in obtaining and handling of personal data by private and public institutions; prevention of the use of anonymous identification tags; and the adoption of an objective test in the granting of court orders pertaining to the implementation of cyber-related law.

6.3.2 Ratification and domestication of the Convention on Cybercrime

Ratification and domestication of the Council of Europe Convention are paramount. Uganda has an option to ratify this Convention, as this would enhance international cooperation in the fight against cybercrime and go a long way in resolving jurisdiction issues when cybercrimes are committed and have to be prosecuted. In fact, the convention's ratification and domestication would further encourage international community members to report incidences of cybercrime to the law enforcement agencies, and establishment of mutual assistance. It is further recommended that Uganda should ratify and implement the African Union Convention on Cyber Security

and Personal Data Protection adopted in 2014 and harmonise IT laws and frameworks accordingly.

6.3.3 Dedicated structures to manage cybercrime

Once the ICT legislative framework has been strengthened to prosecute cybercrimes, the need for dedicated structures is then created. These structures are recommended as they are essential for the preventative, corrective and restorative aspects dealing with cybercrime in Uganda. It is recommended that a national cybersecurity regulatory and policy framework be implemented in Uganda as it will assist in combatting cybercrime by, *inter alia* providing additional definitions for cyber terminology, establishing dedicated bodies for national cybersecurity making, and capacity development for cyber-criminal threat intelligence, investigations, and prosecution.[424]

6.3.4. Cybercrime awareness

Governments are tasked with raising cybersecurity awareness within their countries. Combatting cybercrime does not only require technical and regulatory intervention, but it also relies on people. Public awareness tools may be used to stimulate, motivate, and remind the audience what is expected of them. It is recommended that the Ugandan Government should increase its cybersecurity awareness programmes by collaborating on cybersecurity awareness at government, business, and societal levels, as guided by an African Cyber Security Awareness Framework.[425] It is further recommended that the government should offer and facilitate specialised cyber training for security officers. The rationale is to cater to the gaps in detecting, investigating, and prosecuting cybercrimes in Uganda. Recent trends indicate that cyber-related crimes are becoming rampant. In addition, the lapse in the criminal justice system has facilitated the commission of conventional crimes such as murder, rape, and terrorism with the aid of cyber tools. The growing reliance of courts upon electronic evidence in criminal cases justifies equipping security officers with cyber knowledge

[424] National Cybersecurity Policy Framework for South Africa (2015) 7.
[425] Proceedings of Southern African Cyber Security Awareness Workshop (SACSAW), 2011 IZ Dlamini et al, 'Framework for an African Policy towards creating cyber security awareness' para 4.

BIBLIOGRAPHY

1. Legislation and draft legislation

1.1 South Africa:

Electronic Communications and Transactions Act 25 of 2002.
Electronic Communications Amendment Act 1 of 2014.

Prevention of Trafficking in Persons Act 7 of 2009.

The Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002.

1.2 Uganda:

Anti-terrorism Act of 2002.

Computer Misuse Act of 2011.

Constitution of the Republic of Uganda of 1995.

Copyright and Neighbouring Right Act of 2006.

Criminal Procedure Code Act of 1950.

Data Protection Bill, 2018.

Electronic Signature Act of 2011.

Electronic Transaction Act of 2011.

Evidence Act Chapter 6 of 2000.

National Information Technology Authority, Uganda Act of 2009.

Penal Code Act of 1950.

Prohibition and Prevention of Torture Act of 2012.

Regulation of Interception of Communication Act of 2009.

Uganda Communication Act of 2013.

2. Foreign law

Anti-Pornography Act of 2014.

Common Market for Eastern and Southern Africa (COMESA).

Computer Fraud and Abuse Act 18 U.S.C. 1030.

Computer Misuse Act of 1990 (as amended).

Council of Europe Convention on Cybercrime 2001.

Extradition Act of 1964 (Application of the Act to Commonwealth countries).

Protection from Harassment Act of 1997.

Protection of Children Act 1978 of (as amended).

The Police and Justice Act of 2006.

3. Case law

3.1 South Africa:

S v Miller [2015] 4 All SA 503 (WCC).

Unreported case no. 63/968/07, Johannesburg District Court.

Zoeco System Managers CC v Minister of Safety and Security NO 2013 (2) SACR 545 (GNP).

Motata v Nair NO 2009 (2) SA 575 B(T).

3.2 Uganda:

Digital Solutions v MTN 2004 UGHC 570.

Health Marketing Group v Financial Intelligence Authority (Miscellaneous Cause-2019/179) [2019] UGHCCD 215 (01 November 2019).

Hesse v Senyonga (Civil Suit-2014/612) [2015] UGCommC 90 (25 June 2015).

Hofni Topacho Ongiretho v Uganda (Criminal Appeal – 1993/1) (1994) UGSC 9 (03 March 1994).

Uganda v Dr Aggrey Kiyingi 2006 UGHC 52.

Uganda v Garuhanga and Mugerwa 2004 CR 7.

Uganda v Kato Kajubi 2010 UGCA.

Uganda v Nsubuga (HCT-00-AC-SC-2012/84) [2013] UGHCACD 12 (03 April 2013).

Uganda v Ssentongo (Criminal Session Case-2012/123) [2017] UGHCACD 1 (14 February 2017).

