Addis Ababa University
School of Graduate Studies

Cybercrime in Ethiopia: Lessons to be learned from International and Regional Experiences

By: Iyasu Teketel

January, 2018
Addis Ababa, Ethiopia

Cybercrime in Ethiopia: Lessons to be learned from International and Regional Experiences

By

Iyasu Teketel

Advisor

Wondmagegn Tadesse (Dr. jur.)

A Thesis Submitted to the School of Graduate Studies of Addis Ababa University in Partial Fulfillment of the Requirements for the Masters of Law (LL.M) in Public International Law Stream

Approval Sheet by the Board of Examiners

Cybercrime in Ethiopia: Lessons to be learned from International and Regional Experiences

Approved by Board of Examiners

_____	_____	_____
Advisor	**Signature**	**Date**
_____	_____	_____
Examiner	**Signature**	**Date**
_____	_____	_____
Examiner	**Signature**	**Date**

DECLARATION

Iyasu Teketel, hereby declare that this research paper is original and has never been presented in any other institution. To the best of my knowledge and belief, I also declare that any information used has been duly acknowledged.

Name: Iyasu Teketel

Signature:

This dissertation has been submitted for examination with my approval as University advisor:

Advisor: Wondmagegn Tadesse (Dr. jur.)

Signature:

Table of Contents

DECLARATION i
ACRONYMS v
Acknowledgment vii
ABSTRACT viii
Chapter One: Introduction and Overview of the Study 1
1.1 Background of the Study 1
1.2 Statement of the Problem 5
1.3 Objective of the study 7
1.4 Research Question 7
1.5 Methodology of the Study 8
1.5.1 Literature Review 8
1.5.2 Interview. 8
1.6 Significance of the Study 9
1.7 Scope and Limitation of the Study 9
1.8 Organization of the Study 10
Chapter Two Theoretical Framework and Literature Review 11
2.1 Introduction 11
2.1.1 Definition of Cybercrime 12
2.1.2 Classification of Cybercrime 14
2.2 Why is Cybercrime being considered as a Problem? 15
2.3 Investigation of Cybercrime 18
2.3.1 Evidence Identification and Tracking 19
2.3.2 Jurisdiction 19
2.3.3 Search and Seizure 20
2.4 Cybercrime and Cyber Liberties 21
2.5 International Cooperation and Enforcement 22
2.6 Social, Economic and Political Impacts of Cybercrime 22
Chapter Three International and Regional Experience: The Council of Europe Convention on Cybercrime and AU Convention on Cyber Security and Personal Data Protection 24
3.1 Introduction 24
3.2 The Council of Europe Convention on Cybercrime 24

3.2.1 Background 24
3.2.2 Organization of the Convention 25
3.3 The African Union and Cyber Security 28
3.3.1 Introduction 28
3.3.2 Institutional Hollowness 30
3.3.3 African Union Convention on Cyber Security and Personal Data Protection 31
3.3.4 Sub-regional efforts 34
3.3.5 AU Convention vs. the Council of Europe Convention on Cybercrime 35
3.3.5.1 Offenses against the Integrity of Computer System 36
3.3.5.2 Misuse of Devices 37
3.3.5.3 Computer Related Offences 38
3.3.5.4 Content Related Offenses 39
3.3.5.5 Point of difference between the two Conventions 39
3.3.5.6 Gaps in the AU Convention 42
3.6 The way forward 43
Chapter Four: Cybercrime in Ethiopia 46
4.1 Introduction 46
4.2 Institutional Setup 49
4.2.1 Ministry of Communication and Information Technology 49
4.2.2 Information Network Security Agency 49
4.2.3 Federal Police Commission 50
4.2.4 The National Intelligence and Security Service 52
4.3 The Policy Framework 53
4.3.1 The National Information and Communication Technology (ICT) Policy and Strategy 2009 53
4.3.2 The Criminal Justice Policy 54
4.4 The Legal Framework 54
4.4.1 The Criminal Code 54
4.4.2 The Computer Crime Proclamation 55
Chapter Five Conclusion and Recommendation 62
5.1 Conclusion 62
5.2 Recommendation 63

5.2.1 Concerning International and Regional Agreements 63
5.2.2 Concerning the Federal Police Cybercrime Unit 64
5.2.3 Concerning the Computer Crime Proclamation 64
Bibliography 66

ACRONYMS

ARPANET	Advanced Research Project Agency Network
AU	African Union
AUCCSPDP	African Union Convention Cyber Security and Personal Data Protection
CDPC	Council of Europe's Committee on Crime Problems
CERTs	Computer Emergency Response Team
CMC	Computer Mediated Communications
COMESA	Common Market for Eastern and Southern Africa
CSA	Ethiopian Statistics Agency
CSIRTs	Computer Security Incidents Response Teams
DoS	Denial of Service
EAC	East African Community
ECOWAS	Economic Community of West African States
EU	European Union
FBI	Federal Bureau of Investigation
FDRE	Federal Democratic Republic of Ethiopia
GS	Global South
GTP	Growth and Transformation Plan
ICT	Information and Communication Technology
INSA	Information Network Security Agency

ISP	Internet Service Provider
LDCs	Least Developed Countries
MCIT	Ministry of Communication and Technology
MLAT	Mutual Legal Assistance Treaties
NGOs	Non-Governmental Organizations
NISS	National Intelligence and Security Service
PDAs	Personal Digital Assistants
RECs	Regional Economic Communities
SADC	Southern African Development Community
UN	United Nations
UNECA	United Nations Economic Commission for Africa
WMD	Weapons of Mass Destruction

Acknowledgment

No words could properly acknowledge the amount of gratitude I owe for so many people. First and for most I would like to express my gratitude and everlasting zeal and dedication for the almighty God Jehovah! Secondly I would like to extend my warmest appreciation and gratitude for my Advisor Dr. Wondmagegn Tadesse without whom this work is unimaginable, thank you sir for all your dedication, patience and kindness, I don't have enough words to express how grateful I am for everything you have done for me. I am also great full for all the workers of the Federal Police Commission with whom I had interaction with on the course of my research, especially for Chief Sargent Dagne Negash and Chief Sargent Degu Fayisa.

Next I would like to say thank you to all my family members who has supported me and encouraged me in my endeavors in life. My dad Teketel Alemayehu, my mom Bekelu Kuma, my aunts Nigist and Lemlem, my brothers japi and jc and sisters weli, suna, and shena, THANK YOU ALL!

I would like to extend my special thanks to my friends; Israel Begashaw, thank you for believing in me more than I believe in myself and encouraging me to peruse my dreams, Bruke Paulos, thank you for all the time you spent on me and for being a true friend. Ruth Mekach, I am indebted for all the things you have done for me all these years, and Mintesenot Kindyihun, thank you for making my life in Addis enjoyable. Samuel Taye, thank you for your friendship and dedication, I am indebted to you all.

Lastly I would like to declare this work to be in memory of the sweetest person to ever walk the planet, my grandmother, Enayiye and my cousin and dear friend Ashe who passed away so soon!

ABSTRACT

The world has never been more connected as it is now. The number of computers that are interconnected outnumbers the number of people living on the planet. Technology is expanding fast in every corner of the globe and as a result cybercrime has become the necessary evil states have to deal with if they are to reap the benefits of being interconnected. Cybercrime is no longer the problem of the developed world only, as more and more people in the developing world including the Least Developed Countries (LDCs) are longing online every day. As countries expand their infrastructure, especially in the field of ICT, their vulnerability to attacks through the cyberspace also increase.

Ethiopia is not an exception to this fact, in the past decade or so it has engaged in vast expansion of telecom infrastructure throughout the country and owing to such expansion, the number of people having access to the internet has risen from a mere couple of thousands in to millions. Different institutions are now relying on the internet to deliver their services including banks, airlines and different sectors of the government. Unfortunately the expansion in the infrastructure has not been matched with equal investment in the fields of security and adequate legislation to govern the area. Ethiopia is among countries that are increasingly becoming victims of cybercrime in Africa and until very recently it did not even have adequate legislation to govern the matter.

There is a universal consensus concerning cybercrime as an increasing threat to the world population as a whole and individual efforts cannot yield the desired results in this interconnected world. Hence various efforts have been introduced collectively at the international as well as regional level that are relevant for countries like Ethiopia to be a part of or gather experience from and this paper tries to analyze such experience in light of the situation in Ethiopia.

The paper gives due emphasis on two efforts by the Council of Europe and the African Union as they are the most relevant both in the international arena and vis-à-vis Ethiopia. It assesses the various features the instruments have and discuss the steps taken by Ethiopia to harmonize its legislation in accordance with such instruments.

As a country that is just opening its eyes to the problem of cybercrime, Ethiopia has a lot to learn from international experience and be part of international efforts aimed at averting or mitigating the risks to cybercrime. The paper will at the end indicate the gaps the Ethiopian legal system has in this regard and the way forward so as to be as safe as possible when it comes to cybercrime

Chapter One: Introduction and Overview of the Study

1.1 Background of the Study

The world has never been more connected as it is right now. Things that used to be considered as 'impossible' just a few decades ago are now possible. Even the war front is now changing from an actual battle field in to the unnoticeable electronic world where everything is done through the internet in the Cyberspace. This has been possible as a result of internet connection, which has linked the world from the smallest island in the pacific to the big cities of Europe and America throughout Asia and Africa. Today the technology is ubiquitous and increasingly easy to use, ensuring its availability to both offenders and victims.[1]

In less than two decades, the internet has grown from a curiosity to an essential element of modern life for millions of people across the globe and in addition to socio-economic development the internet has enhanced the capabilities of human interaction.[2]

Now the technology is penetrating the deepest jungles of Africa as more and more people are connected to the internet each year. Internet penetration is rapidly growing in the world, and the rate at which it is growing in Africa is above the international standard,[3] between the years 2000-2015, global internet penetration grew 7 fold from 6.5% to 43%.[4] Ethiopia is not an exception to this. In fact the speed of development that has been witnessed in the past couple of years, even if it is at its infant stage, is staggering. Currently, basic telecom infrastructure is in place, to most of the geographic area of the country and 57% of the geographic area has 3G network coverage.[5] Nowadays different service providers throughout the country are reliant more and more on

[1] Jonathan Clough, Principles of Cybercrime, (2010), p.5
[2] Mohamed Chawki, Ashraf Darwish, Mohamed Ayoub Khan, Sapna Tyagi, Cybercrime, Digital Forensics and Jurisdiction, (2015), p.3
[3] Nir Kshetri, Cybercrime and Cybersecurity in the Global South, (2013), P.153

[4] ITU facts and figures 2015, available at www.itu.int/net/press_releses/2015/17.aspx
[5] Mesifin Belachew, Investment in Broadband Infrastructure in Ethiopia, available at http://unohrlls.org/custom-content/uploads/2017/03/presentation-on-BB-in-Ethiopia.pdf

internet connections in order to run a smooth service for their clients. The number of people that conduct their day to day activity through internet is also increasing rapidly.[6]

However such expansion of infrastructure is not without associated risks. A recent survey made to identify the vulnerability of institutions in Ethiopia to cybercrime has concluded that 'cybercrime is a legitimate problem in the country'[7], given the fact that there is no or very little institutional set up in place to avert or mitigate the problem and the society is new to the technology. A number of government entities and ministries at the federal level, including Ethiopian Statistic Agency (CSA) and regional bureaus' websites have been hacked repeatedly by foreign hackers.[8]The number of attacks and their sources is increasing by the day as more criminals are finding it easy to attack third world countries that have no or little protection but a growing internet penetration and naïve users.

The technology has made life easier for so many portions of the world society and proving its value in the overall development of the global economy. However, the technology is a gift in disguise; as it has a number of risks associated with it apart from the obvious benefits ripped as a result of being interconnected. In other words, the ever-improving communications backbone has provided great benefits to human kind, but it has also provided faster speed to criminals.[9]

The risk of being globally connected has brought a number of hurdles to nations across the globe as it is very difficult and complicated to deal with investigating and bringing to justice a criminal that is half way across the globe. In short, Mohamed, a renowned writer on the field, has put it in his book *Cybercrime, Digital Forensics and Jurisdiction,* Computer networks have done for criminals what they have done for legitimate computer users: they have done the job easier and more convenient.[10]

The development in technology has made it possible for criminals to commit sophisticated crimes. Nowadays criminals do not have to physically carry weapons and walk in to banks or

[6] Halefom Hailu, The State of Cybercrime Governance in Ethiopia,(2015), p. 6

[7] Id., p.8

[8]Kinfe Micheal Yilma, "Developments in Cybercrime Law and Practice in Ethiopia," Journal of Computer Law & Security Review (2014) p. 726, available at www.seciencedirect.com

[9]Will Gragido, Daniel Molina John Pric, Nick Selby, Blackhatonomics An Inside Look at the Economics of Cybercrime, (2013) p.36

[10]Mohamed Chawki and others, cited above at note 2, p.16

other institutions to rob money, they could simply do it from the basement of their homes using a computer. The internet by its nature enables action from a distance. Criminals no longer need to gain physical access to a particular location, as they can access electronic systems from anywhere in the world.[11]

Hence internet has made it possible for a new location for committing a crime, which otherwise would have been committed by physically being present in the area, the cyber space. As a result, many of the fraudulent activities that used to be committed in the face to face world interaction are now being shifted to a new location.[12] The US Secret Service has called credit card fraud the bank robbery of the future.[13] Therefore, the internet has introduced new locations and techniques of committing crimes that are more complicated and devastating than the traditional crimes.

Computers are responsible (directly or indirectly) for every aspects of our life, starting from the operation of our cars to our personal banking and to the flow of data in our business; with the essential rise in the legitimate use of computers, it follows that there would be an inevitable increase in their illegitimate use.[14]

Cybercrime is one of the fastest growing areas of crime; more and more criminals are exploiting the speed, convenience and anonymity that the modern technologies offer in order to commit a diverse range of criminal activities.[15] At present given its rate of expansion so far, it is unlikely that it will decelerate anytime soon.

The ever increasing volume of cyber-attack that is not checked by national boundaries need the cooperation of national and international law enforcements, governments, public and private sector of each country.[16] The use of domestic legislation to target cybercrime offenders is necessary but it cannot by itself be sufficient to solve the problem. Due to the diversity of laws of different countries, an action that is deemed illegal in one country could be legal in the other, even if both countries are victims of an attack. Beside there could be the issue of jurisdictional conflict, both positive and negative. Moreover when it comes to cybercrime the concept of

[11]Majid Yar, Cybercrime and Society, (2006) p.54
[12]George Curtis, The Law of Cybercrimes and Their Investigation, (2012) p.105
[13]Nir Kshetri, The Global Cybercrime Industry, Economic, Institutional and Strategic Perspectives, (2010) P.2
[14]James R. Richards, Transnational Criminal Organizations, Cybercrime and Money Laundering, *A Handbook for Law Enforcement Officers,(*1999) p. 88
[15]Mohamed Chawki and others, cited above at note 2, p.7
[16] Id., p.20

jurisdiction fades away as it is not clear what constitutes a jurisdiction: weather it is the place of the act, the country of residence of the perpetrator, the location of the effect, or the nationality of the owner of the computer that is under investigation or all these at once?[17] A lack of cross-border collaboration in cybercrime investigations, international heterogeneity in cybercrime laws, and the weakness and even non-existence of such laws in some countries have facilitated the globalization of cybercrimes.[18]

The problem of cybercrime has been felt across the globe as it affects the life's of millions of people every day, if not more, and the need to deal with the ever growing problem has prompted different efforts to be undertaken in the International, Regional as well as National level. However owing to different factors, the response to the problem is not always that effective as perpetrators find new ways whenever their methods are discovered. These brought about an international consensus that a single effort by a nation could not solve the problem, rather it need the combined efforts of all to address the problem.