Uganda v Sserunkuma (HCT-00-CR-SC-2013/15) [2015] UGHCACD 4 (27 April 2015).

Uganda v Stella Nyanzi (Criminal Appeal-2019/) [2020] UGHCCRD 2 (20 February 2020).

Uganda vs Dr Aggrey Kiyingi [2006] UGHC 52.

3.3 Foreign cases:

Ahmet Yildirim v Turkey (Application No. 3111/10) 18 December 2012.

Joyce v DPP [1946] A.C. 347.

Sundus Exchange & Money Transfer v Financial Intelligence Authority (Miscellaneous Cause-2018/154) [2018] UGHCCD 100 (27 August 2018).

U.S. v Yunis (No.2) (1988) 82 I.L.R. 344.

Yahoo!, Inc. v La Ligue Contre Le Racisme et L'Antisemitisme, 169 F. Supp. 2d 1192 (N.D. Cal. 2001).

4. International instruments

Additional Protocol to the Convention on Cybercrime, Concerning Acts of a Racist and Xenophobic Nature Committed through Computer Systems available at http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm, accessed on 22 May 2020.

African Union Convention on Cybersecurity and Personal Data Protection available at http://au.int/en/treaties/african-union, accessed 7 October 2020.

Article 29 Data Protection Working Party 'Subject: Article 29 Working Party's comments on the issue of direct access by third countries' law enforcement authorities to data stored in other jurisdiction, as proposed in the draft elements for an additional protocol to the Budapest Convention on Cybercrime' (5 December 2013) Ref. A Res (2013) 3645289 – 05-12-2013.

Budapest Convention and Commonwealth Model Law available at https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3e4.

Chapter 120 of the Laws of Uganda 2000 and as amended by the Penal Code (Amendment) Act 8 of 2007.

Charter of Fundamental Rights of the European Union, OJ C/2007 C 303/1.

Charter of the United Nations (adopted 10 December 1948) UNGA Res 217 (III)

Convention is available at http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm, accessed 24 May 2020.

Council of Europe 'Convention on Cybercrime' available at http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=1&DF=&CL=ENG, accessed on 22 May 2020.

Council of Europe Convention on Cybercrime available at http://coe.int/en/web/convention/ETSNO.185 accessed on 23 June 2020.

Council of Europe Convention on Cybercrime ETS. 185, (Budapest, 2001).

Council of Europe, European Convention on Human Rights, CETS No. 005, 1950.

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89.

Council of Europe Convention on Prevention and Combating Violence Against Women and Domestic Violence (Istanbul Convention) available at http://www.coe.int/t/dghl/standardsetting/convention-violence/thematic_factsheets/Stalking_EN.pdf, accessed on 9 June 2020.

International Convention for the Suppression of the Financing of Terrorism, 1999 available at http://www.un.org/law/cod/finterr.htm, accessed 18 September 2020.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal

data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

SADC Model Law on Computer Crime and Cybercrime Version 2.0 Adopted on 02 March 2012.

SADC Protocol on Extradition (Luanda, 3 October 2002).

SADC Protocol on Mutual Legal Assistance in Criminal Matters (Luanda, 3 October 2002).

United Nations Optional Protocol to the Convention on the Rights of the Child on the State of Children, Child Prostitution and Child Pornography 2002.

5. Books and chapters in books

Bantekas I & Nash S *International Criminal Law* 2 ed (2003), Cavendish: Routledge

Card R *Criminal Law* 21 ed (2014), London: Butterworths.

Casey E *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* 3 ed (2011), San Diego: Academic Press.

Chawki M, A Darwish, A M Khan & S Tyagi *Cybercrime, Digital Forensic and Jurisdiction* (2015), Cham Springer International Publishing.

Clough J *The Principles of Cybercrime* 2 ed (2010), Cambridge: Cambridge University Press.

Deva Bedi S *Extradition in International Law and Practice* (1966), New Delhi: Discovery Pub. House.

Finklea K M *Identity Theft: Trends and Issues* (2010), Washington, D.C.: Congressional Research Service.

Franklin C J *The Investigator's Guide to Computer Crime* (2006), Springfield Ill: Charles C. Thomas.

Glanville Williams *The Text Book of Criminal Law* 2 ed (1983), Stevens & Sons, London.

Kirwan G *The Psychology of Cybercrime: Concepts and Principles* (2011), Hershey: IGI Global.

Kizza J M *Ethical and Social Issues in the Information Age* (2003), London: Springer.

Kshetri N *Cybercrime and cybersecurity in the global south* (2013), Hampshire: Palgrave.

Kuan Hon W & Millard C 'Cloud technologies and services' in C Millard (ed) *Cloud Computing Law* (2013), Oxford: Oxford University Press.

Leslie, D *Legal Principles for Combating Cyber-Laundering* (2014), Cham: Springer.

Lloyd L *Information Technology Law* 7 ed (2014), Oxford: Oxford University Press.

Mason S & Seng D *Electronic Evidence* 4 ed (2017), London: British Institute of International and Comparative Law.

McConville M & Hong W Chui *Research Methods for Law* (2007), Edinburgh : Edinburgh University Press.

McGuire M *Hypercrime: The New Geometry of Harm* (2007), Abingdon; New York: Routledge-Cavendish.

McQuade S C *Encyclopaedia of Cybercrime* (2009), Connecticut: Greenwood.