With this understanding there are efforts at international and regional level to work together in the area of cybercrime. Accordingly, at international level there are various efforts by the United Nations[19]and the European Union[20] to legislate on the issue. The Council of Europe Convention on Cybercrime, though a regional effort, is open for all countries to accede and hence is considered as the most comprehensive legislation on cybercrime at international level.[21] On regional level, the African Union[22] has enacted a convention on the issue and there are various efforts to have a common consensus and cooperation among nations to work together in order to combat the problem. There are also efforts at sub regional level in Africa to bring about consensus and combat the problem. Unfortunately, Ethiopia is not a party to any of such international and regional efforts and until very recently its laws lack comprehensiveness and depth on the issue as they are scattered on different pieces of legislations that were primarily meant to govern other issues.

[17] Ibid.
[18]Nir Kshetri, cited above at note 13, p.45
[19]General Assembly Resolution 45/121, Prevention of Crime and the Treatment of Offenders, A/RES/45/121 (14 December 1990) available from undocs.org/a/RES/45/121.General Assembly Resolution 55/63, combating the criminal misuse of information technologies, A/RES/56/121 (23 January 2002) available from undocs.org/A/RES/56/63.(see also resolutions No.56/121, No.57/239, No. 58/199)
[20]Council of Europe Convention on Cybercrime 2001(ETS No.185)
[21]Jonathan Clough, cited above at note 1, p.22
[22]AU Convention on Cybersecurity and Personal Data Protection

1.2 Statement of the Problem

Many factors contribute for a cybercrime to be among the main challenges Ethiopia has to face in the twenty first century. The first problem when it comes to cybercrime is the issue of definition. There is no consensus among countries as to what exactly encompasses a cybercrime[23] and in the absence of such consensus it will be difficult to set out what exactly constitutes a cybercrime and legislate on the matter.

Secondly the increasing level of internet infrastructure development in the country coupled with inadequately skilled users (including individuals, businesses, and the government) makes Ethiopia a fertile target for cybercriminals. The risk of being a potential target of cybercrime is increasing by the day in the country as more and more people are going online every day owing to expansion of infrastructures in different parts of the country.[24] According to recent a report, Ethio Telecom claims that it has become the largest telecom operator in Africa with 57.34 million mobile subscriptions in 2017.[25]The number of mobile subscription in the country has shown a steady growth in the past ten years, for instance, it has risen from 6.5 million in 2009/10 to 40 million in 2014/15; the number of internet users has increased from 187,000 to 3.7 million in the same time interval.[26]According to ITU facts, by the end of 2016, mobile subscriptions per 100 persons in the country are 50.5 and individuals using the internet are 15.4 out of 100 persons.[27] With roughly a population of 100 million, this would mean that there were around 50.4 million mobile users and 15.4 million internet users in Ethiopia by the end of 2016.

Besides different institutions are increasingly relying on the internet in order to function properly and deliver services to their customers even if the stage of development is still low compared to other countries. Financial institutions are on the fore front of this list,[28] and hence millions of birr is being circulated online, though cash is still the most dominant medium of exchange[29], and that

[23]Nir Kshetri, cited above at note 3, p.13
[24]Haleform Hailu, cited above at note 6, p.4
[25]www.ethiotelecom.et
[26]National Bank of Ethiopia, Annual Report 2014/15, p.24, available at http://www.nbebank.com/pdf/annualbulletin/Annual%20Report%202014-15/Annual%20Report%202014-15.pdf, last accessed on September 16, 2017
[27] ITU Facts &Figures, Available at: https://www.itu.int/net4/itu-/icteye/CountryProfileReport.aspx?countryID=77, last accessed on September 16, 2017
[28] Gardachew Worku, Electronic-Banking in Ethiopia- Practices, Opportunities and Challenges, Journal of Internet Banking and Commerce, vol. 15, no.2,(August 2010), p. 5
[29]Haleform Hailu, cited above at note 6, p. 6

is fertile target for cybercriminals. Most of the users of internet in the country are new to the technology and that could be described as naïve users compared to the more experienced hackers that use different complicated techniques to cheat their victims. Hence they could easily be defrauded and become victims without even knowing what they did wrong.

Thirdly, the existing laws that deal with cybercrime in Ethiopia are not sufficient to cover the nascent forms of cybercrimes and they do not provide severe punishment so as to deter cybercriminals.[30] One of the deterrence factors when it comes to cybercrime is the availability of a strong legal frame work to effectively prosecute potential cybercriminals. The absence of such strong legal system actually serves as an incentive for cybercriminals as they could gain so much while they put themselves at a minimal risk. In short, as Nir Kshetri, who has written a number of books on the subject, describes it, 'weak law and permissive regulatory regimes provide a fertile ground for cybercrime activity.'[31]

Fourthly the law enforcement agencies including the police, the prosecutors and judges are new to the concept of cybercrime and do not have the necessary skills and tactics to deal with cybercrime investigation and prosecution.[32] Until very recently, even the laws dealing with cybercrime were scattered in different legislations that were primarily meant to govern other aspects and were far from being adequate.[33] In 2016, a new proclamation has been enacted to govern the area. According to the interview the researcher conducted with a public prosecutor in Federal Attorney General Administration of Criminal and Civil Justice office, as of yet, no prosecution has been made using the new proclamation. However, there is still a long way ahead for Ethiopia as a country to minimize its vulnerability to cybercrime.

[30]Molalign Asmare, "Computer Crimes in Ethiopia: An Appraisal of the Legal Framework," International Journal of Social Science and Humanities Research. , vol. 3,(2015), P. 103
[31]Nir Kshetri, cited above at note 3, pp. 12-13
[32]Haleform Hailu, cited above at note 6, p. 14
[33] The criminal code has four articles dealing with the issue (articles 706-709), the National Payment System Proclamation No. 718/2011, the Registration of Vital Events and National Identity Card Proclamation No.760/2012 and the Telecom Fraud Proclamation No.761/2012 are the other piece of legislations that have articles with some implications to cybercrime.

1.3 Objective of the study

The study discusses and attempts to identify the problems related with the Ethiopian cyber legal regime as a whole. Along this line, the overall objective is to analyze the international and regional experiences with particular emphasis on efforts by the European Union and African Union and gather possible lessons the Ethiopian legal system could learn from such systems. In the process of analyzing the relevant issues, attempt is made to achieve the following interrelated specific objectives:

1.3.1 To discuss the Features of international frameworks dealing with cybercrime at international, regional and sub-regional level.

1.3.2 To assess the AU Convention in light of the Council of Europe Convention critically.

1.3.3 To provide an overview for understanding cybercrime particularly in the context of the Ethiopian legal regime.

1.3.4 To assess the institutional and legal framework to combat cybercrime in Ethiopia.

1.3.5 To discuss variation in the international and regional efforts to combat cybercrime and point out a way forward for Ethiopia

1.3.6 To pinpoint the major lessons and measures that Ethiopia should draw and take from international and regional experiences towards controlling cybercrime.

1.4 Research Question

The research questions of the study are designed in a way that could enable the researcher to answer the above stated objectives of the study. Thus the central question of the study is: what lessons could the Ethiopian cyber legal regime learn from the experiences of international and regional cyber legal regimes on cybercrime control in general? With this general research question, the following interrelated research questions were posed.

1.4.1 What are the basic features of international frameworks that deal with the problem of cybercrime?

1.4.2 What are the features and significance of the African regional and sub-regional cybercrime control legal regime to effectively deal with the problem?

1.4.3 What are the variations found in International and regional efforts and what should Ethiopia do in this regard?

1.4.4 What are the gaps in the existing laws against cybercrime in Ethiopia?

1.4.5 What are the lessons that Ethiopia should learn from international and regional experiences and what measures should it take to tackle cybercrimes?

These interrelated research questions are asked in line with the objectives and will be answered under different chapters.

1.5 Methodology of the Study

Given explorative nature of the research questions, the study has employed a qualitative research methodology. The paper employs a doctrinal method for the most part, and in order to achieve the study objectives, both primary and secondary data have been used. Under the primary sources, international conventions, regional and sub-regional conventions and bills as well as domestic laws were consulted.