Mell P & Grance T *The NIST Definition of Cloud Computing* (2011), Gaithersburg, MD: U.S. Dept. of Commerce.

Mitnick K & William S L *The Art of Intrusion, The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers, Hardback* (2005), Hoboken: John Wiley & Sons.

Okafor K 'Legal perspectives to cyber security in Nigeria: Bold Perspectives' in A Adekunle (ed) *Combatting Cybercrimes in Nigeria: Trends and Issues* (2017), Lagos, Nigeria: Nigerian Institute of Advanced Legal Studies.

Oyebode A *International Law and Politics: An African Perspective* (2003), Lagos Bolabay Publishers.

Papadopoulos S & Snail *Cyberlaw@SA III The law of the internet in South Africa* 3 ed (2012), Pretoria: Van Schaik.

Pollitt M M 'Cyberterrorism – fact or fancy?' in E V Linden (ed) *Focus on Terrorism* (2001), New York: Nova Science Publishers.

Shaw M N *International Law* 5 ed (2003), Cambridge: Cambridge University Press.

Stevens T *Cyber Security and the Politics of Time* (2016), Cambridge: Cambridge University Press.

Tavani HT *Controversies, Questions, and Strategies for Ethical Computing* 4 ed (2013), Hoboken, NJ John Wiley et Sons, Inc.

Van der Merwe D P et al *Information and Communications Technology Law* 2 ed (2016), Durban: LexisNexis.

Walden I *Computer Crimes and Digital Investigation* 3 ed (2007), Oxford: Oxford University Press.

Zittrain J *The Future of the internet and How to Stop It* (2008), London: Penguin.

6. Journal articles

Ajayi EFG 'The impact of Cybercrimes on Global Trade and Commerce' (2016) 5 *International Journal of Information Security and Cybercrime* 31.

Aslan Y 'Global nature of computer crimes and the Convention on Cybercrime' (2006) 2 *Ankara Law Review* 129.

Ayofe A N 'Towards ameliorating cybercrime and cybersecurity' (2009) 3 *International Journal of Computer Science and Information Security* 1.

Babalola A 'Extradition under International Law: Tool for Apprehension of Fugitives' (2014) 22 *Journal of Law, Policy and Globalization* 25.

Baron MF 'A Critique of the International Cybercrime Treaty' (2002) *10 Common Law Conspectus* 263.

Barry C 'The Future of Cyber Terrorism, Crime and Justice International' (1997) 13 *Crime and Justice International Journal* 15-18.

Baryamureeba V & Tushabe F 'The enhanced digital investigation process model' - (2004) *The Digital Forensic Research Conference* 4.

Besen S M & Raskind L J 'An introduction to the law and economics of intellectual property' (1991) *The Journal of Economics Perspective* 3.

Biegel N A 'Modern stalking laws: A survey of state anti-stalking statutes considering modern mediums and constitutional challenges' (2001) 14 *Chapman Law Review* 457.

Bonanno R A & Hymel S 'Cyber bullying and internalizing difficulties: Above and beyond the impact of tradition forms of bullying' (2013) 45 *Journal of Youth and Adolescence* 685.

Bouwer G P 'Search and Seizure of electronic evidence: Division of the traditional one-step process into a new two-step process in a South African context' (2014) 2 *South African Journal of Criminal Justice* 156.

Brenner S 'Cybercrime investigation and prosecution: the role of penal and procedural' (2001)1 *Murdoch University Electronic Journal of Law* available at http://www.murdoch.edu.au/elaw/issues/v8n2/brenner82.html.

Brenner S W & Koops B-J 'Approaches to cybercrime jurisdiction' (2004) 4 *Journal of High Technology Law* 1.

Brenner S W & Schwerha J J IV 'Transnational evidence gathering and local prosecution of international cybercrime' (2001) 20 *John Marshall Journal of Information Technology and Privacy Law* 347.

Brenner S W and Ber-Jaap Koops 'Approaches to cybercrime jurisdiction' (2004) 4 *Journal of High Technology Law* 1.

Broadhurst R 'Developments in the Global Law Enforcement of Cybercrime' (2006) 29 *Policing: An International Journal of Police Strategies & Management* 408.

Byers S 'Internet: Privacy Lost, Identities Stolen' (2001) 40 *The Brandeis LJ* 141.

Cassim F 'Addressing the growing spectre of cybercrime in Africa evaluating measures adopted by South Africa and other regional role players' (2011) 44 *Comparative and International Law Journal of Southern Africa* 123.

Cassim F 'Addressing the spectre of terrorism: a comparative perspective' (2012) 15 *Potchefstroom Electronic Law Journal* 381.

Cassim F 'Formulating specialised legislation to address the growing spectre of cybercrime: a comparative study' (2009) 12 *Potchefstroom Electronic Law Journal* 59.

Chawki M & el Shazly Y 'Online sexual harassment: Issues and solutions' (2013) 4 *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 2.

Clark K et al ‘A Dutch approach to cybersecurity through participation’ (2014) 5 *Security & Privacy, IEEE* 27.

Clark K et al ‘A Dutch Approach to Cybersurity through Participation’ 2014 (5) *Surity & Privacy, IEEE* 27.

Clough J ‘A world of difference: The Budapest Convention on Cybercrime and the challenges of Harmonisation’ (2014) 40 *Monash University Law Review* 698.