On the secondary sources, the paper has given emphasis on the analysis of the relevant available literatures on the subject. In relation to literature, the researcher has specifically relied on examining books, academic articles, which have relevance to the study. In addition, various internet sites have been consulted for relevant data and information. In line with these the paper employs the following methods:

1.5.1 **Literature Review.** An attempt has been made to evaluate materials; both soft copy and hard copy that are relevant to the issue at hand and that could give insight in to the trend that is currently being followed by entities whose experience is being investigated under this thesis. The various steps taken by such institutions and the reasons behind doing so as well as their relevance to the Ethiopian legal system were evaluated.

1.5.2 **Interview.** An interview has been conducted with the Federal Police Commission Cybercrime unit to examine the current status of the unit, the practical challenges associated with investigating and prosecuting cybercrimes as well as the reality of cybercrime in Ethiopia. The entire Cybercrime Unit is composed of four people and an interview has been conducted with two of them. Chief Sargent Dagne Negash and Chief Sargent Degu Fayisa are chief investigators in the unit with a reach experience as they are part of the founding members of the unit in 2012.The participants of the interview were

randomly selected as all members of the unit are of the same qualification and sex. The researcher used semi structured interview questions so as to allow the researcher to follow up on issues raised by the interviewees. Furthermore an interview has also been conducted with the Office of the Attorney General as they are the main actors dealing with the issue directly. The cyber division within the Attorney General is on the processes of being organized and hence the researcher was only able to conduct an interview with one public prosecutor that is currently working on the first case to the unit. All the interviewees have been told in advance what the researcher is working on the issues he hopes to address in his research. All were eager to answer the questions honestly and to the best of their knowledge.

1.6 Significance of the Study

Cybercrime is a new field of study, not just in Ethiopia, but elsewhere in the world. Even if the stage of development is different, it is safe to say that every country in the world is still trying to come up with ways both legal and technical to fully address the issue. In this regard, owing to the lack of legislation on the part of the Ethiopian legislature, until very recently, a lot has not been written on the issue.

There are some articles that address the point but either they deal with provisions of the Criminal Code on the cybercrime, or they focus on a draft proclamation that has been enacted now with major deviation from the draft and they are too narrow in scope. Hence, this thesis will give insight on the current structure of the Ethiopian legal regime, serve as an insight for policy makers in identifying the gaps in our legal system and formulating lessons from other international entities and could serve as a base for further researches on the point.

1.7 Scope and Limitation of the Study

The study tries to analyze lessons that could be learned from regional and international experiences, and hence covers legislative efforts by entities like the Council of Europe and the AU. It also tries to examine the current shape of the Ethiopian legal system on cybercrime. As such the scope of the paper is limited to the Council of Europe Convention on Cybercrime, AU Convention on Cyber Security and Personal Data Protection, sub regional efforts in the African continent and their implications to the Ethiopian legal system and measures to be taken by Ethiopia.

In terms of limitations, both the issue of cybercrime and cybercrime legislations are relatively new to Ethiopia and hence there are no bulks of literatures that could be consulted with respect to Ethiopia on the matter. Moreover the researcher was unable to find any decided court cases on the issue; hence no court cases are analyzed in the paper. Lastly Multiple efforts by the researcher to conduct an interview in Information Network Security Agency (hereinafter INSA) both in person and via the telephone has been unsuccessful. The researcher has gone in person to the Head office of INSA and has submitted a letter of collaboration from the School of Law intended for this purpose. More over multiple telephone calls has been made to the Agency as per their request to follow up on my application which was futile. I have also tried to contact people who work for the Agency through a friend and was turned down. The researcher has made use of the Agency's website to gather as much information as possible but was unable gather firsthand information about the practice on the ground as INSA is the main organ that deals with the issue of cybercrime.

1.8 Organization of the Study

As described above, the thesis tries to analyze lessons that could be learned by Ethiopia in the fields of cybercrime from regional and international experiences as well as the measure it should take in order to effectively protect its citizens from cybercrime. To this end, the thesis is divided in to five chapters. Chapter One deals with introduction and overview of the study. Chapter two deals with theoretical framework as well as literature review and gives a brief explanation of historical, conceptual and factual analysis of issues related with cybercrime that are relevant for issues explained in the subsequent chapters.

Chapter Three discusses the international and regional experience with due emphasis on efforts by the Council of Europe and the African Union and sub-regional efforts, specifically the Council of Europe Convention on Cybercrime, and AU Convention on Cyber Security and Personal Data Protection. Chapter Four deals with cybercrime in Ethiopia in relation to the experience gathered under the previous chapters. As such it examines the Proclamation on Cybercrime and various legislations that deal indirectly with cybercrime and evaluate them in line with findings under the previous chapters. Finally, Chapter five by way of conclusion forwards measures that should be taken to ensure cyber security in the country without infringing other right of citizens.

Chapter Two Theoretical Framework and Literature Review

2.1 Introduction

An examination of cybercrime should be anchored in an examination of the history of internet as the latter is the tool that makes cybercrime possible in the first place. According to Majid, 'the internet as its name suggests, is in essence a computer network; or to be more precise, a network of networks.'[34] The origin of the internet could be traced back to the 1960s ARPANET (Advanced Research Project Agency Network), which was a development of networks sponsored by the US military, as a possible solution for a feared missile attack by the Soviet Union that could cripple the telecommunication network of the US thereby making communications difficult.[35] Efforts to develop it further were undertaken in the decades that followed but a huge breakthrough was achieved in the 1990s when the government released the ARPANET to civilian control.[36]

The 1990s also saw the development of different browsers that make it possible to access the internet; starting form the first web browser, Nexus which was introduced in 1992, to NCSA Mosaic in 1993, Internet Explorer in 1995 and Opera in 1996[37] they made accessing the internet easier and each development has brought new features that made it popular among the users. By the end of the twentieth century, more than 400 million people around the world were connected using the internet, which grew to 3.2 billion by the end of 2015 and half of the world's population is expected to be online by the end of 2017.[38]

The history of crime dates back to the earliest known history of human beings on earth, while the history of cybercrime only dates back a few decades. For instance the first computer crime statue in the United States was enacted in 1984, The Counterfeit Access Devise and Computer Fraud and Abuse Law.[39] This act made it a crime to 'knowingly access computers without

---

[34] Majid Yar, cited above at note 11, p.7

[35] Available at www.history.com/topics/inventions/invention-of-the-internet, last accessed on May 10, 2017, 10:21 am

[36] Majid Yar, cited above at note 11, p.7

[37] The Telegraph, 2 May 2015,available at: http://www.telegraph.co.uk/tecnology/microsoft/11577364/Web-browsers-a-brief-history.html, last accessed on May 10, 2017, 10:21 am

[38] ITU Facts &Figures, Available at: https://www.itu.int/net4/itu-/icteye/CountryProfileReport.aspx?countryID=77, last accessed on September 16, 2017

[39] George Curtis, cited above at note 12, p.3

authorization, obtaining unauthorized information with intent of defraud, or cause damage to protected computers'[40]

Since then a lot of efforts worldwide has been undertaken by states that resulted in a bulk of legislations around the world. However, in the case of cybercrime, the law has experienced difficulty in keeping peace with advances in technology.[41] And hence there is a room for improvement in terms of actions to be taken by each state worldwide whether collectively or individually, and the need will only be greater in the case of Ethiopia as the concept remains alien for many portion of the society including law enforcement agencies.

2.1.1 Definition of Cybercrime

It is difficult to define the concept of cybercrime with absolute certainty as there is no universally agreed upon definition for the term. Different scholars have pondered around the idea of defining the term, but all acknowledge the difficulty associated with doing so. A definition that is too broad would make the term obsolete and hence difficult to apply where as a too narrow definition could restrict the scope of application and allow free riders. Owing to this fact, the conceptual definition of cybercrime varies considerably across survey and studies with regard to their clarity, comprehensiveness and currency.[42]

Most scholars and instruments on the cybercrime either try to give the term a working definition or stipulate the scope of the term under their articles or instrument. For instance the definition given by the US Department of Justice which states "any violation of criminal law that involves the knowledge of computer technology for its perpetration, investigation or prosecution" is criticized for being too wide because under this definition virtually any crime has a possibility of becoming a cybercrime.[43]The fact that many jurisdictions define the term differently also contributes for the over complication of the effort to define the term and the absence of any hard and fast rule to do so.[44]

[40] Majid Yar, cited above at note 11, p.40
[41]George Curtis, cited above at note 10, p.3
[42]Nir Kshetri, cited above at note 13, p.3
[43]Mohamed Chawki and others, cited above at note 2, p.4
[44] Ibid.

Mohamed, a prominent writer on the area, defines the term generally as "unlawful act wherein the computer is either a tool or target or both.*"*[45]Hence according to this definition a criminal activity that involves computer either as an instrument, target or means of perpetuating a further crime comes within the ambit of cybercrime.

There is also a disagreement between scholars as to the exact meaning and definition of the term cybercrime and other related words like *Computer Crimes*, *E-Crimes* and *Internet Crime*. When some scholars identify a difference for instance, between cybercrime and computer crime, others simply use them interchangeably. For instance, George Curtis in his book titled *The Law of Cybercrimes and Their Investigation* quote Parker and state that he "agrees by the distinction made by Parker[46] which stipulates computer crime as 'a crime in which the perpetrator uses a special knowledge about the computer technology'" whereas the cybercrime does not necessary require such knowledge.[47]

On the other hand there are scholars like Haleform Hailu[48] and Molalign Asmare[49]who propagate as the words have the same definitions and hence could be used interchangeably. In addition to these, Mohamed[50] has also used the words interchangeably. Their choice to do so has been summarized by Igor who stated **"**Without an agreed definition of cybercrime, the term 'cybercrime', 'computer crime' 'computer related crime' 'high-tech crime' are often used interchangeably*"*[51] It is interesting to note that Black's Law Dictionary defines cybercrimes as computer crimes.[52] On the other hand the Encyclopedia of Cybercrime stipulates "Cybercrime is a broad term covering all the ways in which computers and other types of portable electronic devices such as cell phones and Personal Digital Assistants (PDAs) capable of connecting to the internet are used to break laws and cause harm."[53](Generally speaking, the term "cybercrime" includes various offenses: offenses related to the misuse of data and computer systems (hacking); the forgeries and frauds committed by the use of a computer (phishing); offenses regarding the

[45] Id., p. 3
[46] Parker Donn.,Fighting Computer Crime: A New Framework for Protecting Information, (1998) p.72 cited by George Curtis at note 12 above, note 4.
[47]George Curtis, cited above at note 10, p. xii
[48]Haleform Hailu, cited above at note 6, p.3
[49]Molalign Asmare, cited above at note 30, P. 93
[50] Mohamed Chawki and others, cited above at note 2, P. 3
[51]I Igor Bernik, Cybercrime and Cyberwarfare, (2014) p., p.3
[52] Bryan A. Garner (ed.) Black's Law Dictionary,(9*th ed.,2011) p.443*
[53] Samuel C. McQuade III, (ed.) Encyclopedia of Cybercrime, (2009), p. 43

redistribution of unauthorized content (dissemination of child pornography) and computer infringement including distribution of pirated content).[54]

Unsurprisingly the definition of cybercrime varies dramatically across countries, religions and culture.[55]For instance web contents that are considered to be obscene in Arab countries are socially acceptable in the western world and at the same time an "obscene" website in the UK could be acceptable in the Scandinavian countries.[56]

In line with the above discussion the researcher chooses to use the terms interchangeably. The researcher chooses to do so because the use of the terms interchangeably does not affect the core issue the research meant to address. Beside the Ethiopian legal system as it will be discussed later on uses the term interchangeably. In fact the proclamation is also called a Computer Crime Proclamation.

2.1.2 Classification of Cybercrime

Different scholars classify cybercrime using different parameters. For instance Majid classifies it based on the involvement of computer or the role played by the internet, whether it has a mare assistant role or whether it is absolutely necessary for the commission of the crime.[57] Accordingly, he identifies computer assisted crimes (those crimes that pre date the internet but which take on a new life in cyberspace e.g. fraud, theft, money laundering, sexual harassment, hate speech, and pornography) and computer focused crimes (those crimes that have emerged in tandem with the establishment of the internet and could not exist apart from it. for example, hacking, viral attack, and website defacement)[58]

According to Parker, Generally cybercrime could be classified in to four categories based on the role the computer plays; which are object, subject, tools and symbols.[59] They become the object when they are stolen or damaged as part of commission of a crime, like theft and destruction of property. They will be subjects when they are the environment within which the crime is committed, like a virus attack using a computer. They will be tools if they enable the criminal to

[54]Igor Bernik, cited above at note 51, p.12
[55]Nir Kshetri, cited above at note 3, p.13
[56]Nir Kshetri, cited above at note 13, p. 3
[57]Majid Yar, cited above, at note 11, p. 10
[58] Ibid.
[59]Mohamed Chawki and others , cited above at note 2, p. 4

produce false information or plan. Finally they will be symbols if they are used to deceive victims, like when their capacity is over exaggerated as if they are super computers capable of doing things that could not be accomplished using a simple computer.[60]

On the other line of the spectrum Nir's classification uses different methods. First considering whether they were targeted or opportunistic; secondly based on whether they are predatory or market based and thirdly taking in to account the relative role of humans and technology element. (Weather mainly human or technology element is there?)[61]

The debate whether cybercrime is a novel crime or a continuation of old crimes in a new technique is an ongoing one. Some argue that cybercrime is pretty much the same as 'old fashioned' non-virtual crime, like 'an old wine in a new bottle' whereas others argue that it is a new form of crime that is radically different from the kinds of real world crimes that predate it.[62]In this regard the researcher is of the opinion that it is pretty much the same forms of crime but in a different spectrum and using different and somewhat sophisticated techniques. As the supporter of the 'new crime' line of argument like to point out, the medium in which the crime is committed, cyber space, is different than that of the space 'ordinary crimes' are committed in. However, the fact that the method used is different does not change the end result or the rights affected in any way. For instance crimes like hacking, phishing, hate speeches and the like affect the same rights as those of theft, fraud, deception, defamation and the like. Therefore, cybercrimes are old crimes that are committed in a new spectrum and which speed up the time and perhaps the level of harm done to such interest.

2.2 Why is Cybercrime being considered as a Problem?

Crime follows opportunity: virtually every advance has been accompanied by a corresponding niche to be exploited for criminal purposes.[63] Advancement in technology especially in the field of information communication or the internet is not an exception to this. True such advancement has made life easier for millions of people across the globe, but it has also increased the risk of vulnerability of such people and made many of them victims of one or more forms of cybercrime.

[60] Ibid.
[61]Nir Kshetri, cited above at note 13, p.11
[62]Majid Yar, cited above at note 11, p.11
[63]Igor Bernik, cited above at note 51, p. 20s

For instance, the development in the digital world in taking and sharing of pictures is exploited by child pornographers; electronic banking and online sales create room for fraud; electronic communications and the social media could be used for stalking and harassment; and the ease in sharing digital media has created a room for copyright infringement.[64] The list goes on as every development in the area creates an opportunity for exploiters to take advantage of.