Cottim ‘Cybercrime, Cyber terrorism and Jurisdiction: An analysis of Article 22 of the COE Convention on Cybercrime’ (2010) 1 *European Journal of Legal Studies* 55.

Decker C ‘Cybercrime: An Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cybercrime’ (2008) 81 *South California Law Review* 959.

Dejoolowu ‘Cyber-crimes and the Boundaries of Domestic Legal Responses: Case for an Inclusionary Framework for Africa’ (2009) 1 *Journal of Information, Law & Technology* 6.

Desuoza K C & Hensgen T ‘Semiotic emergent framework to address the reality of cyberterrorism’ (2003) 70 *Technological Forecasting and Social Change* 385.

Ebersohn G J ‘Catching Hackers’ (2003) 12 *Juta Business Law* 1.

Eboibi F ‘Cybercrime Prosecution and The Nigerian Evidence Act, 2011: Challenges of Electronic Evidence’ (2011) 10 *Nigerian Law and Practice Journal* 139.

Embar-Seddon A ‘Cyberterrorism: are we under siege?’ (2002) 45 *American Behavioural Scientist* 1033.

Florence Tushabe and Baryamureeba Venansius ‘Cybercrime in Uganda: Myth or reality?’ (2005) 8 *Proceedings of the World Academy of Science, Engineering and Technology* available at https://www.semanticscholar.org/paper/Cyber-Crime-in-Uganda%3A-Myth-or-Reality-Tushabe-Baryamureeba/8d1e0de4fdce3d6d593f510f378f6fab704098bd.

Gereda S L ‘The Electronic Communications and Transactions Act’ (2006) *Telecommunication Law in South Africa* 281.

Glyn E A ‘Computer abuse: The emerging crime and the need for legislation’ (1983) 12 *Fordham Urban Law Journal* 73.

Golak P. S '*Jurisdictional Jurisprudence and Cyberspace*' (2009) 4 *Assam University Journal of Science &Technology: Physical Sciences and Technology* 58.

Goodman M D & Brenner S W 'The emerging consensus on criminal conduct in cyberspace' (2002) 3 *UCLA Journal of Law & Technology* 4.

Goodno N 'Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws' (2007) 12 *Missouri Law Review* 125.

Gordon S & Ford R 'On the definition and classification of cybercrime' (2006) 2 *Journal of Computer Virology* 13.

Hildebrandt M 'Extraterritorial jurisdiction to enforce in cyberspace? Bodin, Schmitt, Grotius in cyberspace' (2013) 63 *University of Toronto Law Journal* 196.

Jahankhani H 'Evaluating of cyber legislations trading in the global cyber village' (2007) 11 *International journal of Electronic Security and Digital Forensics* 9.

Jignesh V, Meniya A & Jethva HB 'A review on botnet and detection technique' (2003) 4 *International Journal of Computer Trends and Technology* 23.

Johnson D R & Post D 'Law and borders: The rise of law in cyberspace' (1996) *Stanford Law Review* 1367.

Kadir R M 'The scope and the nature of computer crime statutes: A comparative study' (2010) 11 *German Law Journal* 614.

Kakooza A C 'Cybercrime and Social-economic development in Uganda: A legal perspective available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1715637, accessed 30 September 2020.

Kakungulu-Mayambala R & Rukundo S 'Digital activism and free expression in Uganda' (2019) 19 *African Human Rights Law Journal* 167.

Kassim-Momodu M 'Extradition of fugitives by Nigeria' (1986) 3 *International and Comparative Law Quarterly* 512.

Katyal N K 'Criminal law in cyberspace' (2001) *University of Pennsylvania Law Review* 1003.

Kerr, O.S. 'Searched and seizures in a digital world' (2005) Havard Law Review 531.

Keyser M ‘Council of Europe Convention on Cybercrime’ (2002) 12 *Journal of Transnational Law & Policy* 287.

Kuner C ‘Extraterritoriality and regulation of international data transfers in EU data protection law’ (2015) 5 *International Data Privacy Law* 235.

Lovet G ‘Fighting cybercrime: Technical, juridical and ethical challenges’ (2009) *Virus Bulletin* 67.

Lynne V, Copes H & Birch I ‘Identity theft’ (204) In *Encyclopaedia of Criminology and Criminal Justice* 2419.

Marion N E ‘The Convention on Cybercrime Treaty: An exercise in symbolic legislation’ (2010) 4 *International Journal of Cyber Criminology* 701.

Mayer J ‘Cybercrime Litigation’ (2006) 164 *University of Pennsylvanian Law Review* 1458.

Merschman J C ‘Dark side of the web: Cyberstalking and the need for contemporary legislation’ (2001) 24 *The Harvard Women’s Law Journal* 255.

Musoni M ‘Is cyber search and seizure under the Cybercrimes and Cybersecurity Bill consistent with the Protection of Personal Information Act? (2016) 37 *Obiter* 687.

Neal Kumar Katyal, ‘Digital Architecture as Crime Control’ (2003) 8 *The Yale Law Journal* at 2261.

Nganda S I & Abdallah H ‘Interpol pursues Zzimwe fraud case’ *The Weekly Observer*, 13 January 2015.

Nkechi A O ‘Effective strategies for the improvement of human and material resources management in the Nigerian local government system’ (2014) 3 *International Review of Management and Business Research* 1264.

Onyeozili E C ‘Obstacles to effective policing in Nigeria’ (2005) 1 *African Journal of Criminology and Justice Studies*, 32.

Orji U J ‘Examining Missing Cybersecurity Governance Mechanism in African Union Convention on Cybersecurity and Personal Data Protection’, (2014) 5 *Computer Law Review International* 131.

Paust J. “*Panel:Cybercrimes and the domestication of international criminal law”* (2007) 5 *Santa Clara Journal of International Law* 432.

Pittaro M L 'Cyber stalking: An analysis of online harassment and intimidation' (2007) 2 *International Journal of Cyber Criminology* 180.

Pollicino O 'The new relationship between national and the European Courts after the enlargement of Europe: Towards a unitary theory of jurisprudential supranational law?' (2010) 29 *Yearbook of European Law* 65.

Power R 'CSI/FBI Computer Crime and Security Survey' (2002) 17 *Computer Security Journal* 2.

P Maguta & C Ipu 'Effects of Cybercrime on State Security: Types, Impact and Mitigations with the Fiber Optic Deployment in Kenya' *Journal of information Assurance & Cybersecurity* Vol. 2011.

Redi J A, Taktak W & Dugelay J-L 'Digital image forensics: A Booklet for Beginners' (2011) 51 *Multimed Tools Application* 133.

Reith M et al 'An Examination of Digital Forensic Models' (2002) 1 *International Journal of Digital Evidence* 2.

Robert D & Doyle J 'Study on cyberstalking: Understanding investigative hurdles' (2003) 72 *FBI Law Enforcement Bulletin* 10.

Scannell J 'The 419 scam: An unacceptable power of the false?' (2014) 11 *PORTAL Journal of Multidisciplinary International Studies* 11.

Sundaresh M & Siew T G 'Key challenges in tackling economic and cybercrimes: Creating a multilateral platform for international co-operation' (2012) 15 *Journal of Money Laundering Control* 243.

Talbot J E 'Computer Attacks on Computer National Infrastructure: A Use of Force Invoking the Right of Self-Defence' (2002) 38 *Stanford Journal of International Law* 232.

Umejiaku N O & Anyaegbu M I 'Legal framework for the Enforcement of Cyber law and Cyber Ethics in Nigeria (2016) 15 *International Journal of Computer & Technology* 1.

Van der Merwe D 'A comparative overview of the (sometimes uneasy) relationship between digital information and certain legal fields in South Africa and Uganda' (2014) 17 *Potchefstroom Electronic Law Journal* 289.

Weber A M ‘Council of Europe’s Convention on Cybercrime’ (2003) 18 *Berkeley Tech Law Journal* 425.

Williams P ‘Organized crime and cybercrime: Synergies, trends, and responses’ (2001) 6 *An Electronic Journal of the US Department of State* 22.

Yasin Aslan ‘Global Nature of Computer Crimes and the Convention on Cybercrime’ (2006) 2 *Ankara Law Review* 3.

Zeviar-Geese G ‘The State of the Law on Cyber jurisdiction and Cybercrime on the internet’ (1997-1998) *Gonzaga Journal of International Law* 119.

7. Theses

Amanya T *A Critical Examination of the Law Relating to Cybercrime in Uganda* (unpublished LLM dissertation, University of the Western Cape, 2019).

Deen-Racsmány Z *Active personality and non-extradition of nationals in international criminal law at the dawn of the twenty-first century: Adapting key functions of nationality to the requirements of International Criminal Justice* (unpublished Doctoral dissertation, EM Meijers Institute of Legal Studies, Faculty of Law, Leiden University, 2007).

Emmanuel C *An analysis of the adequacy of the Electronic Transactions Act, 2011 in governing e-commerce in Uganda: A case study of online motor vehicle trade in Uganda’* (unpublished LLM dissertation, Uganda Christian University, 2016).

Kortjan N ‘A cyber security awareness and education framework for South Africa (unpublished Masters dissertation, Nelson Mandela Metropolitan University, 2013).

Schultz C Cybercrime: An Analysis of current legislation in South Africa (unpublished LLM, University of Pretoria, 2016).

Tushabe F *Computer Forensics for Cyberspace Crimes* (unpublished Masters Dissertation, University of Makerere 2004).

Tushabe F *Computer Forensics for Cyberspace Crimes* (unpublished Masters Dissertation, University of Makerere, 2004).

Zomba L B *Computer Related Crime: A Comparative Analysis of Tanzania and South Africa Frameworks* (unpublished Post Graduate Diploma in Law, University of Cape Town, 2014).

Zomba Lincoln Benn Computer Related Crime: A Comparative Analysis of Tanzania and South Africa Frameworks (unpublished Post Graduate Diploma in Law, University of Capetown 2014).

8. Other documents (white papers, draft documents, reports, etc.)

A brief study of the EU, the UK, France, Germany and the Netherlands' (2006) Perpetuity Research & Consultancy International, Leicester.

Admissibility of Electronic evidence in criminal proceedings. An outline of the South African legal position.

African Union (AU) Convention on Cyber Security and Personal Data Protection EX.CL/846(XXV).

Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY: Final report of the T-CY Cloud Evidence Group', and the open letter of the Article 29 Working Party on the issue of direct access by third countries' law enforcement authorities to data stored in other jurisdiction.