Three factors contribute for the structural uniqueness of cybercrimes: technology and skill intensiveness, a higher degree of globalization than conventional crimes and the newness of the crime itself.[65] Compared to other ordinary crimes, cybercrimes need the utilization of technology and high level of skill or know how of the technology. On the other hand compared to other conventional crimes that are committed close to home, cybercrimes are not bared by distance or boundaries as they could be committed internationally. Accordingly advances in technology that connects us to work, family and entertainment have created nefarious and dangerous underlying capabilities that are concealed and repeatable from almost anywhere on earth.[66]

The fact that the crime is relatively new compared to other crimes has brought about a number of hurdles. First of all authorities across the world are relatively inexperienced to deal with the problem. Some argue that it is a great time to be a cybercriminal: not only have the laws of most countries not yet caught up with the technology (let alone the crime), but the politics of creating cybercrime laws are mired in a power struggle between agencies in single country and are stuck in absolute greed lock when more than one country is involved.[67]Secondly, legal systems governing the area are not well developed yet and there are a number of countries who do not have any laws at all. In fact, in those countries which have legislations dealing with the matter, no law maker understands the subject matter well enough to argue very effectively for or against anything yet.[68]Thirdly, there is lack of previously developed mechanisms and established codes, policies and procedures.[69]

[64]Mohamed Chawki and others, cited above at note 2, p. 4
[65]Nir Kshetri, cited above at note 13, p. 35
[66]Will Gragido, cited above at note 9, p. 36
[67] Id., p. 2
[68] Ibid.
[69]Nir Kshetri, cited above at note 13, p. 36

The development of Cyberspace, which is "the realm of computerized interaction and exchanges, seems to offer a vast range of new opportunities for criminal and deviant activities."[70] Businesses cite threats to economic performance and stability ranging from vandalism to e-fraud and piracy; governments' talk of 'cyberwarfare'[71] and 'cyberterror'[72] especially in the wake of September 11 attacks.

On the other hand, "The ability of the potential offender to target individuals and property is seemingly amplified by the internet as Computer Mediated Communications (hereinafter CMC) enables a single individual to reach, interact with and affect thousands of individual at the same time."[73] In short, today's criminals can cut across time and proximity, with blinding efficiency.[74]

Hence the technology is at the stage where an individual with minimal resource could potentially generate huge negative effect such as mass distribution of email scams and distribution of virus. In short it could be concluded that "the internet turns actors with relatively small numbers and limited financial and material resource in to what have been called 'empowered small agents.'"[75]

No doubt cybercrime rate is increasing by the minute and it is costing states a fortune every year. According to a new report published by Cyber Security Ventures, in the year 2015, cybercrime has cost the global economy over $3 trillion and this figure is expected to double by the year 2021.[76] The victims of cybercrime are reluctant to report their losses due to different reasons. Victims could lose a lot from reporting a crime than they lose from the crime itself. Embarrassment and negative publicity, lengthy and time consuming trials that divert key experts out of their jobs and exposure of vulnerability are some of the reasons people choose not to report incidents most of the time.[77]

---

[70] Majid Yar, cited above at note 11, p. 3

[71] Cyber warfare in all its definition's include defensive action apart from offensive actions and it is not necessary politically motivated.(George, cited above at note 10,p. 29)

[72] Cyberterror or Cyber terrorism has been defined as 'the execution of a surprise attack by a subnational foreign terrorist group or individuals with domestic political agenda using computer technology and the internet to cripple or disable a nation's electronic and physical infrastructures. (Majid Yar Cited above at note 9, p. 51)

[73] Majid Yar, cited above at note 11, p. 11

[74] Will Gragido, cited above at note 9, p. 36

[75] Majid Yar, cited above at note 11, p. 39

[76] https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016

[77] Nir Kshetri, cited above at note 13, p 42

The techniques used for committing of a crime in cyberspace are becoming increasingly sophisticated as cybercriminals collaborate with a growing number of educated people who cannot get appropriate employment or adequate payment for their work.[78]

There are also other contributing factors for the exponential increase of cybercrime. As the technology is growing in a very fast rate, it makes it possible for tools that could bypass securities to be easily available. Such tools makes it possible for a wide range of people to become potential offenders, even for the people who have minimal know how of the technology.[79] Beside compared to other crimes, cybercrime could be committed with smaller investment in various locations without any constraints of geographical locations and international borders.[80] This coupled with the fact that the lack of public's awareness of the cybercrime has made it possible for cybercriminals to take advantage of the user's ignorance.[81] In fact, most abuses occur due to the ignorance or indifference of people who use computers connected to the internet, for they mostly deal with information resources unconscientiously.[82]Because a large number of users have very limited knowledge of how the technology works and the potential danger of cyberspace, and are at the same time, naïve enough and wish to earn or progress quickly, the testing ground for cybercriminals is practically endless.[83]Some location based services and posts in social media about future travel planes are like Times Square-sized billboards that says, 'I am not home, please come and rob me blind.'[84]Because many users recklessly publish many items of their personal data online on a daily basis, they are faced with the risk that these data will be misused.[85]

2.3 Investigation of Cybercrime

Due to the advancement of technology and the associated use of sophisticated methods by cybercriminals, investigating cybercrime is both demanding and time consuming.[86] As time goes by **"**Cybercrime perpetrators are becoming more experienced every day and use a number of techniques that are relatively unknown, which forces defenses to always be one step behind the

[78]Igor Bernik, cited above at note 51, p. 4
[79]Mohamed Chawki and others, cited above at note 2, p.10
[80] Ibid.
[81]Nir Kshetri, cited above at note 13, p.42
[82]Igor Bernik, cited above at note 51, p 3
[83] Id., p.4
[84]Will Gragido, cited above at note 9, p. 36
[85]Igor Bernik, cited above at note 51, p. 8
[86] Id., p. 37

attackers.*"*[87]The website on which they carry out their unlawful activities (dissemination of child pornography, illegal sale of copyrighted works etc.) are usually placed on servers in countries with inadequate laws, no international agreements and with less qualified law enforcement authorities.[88]

The good news is that Just as cybercriminals exploits new technologies for bad, so can law enforcement and world governments use the same technologies to capture and/or monitor wanted individuals.[89]However the phase at which the law enforcement and authorities are coping up with the problem is not the same as the phase at which criminals are inventing new ways to evade responsibility.

2.3.1 Evidence Identification and Tracking

The dynamic and distributed nature of cyberspace makes it difficult to find and collect all the relevant digital evidences of cybercrimes, as the data could be spread across cities, states or even countries.[90] Offenders make it more difficult to find them as usually they use encrypted messages and invisibility futures. Moreover, almost all cyber offenders are concerned about their identities and hence use identity concealing technology or communicate anonymously.[91]

The internet makes it possible for cybercriminals to communicate globally while they stay anonymous and at the same time, they will be able to "communicate directly and safely,[which] opens the way to knowledge, generate a large number of victims and gives plethora of opportunities and assistances for carrying out illegal transaction."[92] Hence it is a challenge for law enforcement agencies to keep up with cybercriminals and effectively investigate and prosecute them.

2.3.2 Jurisdiction

Prosecuting a cybercrime presents a unique challenge as the crime could be committed from any part of the world against victims residing in different part of the world. According to a European Report "computer crimes are committed across the cyber space and don't stop at the

[87] Id., p. 8
[88] Id., p. 39
[89]Will Gragido, cited above at note 9, p.37
[90]Mohamed Chawki and others, cited above at note 2, p.20
[91] Id., p.21
[92]Igor Bernik, cited above at note 51, p. 10

conventional state borders. They can be perpetrated from anywhere and against any computer user in the world."[93] In fact some forms of attacks are so easy they could be committed by minors. In one instance a 13 year old hacker has used denial of service attack to shut down a computer company.[94]

Thus, national boundaries have created serious obstacles to law enforcement agencies as the cooperation between different law enforcement agencies is far from sufficient[95]whereas the cybercriminals knows how to exploit such gaps. The ever increasing volume of cyber-attack that is not checked by national boundaries need the cooperation of national and international law enforcements, governments, public and private sector of each country.[96] The use of domestic legislation to target cybercrime offenders is necessary but it is not sufficient to solve the problem by itself.

Due to diversity of laws of different countries, an action that is deemed illegal in one country could be legal in the other, even if both countries are victims of an attack. Besides there could arise jurisdictional conflict, both positive and negative.[97] Moreover when it comes to cybercrime the concept of jurisdiction fades away as it is not clear what constitute a jurisdiction: as controversial, to say the least, whether it is the place of the act, the country of residence of the perpetrator, the location of the effect, or the nationality of the owner of the computer that is under attack, or all these at once?[98]In this regard the best way out would be to have an international agreement which address the issue precisely and enable parties to work together.

2.3.3 Search and Seizure

At some point in every cybercrime investigation, the investigator will need to obtain evidence of a crime. Most of the time the investigator needs to search a work place, home or other physical location for digital evidence and seize a computer or other devices, removing it to a forensic lab and analyzing the device in search of evidence."[99] Hence in order to do his job effectively, the

[93]Mohamed Chawki and others, cited above at note 2, p.8
[94]Ibid.
[95]Nir Kshetri, cited above at note 12, p.44
[96]Mohamed Chawki and others, cited above at note 2, p. 20
[97] Ibid.
[98] Ibid.
[99]George Curtis, cite above at note 12, p. 174

investigator needs to know the law regarding search and seizure clearly and there should be clearly defined set of rules in this regard as well.

Anonymity and pseudonymity in this respect demonstrate the rights of individuals to privacy, while at the same time highlight the conflict of interests between the individual and society, since the abuse is the price that the society has to pay in order to preserve benefits.[100] Therefore a clearly stipulated sets of rules to be followed by the investigator that are in line with International and national Fundamental Human Right standards are a must so that any grievance on the part of an individual could be resolved while at the same time protecting interest of the society.

2.4 Cybercrime and Cyber Liberties

Regulation and monitoring of the internet in order to control crime raises a number of problems and a series dilemma. The tension between surveillance and monitoring of online activities on the one hand and the need to protect user's privacy and confidentiality on the other hand is ever increasing by the day.[101] The law enforcement agencies need to monitor online activity in order to effectively prevent crimes and punish criminals whenever such incident happens. However the advancement of technology has made their jobs even more difficult as the criminals could use privacy enhancing technologies that could hide their identities. "Consequently, the imperative for criminal justice actors is to reduce the potential abuse of internet privacy by greater surveillance and monitoring of peoples activities, which inevitably invades the privacy and confidentiality of online communications."[102]

While authorities move towards greater monitoring in order to tackle organized criminals, terrorists, pedophiles, stalkers, and so on, civil-libertarians encourage users to evade such invasions of privacy by making greater recourse to privacy-enhancing tools.[103]Law enforcement agencies such as the police forces and public prosecutors are inexperienced with the new technologies and are not well equipped to deal with global nature of cybercrime. According to

[100]Igor Bernik, cited above at note 51, p. 22
[101] Majid Yar, cited above at note 9, p. 140
[102]Ibid.
[103]Ibid.

Nir Kshetri, a renowned scholar on the area, law enforcement is presently 5 to 10 years behind the global crime curve in relation to technological capability.[104]

2.5 International Cooperation and Enforcement

As the forgoing discussion discloses, no state, no matter how advanced in both technology and economy it is, could single handedly resolve or minimize cybercrime and potential exposure of its citizens to such attacks, unless it totally cuts of internet connections with the rest of the world. Hence cooperation among states and their respective agencies is of a paramount importance in this regard. There are three essential methods of international cooperation: informal, letters rogatory and treaties. By informal we mean direct contact and cooperation between law enforcement colleagues of different countries who know each other or trust each other."[105] This form of cooperation is the most effective one but owing to different reasons such cooperation is not that flourished among states and hence in default of such mechanisms, states are forced to resort to formal legal arrangements.

The term letter rogatory traditionally refers to a request from a court in one country to a court in another country that a witness be examined in the requested country upon interrogatories (questions) forwarded by the questioning court.[106] Mutual Legal Assistance Treaties are treaties that contain provisions enabling one country to request the collection of evidence or apprehension of a suspect from law enforcement officials in another country.[107]

2.6 Social, Economic and Political Impacts of Cybercrime

The actual number of cyber-attacks is not known as not all cyber-attacks are reported to the authorities as discussed above there are a number of reasons for doing so. However when it comes to the exact figures there are two types of arguments; one stating that the figure is underreported for reasons discussed above, such as fear of loss of good will, and public trust whereas the other claims that security companies exaggerate the level of cybercrime as they have a vested interest in doing so.[108] As a result, it is not surprising to find estimates that vary so

[104]Nir Kshetri, cited above at note 13, p. 40
[105]George Curtis, cite above at note 12, p. 368
[106]Ibid.
[107] Ibid.
[108]Nir Kshetri, cited above at note 13, p. 4

much. For instance, recent estimated regarding the size of cybercrime industry varies from US $100 billion to US $1 trillion.[109]

Cybercrime has various social impacts that affect different section of the society. According to one study, 20-25% of young people have been victims of cyber bullying.[110] "According to a survey conducted by University of Calgay's Rozsa Centre, the average citizen is more likely to be victim of cybercrime than that of physical" in the US.[111]Entire infrastructures including those of emergency service call centers, electricity, communications, dams, air traffic control and transportation, commercial databases and information systems for financial institutions and health care providers, and military applications are vulnerable to attacks by cyber terrorists or hostile state actors.[112] For instance, the FBI has ranked cybercrime as the third biggest threat to US national security after nuclear war and weapons of mass destruction.[113] A single wave of cyber-attacks on US infrastructure could exceed US $700 billion, which is about the same as the costs associated with 50 major hurricanes.[114]

An estimate suggests that more than 2 million malicious programs such as viruses, worms, and Trojans were created in 2007, which increased to more than 20 million in 2008.[115]Experts also predict possible increase in cyber-attacks targeting new mobile technologies and Wi-Fi enabled devices.[116] The fact that many consumers have weak technological and behavioral defenses against cybercriminals makes them vulnerable to such crimes.[117]

In order to tackle the problem of cybercrime, governments across the world have created various agencies and they have devoted resources to strengthen regulative institutions and enacted different laws to govern the area.[118] There are also efforts taken to work together in order to effectively address the problem, both at the international arena and regional level. Such efforts and the subsequent legislation as a result of such efforts will be discussed in the next chapter

[109] Ibid.
[110] Id., p. 5
[111] Id., p. 6
[112] Ibid.
[113]Ibid.
[114] Id., p. 7
[115] Id., p. 9
[116]Ibid.
[117] Id., p. 15
[118]Ibid.

Chapter Three International and Regional Experience: The Council of Europe Convention on Cybercrime and AU Convention on Cyber Security and Personal Data Protection

3.1 Introduction

Cybercrime is an international issue that requires an international solution if states are to effectively address the issue and mitigate its effect. Apart from domestic legislations on the issue, cooperation at the international arena will bring about stake holders together and enable the parties to work together towards the same goal. The primary forum where states will engage in such cooperation, the United Nations, has initiated efforts to enact legislation on cybercrime. However, so far such efforts have not been translated into a concrete Convention on cybercrime. Surprisingly, the Council of Europe Convention on Cybercrime, (hereinafter CoE Convention) which was initially meant to be a Regional Convention, has addressed the issue of cybercrime comprehensively and enjoyed wider international acceptance. As such non EU members were participants in its negotiation and it has become open to all nations to be part of, once it was adopted.

The African Union also has adopted a Convention on Cyber Security and Personal Data Protection (hereinafter AU Convention) that is meant to address the issue of cybercrime, among other things. This chapter will examine the features of both Conventions dealing with issues which are pillars for a cyber-legislation and critically examine the AU Convention in light of the European Councils Convention and discuss the rationales behind African Union's decision to adopt a regional Convention instead of simply resorting to CoE Convention. Moreover, it will discuss the implications of both Conventions to the Ethiopian legal system.

3.2 The Council of Europe Convention on Cybercrime

3.2.1 Background

In November 1996, the Council of Europe's Committee on Crime Problems (CDPC) began studying a proposed Convention on Cybercrime.[119] Five years later the complete convention was open for initial signature by initiating nations in November 23, 2001 in Budapest, Hungary and has entered in to force on July 1, 2004.