Dunlevy W 'Intelligence analysis for internet security' Carnegie Mellon Software Engineering Institute, and CERT Coordination Centre (2005).

ENISA Position Paper No.1 'Security Issues and Recommendations for Online Social Network' 2007 available at http://www.enisa.europa.eu, accessed 2 December 2020.

European Commission Directorate-General, Joint Research Centre. Available at http://primeproject.eu/community/furtherreading/studies/IDTheftFIN.pdf, accessed on 8 June 2020.

Explanatory Report to the Convention on Cybercrime European Treaty Series No 185.

Grobler M & Van Vuuren JJ 'Combating cyberspace fraud in South Africa (2007) slides from Council for Scientific and Industrial Research.

Information Security: Computer Controls over Key Treasury Internet Payment System, GAO-03-837 (U.S. Government Printing Office, 2003).

International Telecommunication Union ‘Understanding Cybercrime: A Guide for Developing Countries’ (2011).

International Telecommunication Union Cybercrime Legislation Resources *Understanding cybercrime: A guide for developing countries* (2009).

International Telecommunications Union ‘Understanding cybercrime: Phenomenon, challenges and legal response’, ITU Telecommunications Development Sector (September 2012).

ITU Global Cyber-Security Agenda (GCA) High Level Experts Group [HLEG] Global Strategic Report (2008).

McGuire M & Dowling S ‘Cybercrime: A review of the evidence’- Summary of key findings and implications (2013).

Memorandum on the objects of the Cybercrimes and Cybersecurity Bill (2017).

Ministry of Information and Communications Technology *National Information Security Strategy* (NIIS) (2011).

Mwaita P & Owor M ‘Workshop Report on Effective Cybercrime Legislation in Eastern Africa’ Dar es Salaam Tanzania (2013) available at http://rm.coe.int/16802f2349, accessed 24 May 2020.

National Cybersecurity Policy Framework for South Africa.

Proceedings of Southern African Cyber Security Awareness Workshop (SACSAW), 2011 IZ Dlamini et al, ‘Framework for an African Policy towards creating cyber security awareness’.

Provisional Text of Provisions, Preparation of a 2nd Additional Protocol to the Budapest Convention on Cybercrime, Cybercrime Convention Committee (T-CY), Council of Europe (1 October 2019) available at http://rm.coe.int/provisional-text-of-provisions-2nd-protocol-/168097fe64, accessed 11 November 2020.

Report to the Council of Europe Cybercrime Convention, ETS No. Criminal Policy and Research, 10(1) 27-37.

Shavers B ‘Cybercrime investigation case studies: An excerpt from placing the suspect behind the keyboard’ (Newnes, 2012).

Spoenle J ‘Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal?’ (Council of Europe, Strasbourg, 31 August 2010).

T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime.

Uganda Communication Commission ‘Report on status internet Users March 2017’ available at http://www.internetworldstats.com/af/ug.htm, accessed 24 May 2020.

United Nations Statistical Commission, 2012. National Institute of Statistics and Geography of Mexico Report on Crime Statistics: Note by the Secretary General E/CN.3/2012/3, 6 December 2011.

Vastina Rukimirana Nsaza presentation By Uganda Law Reform Commission on the Law of Evidence ALRAESA conference on 29th – 30th June 2017.

Vatis M A ‘The Council of Europe Convention on Cybercrime’ (2010) *Proceedings of a workshop on deterring cyberattacks*.

9. Online Sources

Additional Protocol to the Convention on Cybercrime, Concerning acts of a Racist and Xenophobic Nature Committed through Computer Systems available at http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm, assessed on 22 May 2020.

Adogame, A ‘The 419 Code as Business Unusual: Youth and the Unfolding of the Advance Fee Fraud Online Discourse’*, International Sociological Association e-bulletin*, 2007 available at http://www.isa-sociology.org/public/e-bulletin/E-bulletin 7,pdf, accessed on May 05, 2020.

Bellovin S M, Blaze M, Clark S & Landau S ‘Security implications of applying the communications assistance to Law Enforcement Act to voice over IP’ (2006). Available at http://www.itaa.org/news/docs/CALEAVOIPreport.pdf, accessed on 7 June 2020.

Brenner S W ‘Cybercrime Investigation and Prosecution: The Role of Penal and Procedural Law’ available athttp://unpan1.un.org/intradoc/group/public/documents/APCITY/UNPAN003073.pdf , accessed on 7 June 2020.

Business Vision Huawei delivers Uganda fibre internet backbone. *The New Vision* available at http://www.newvision.co.ug/newa/18322-huawei-delivers-uganda-fiber-internet-backbone.html, accessed 18 September 2020.

Chong Steven 'The role and duties of a Prosecutor – The Lawyer Who Never "Loses" A Case, Whether Conviction or Acquittal', being delivered Legal Service Officers and Assistant Public Prosecutors, 2-5, available at https://www.lawsociety.org.sg/.../Law%20Gazette/.../SLG_APR_20, accessed on 24 April 2020.

CIFAS identity fraud report is available at https://www.cifas.org.uk/identity_fraud accessed on the 8 June 2020.

Clarke R A & Knake R K 'Cyber War Excerpt' 5 available at https://richardaclarke.net/wphttps://richardaclarke.net/wp-content/uploads/2019/05/Cyber-War-Excerpt.pdfcontent/uploads/2019/05/Cyber-War-Excerpt.pdf, accessed 6 June 2020.

Clarke R A & Robert K Knake, "Cyber War Excerpt" page 5, available at https://richardaclarke.net/wphttps://richardaclarke.net/wp-content/uploads/2019/05/Cyber-War-Excerpt.pdfcontent/uploads/2019/05/Cyber-War-Excerpt.pdf accessed on 6 June 2020.

Cohen-Tanugi L 'The Extraterritorial application of American Law: Myths and Realities', February 2015, available at http://paper.ssrn.com/so13/papers.cfm?abstract_id=2576678 accessed 13 December 2020.

Council of Europe 'Chart of signatures and ratifications of Treaty 185' available at http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/treaty/185/signatures?p_auth=XvRotrxg accessed on 18 October 2020.

Council of Europe 'Explanatory Report to the Convention on Cybercrime' (Budapest, 23 November 2001) https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cc e5b, accessed on 8 February 2018.

Council of Europe 'T-CY Committee: Guidance Notes' https://www.coe.int/en/web/cybercrime/guidancenotes, accessed on 8 February 2018.

Council of Europe 'The Role of Public Prosecution in the Criminal Justice System', Recommendation Rec (2000) 19 Adopted by the Committee of Ministers of the Council of Europe on 6 October 2000 and Explanatory Memorandum, 4, 14-15, available at https://rm.coe.int/16804be55a, accessed on 14 April 2020.

Council of Europe available at http://conventions.coe.int/treaty/en/cadreprincipal.htm, accessed on 25 April 2020.

Cyber security survey 'African financial institutions and governments incurred a massive $3.5 billion loss to a wave of cyber-crime attacks in 2018' News, 10 April 2019, last accessed from *http://www.apanews,net/mobile/uneinternet/last* on 23 April 2020.

Cybercrime Convention Committee (T-CY) 'The Budapest Convention on Cybercrime: benefits and impact in practice' available at http://rm.coe.int/t-cy-2020-16-bc-benefits-rep...116809ef6ac accessed on 26 July 2020.

Cybercrime Convention Committee '(Draft) elements of an additional protocol to the Budapest Convention on Cybercrime regarding transborder access to data: Proposal prepared by the Ad-hoc Subgroup on Transborder Access and Jurisdiction available at https://rm.coe.int/cybercrime-convention-committee-t-cy-transborder-access-to-data-and-ju/168073dc0b, accessed 10 May 2021.

Cybercrime Convention Committee 'Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY: Final report of the T-CY Cloud Evidence Group 16 September 2016 available at http://rm.coe.int/16806a495e, accessed on 27 October 2020.

Cybercrime Convention Committee 'Terms of Reference for the Preparation of a Draft 2nd Additional Protocol to the Budapest Convention on Cybercrime' Strasbourg, 9 June 2017 available at http://rm.coe.int/terms-ofreference-for-the-preparation-of-a-draft-2nd-additional-proto/168072362b, accessed 27 October 2020.

Cybercrime Convention Committee, 'Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY: Final report of the T-CY

Cloud Evidence Group' 16 September 2016 available at http://rm.coe.int/16806s495e, accessed 27 October 2020.

Denning D 'Statement of Dorothy E. Denning before the United State Congress's House Armed Service Committee' (2000) available at http://www.house.gov/hasc/testimony/106thcongress/00-05-23denning.htm, accessed on 7 June 2020.

Development of surveillance technology and risk of abuse of economic information, 2.4 available at http://cryptome.org/stoa-r3-5.htm, accessed on 7 June 2020.

Dykstra J 'Seizing electronic evidence from cloud computing environments' (2013) Available at http://www.csee.umbc.edu/-dykstra/Seeizing-Electronic-Evidence-from-Cloud-Computing-Environments.pdf, accessed on 7 June 2020.

Effective Inter-Agency Co-Operation in Fighting Tax Crimes and Other Financial Crimes 3 ed (2017) available at https://www.oecd.org/tax/crime/effective-inter-agency-co-operation-in-fighting-tax-crimes-and-other-financial-crimes-third-edition.pdf, accessed 4 May 2021.

Faisal M 'Uganda's legal and institutional framework in combating cybercrime: A review of Uganda's ICT law new opportunities in the wake of recent enactments, old challenges as to implementation and sensitisation' Kampala International University available at http:// http://rm.coe.int/16802f2349, accessed on 6 June 2020.

Gercke M 'Challenges in developing a legal response to terrorist use of the internet' (2010) *Gabor IKLODY* 37, available at http://www.tmmm.tsk.tr/publication/datr/volumes/datr6.pdf#page=42, accessed on 29 July 2020.

Internet Crime Complaint Centre, 2010: http://pdf.ic3,gov/2010 IC3Report.pdf. Accessed 5 April, 2020.

IP Location available at http://www.iplocation.net/internet, accessed on 27 May 2020

Lewis J A Assessing the risks of cyber terrorism, cyber war and other threats. (Centre for Strategic & International Studies, 2002) available at http://csis.org/files/media/csis/pubs/021101_risks-of_cyberterror.pdf, accessed on 7 June 2020.

List of African Union Convention on Cyber Security and Personal Data Protection. Available at http://au.int/en/treaties/african-union accessed on 23 June 2020.

List of Signatories to Additional Protocol to the Convention on Cybercrime, Concerning acts of a Racist and Xenophobic Nature Committed through Computer Systems available at http://conventions.coe.int/Treaty/Commun/ChercheSig,asp?NT=189&CM=4&DF=&CL=ENG, accessed on14 April 2020.

List of Signatories to Additional Protocol to the Convention on Cybercrime, concerning acts of a Racist and Xenophobic Nature Committed through Computer Systems available at http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT-189&CM-4&DF-&CL-ENG, accessed on 23 June 2020.

Mcafee Inc 'A Good Decade for Cybercrime' (2013) available at http://www.biz-file.com, accessed 2 October 2020.

Morris S 'The Future of Net-crime Now: Part 1 – Threats and Challenges', Home office Online Report 62/04, available at http://www.globalinitiative.net/download/cybercrime/europe-russia/Home%20Office%20-%20The%20future%20of%20netcrime%20now%20-%20Part%201%20%E2%80%93%20threats%20and%20challenge.pdf, accessed on 7 June 2020.

Office Research report 75 available at http://www.justiceacademy.org/ishare/Library-UK/horr75-chap1.pdf accessed on 23 June 2020.

Overview of the Electronic Communications Amendment' Available at http://www.ellipsis.co.za/wp-content/uploads/2014/04/Overview-of-the-Electronic-CommunicationsAmendment-Act-1-of-2014.pdf accessed 27 May 2020.

PWC's Global Economic Crime and Fraud Survey 2020 available at http://pwc.com/gx/en/services/advisory/forensics/economic-crime-survey.html, accessed on 30 June 2020.

Questions and Answers: Mandate for the Second Additional Protocol to the Budapest Convention available at http://europe.eu/rapid/press-release.htm, accessed on 25 April 2020.

Ruwanthika Gunaratne and Public International Law available at https://ruwanthikagunaratne.wordpress.com,2008 accessed 27 September 2020

Sieber U 'Legal Aspects of Computer-Related Crime in the Information Society' (1998) COMCRIME Study, available at http://www.edc.uoc.gr/~panas/PATRA/sieber.pdf, accessed on 9 June 2015.

Singh Poonia A, Bhardwaj A & Dangayach G S 'Cyber Crime: Practices and Policies for Its Prevention' (2011) In The First International Conference on Interdisciplinary Research and Development, Special No. of the International Journal of the Computer, the Internet and Management vol 19, available at https://www.academia.edu/41411512/Meaning_and_Nature_of_Cyber_Crime, accessed on 7 June 2020.

The Cybercrimes Bill is one step away from becoming law, available at http://www.clifffedekkerhofmeyr.com accessed 7 October 2020.

The Ministry of Information and Communications Technology (2011), National Information Security Strategy (NIIS) Final Draft, 2011 available at http://www.nationalsecuritystrategy.org, accessed on 18 September 2020.

The role of Computer emergency team available at http://Ucc.co.ug/cert/, accessed 26 April 2020.

The State of ICT in Uganda (2019) available at https://researchictafrica.net/wp/wp-content/uploads/2019/05/2019_After-Access-The-State-of-ICT-in-Uganda.pdf, accessed on 18 September 2020.

Uganda 2020 Crime & Safety Report available at https://www.osac.gov/Country/Uganda/Content/Detail/Report/972253e2-8a5b-4164-b3c5-18824394519c, accessed May 4 2021.

Uganda acceded to the United Nations' Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography 2002 on 30 November 2001 available at http://indicators.ohchr.org, accessed 27 October 2020.

Uganda Communication Commission (2017) "Report on status internet Users March 2017", available at http://www.internetworldstats.com/af/ug.htm accessed 24 May 2020.

United States The White House, National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, Washington, DC 2003, 6, 47-79 available at http://www.whitehouse.gov/pcipb/physical.html, accessed on 7 June 2020.

Urbas G & Krone T 'Mobile and Wireless Technologies: Security and Risk Factors' (2006) *Australian Institute of Criminology*, available at http://www.aic.gov.au/publications/tandi2/tandi329t.html, accessed 18 September 2020.

Vogel J 'Towards a Global Convention against Cybercrime, First World Conference on Penal law in Guadalajara, Mexico' (2007) available at http://www.penal.org/sites/default/files/files/Guadalajara-Vogel.pdf accessed on 25 May 2020.

Vogel J 'Towards a Global Convention Against Cybercrime, First World Conference on Penal law in Guadalajara, Mexico' (2007) available at http://www.penal.org/sites/default/files/files/Guadalajara-Vogel.pdf, accessed on 25 May 2020.

Wanyama E 'The Upsurge of of cybercrime in Uganda: where the Gaps and Loops lies; Analysis of the Need For Legislative and Policy Framework' available at https://www.academia.edu/8949753/The_Upsurge_of_Cyber_Crime_in_Uganda_Where_the_Gaps_and_Loops_lie_Analysis_of_the_Need_for_Legislative_and_Policy_Framework accessed May 13 2021.

Williams P 'Organised Crime and Cybercrime: Organized Crime and Cybercrime: Synergies, Trends, and Responses' (2001) 6 *An Electronic Journal of the U.S. Department of State* 2 available at http://guangzhou.usembassy-china.org.cn/uploads/images/sqVFYsuZI0LECJTHralS_A/ijge0801.pdf, accessed on 24 April 2020.