[119]Explanatory Report to The Council of Europe Convention on Cybercrime 2001, (ETS No.185), (herein after Explanatory Report) para.7

The Convention is the first international treaty on crimes committed via the internet and other computer networks, dealing particularly with infringements of copyright, computer related fraud and violation of network security.[120] As of August, 2017, 55 states have signed and ratified and acceded to the Convention, while further 4 states had signed the convention but not ratified it yet.[121] Australia, Canada, Chile, Dominican Republic, Israel, Japan, Mauritius, Panama, Senegal, South Africa, Sri Lanka, Tonga and United States of America are so far the non-EU Council members that have either signed and ratified the Convention or acceded to it. All in all, over 130 countries are using the convention as framework to develop their cybercrime related regulative institutions[122]

3.2.2 Organization of the Convention

The Convention is organized under four chapters that have a number of titles within them, dealing with substantive, procedural and international cooperation issues. Chapter I is Use of terms, Chapter II measures to be taken at domestic level- (substantive law, procedural law and Jurisdiction) Chapter III International cooperation and Chapter IV Final Clauses

Chapter I of the Convention deals with use of terms; as such it provides meaning of technical terms that are used under the Convention and provide their scope. The definitions given under this chapter need not be copied *verbatim* in to the domestic laws of each state so long as the overall principles of the Convention are not contradicted.[123]As such the Convention provides definition for terms like *Computer System*[124]*Computer Data*[125]*Service Provider*[126] and *Traffic data.*[127]

Chapter II generally deals with measures to be taken at the national level and as such State parties to the Convention undertake that they will carry out the prosecution of all offenses

http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=KDnvg84D) last acceded on 8/21/17

[121]https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=iAketJ2M
[122]Nir Kshetri, cited above at note 13, p.19
[123] Explanatory Report, *Convention on Cybercrime, part III*, para.22
[124]Council of Europe Convention on Cybercrime, 2001 (ETS No. 185), [herein after Convention on Cybercrimes], *chapter I*, art 1(a)
[125]Id., art 1(b)
[126]Id.,, art 1(c)
[127]Id.,, art 1(d)

defined in the second chapter of the Convention on their territory.[128] As discussed above, Chapter II contains three sections: Substantive criminal law (articles 2-13) Procedural law (Articles 14-21) and Jurisdiction (article 22)

Chapter III starts by providing an equivalent of extradition treaty between two countries that do not already have such an agreement, for offenses listed under the convention.[129]It contains provisions concerning traditional and computer crime-related mutual assistance as well as extradition rules. It covers traditional mutual assistance in two situations: where no legal basis (treaty, reciprocal legislation, etc.) exists between parties-in which case its provisions apply- and where such a basis exist- in which case the existing arrangements also apply to assist under the Convention. The rest of Chapter III lists and describes in detail the types of actions that make up Mutual Legal Assistance Treaties (MLAT) and how participating countries are obliged to incorporate them in to their domestic laws.

International cooperation covered by Chapter III of the convention is one of the biggest achievement of the Convention as it lay out the details on how states parties to the Convention could effectively work together in order to respond to one of the greatest threats of the twenty first century that is felt by all. Due to the anonymity and geographical vagueness of countries, law enforcement authorities are often faced with the limitation of their powers, which usually, in the absence of relevant international agreements, prevent them from effectively prosecuting and arresting cybercrime offenders.[130] This portion of the Convention aims at abolishing such barriers for the effective investigation and prosecution of cybercrime around the world.

The final article of substance requires each party to designate a point of contact available on a twenty-four-hour, seven-day-a-week basis, to provide immediate investigative or procedural assistance.[131]Chapter IV deals with the final provisions including the rules of accession and the territorial application of the convention.

[128]Id., art 2-22
[129]Id.,, art 24
[130]Igor Bernik,cited above at note 51,p52.
[131] Convention on Cybercrimes, *chapter III, Section 2,* art 35

A protocol "Concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems" was drafted and opened for signature on January 28, 2003 and entered into force on March 1, 2006.[132]

The Convention on Cybercrime and the Additional Protocol may serve as a model for a broader use of international agreements against cybercrimes; there may be questions concerning privacy, the security of commercial data, and the cost of complying with information request from law enforcement, but the idea of expanding the reach of international law to combat cybercrimes must be seriously examined and if possible, implemented.

The Convention on Cybercrime is the most comprehensive international treaty yet to define, prevent and prosecute cybercrimes.[133] One of the goals of the Convention is to harmonize laws against cybercrime by achieving a greater unity among the signatories.[134] In so doing, the *Convention principally aims at;*

> *'(1) harmonizing the domestic criminal substantive law elements of offences and connected provisions in the area of cybercrime (2) providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic from (3) setting up fast and effective regime of international co-operation.'*[135]

It also aims to ensure police forces and investigators in individual countries follow a standard evidence gathering techniques and promote the use of latest technology for tracking and catching cybercriminals.[136] Hence, generally, the Convention aims at creating common policy for state parties which would protect society against cybercrime, including the adoption of appropriate national legislation and fostering international cooperation.[137] In doing so the Convention aims to meet this goals with due respect to human rights in the new information society.[138]

Cybercrime is an international issue that is a concern for all states of the world irrespective of their economic development or geographical location. An effort that was started to be a Regional

[132] Samuel C. McQuade III, (ed.), cited above at note 53, p.32
[133] Id.,, p.35
[134]Convention on Cybercrimes, preamble, para. 2.
[135]Explanatory Report, *Convention on Cybercrime, part III, para.* 16
[136] Nir Kshetri, cited above at note 13, p. 19.
[137]Igor Bernik, cited above at note 51, p. 50
[138] Explanatory Report, *Convention on Cybercrime, part I*, para. 6

Convention has thus developed in to an international consensus precisely owing to this fact. Most of the major economies of the world has in one way or the other taken part in this international effort and has set up a mechanism whereby the issue could be governed and states easily cooperate in order to effectively prosecute and govern the area of cybercrime. Therefore, owing to its wide acceptance by the international community either in the form of taking part in the Convention by being signatory or subsequent ratification or taking it as a model to legislate domestic laws, the CoE Convention is cited as the most comprehensive international treaty to address the issue of cybercrime like no other.[139]Owing to this fact, it has laid down minimum standards that should be followed while legislating on cybercrime and such standard could help countries around the world, including Ethiopia, in their endeavors to keep up the ever increasing complicated problems of cybercrime and its governance.

3.3 The African Union and Cyber Security

3.3.1 Introduction

Africa is set to be the new frontiers of cybercrime in the world. Three reasons are forwarded by experts as a justification for this. Africa is poised to become a new cybercrime harbor because of availability of fast internet access, the expanding internet user base, and the lack of cybercrime laws in some African countries.[140]

The advancement in technology and the falling cost of such technologies has facilitated the rapid digitalization of economies in Africa. In the past, one of the reasons why computers in developed part of the world were attractive target for cybercriminals is because they are always online; whereas African networks were not that attractive for cybercriminals because of low connectivity of the region and low broadband penetration.[141]However this fact is changing and it is changing fast in Africa.

The newly launched submarine cables in east and west Africa has made it possible for a faster internet connection trough out the continent and now the continent enjoys almost a full cable

[139] Samuel C. McQuade III, cited above at note 53, p.35
[140]Loucif Kharouni, Africa A new Safe Harbor for Cybercriminals?, 2013, , p.1, available at:http://www.trendmicro.nl/media/misc/africa-new-safe-harbor-for-criminals-en.pdf
[141]Nir Kshetri, cited above at note 13, p.169.

coverage owing to infrastructure developments in all corners of the continent.[142]Such fast digitalization of the continent is good news for cybercriminals and hence the numbers of cybercrimes are growing faster in Africa compared to the rest of the world.[143]In 2016, the continent has lost an estimated $2billion for cybercrime where the lions share is taken by Nigeria which lost around $550 million.[144]Analysts are concerned about the danger associated with the potential cybercrime explosion from the Global South (GS) with its increased digitalization and some has gone as far as strongly arguing that Africa's "Cyber WMD" potentially poses a direct threat to the world.[145]If African policy makers fail to address this concern, there will be negative impact on economic growth, foreign investment and security.[146]

Internet penetration is growing exponentially around the world and especially in Africa[147]Mobile phone penetration is rapidly increasing in Africa, as of April 2017, there are 960 million mobile subscriptions across Africa, an 80 percent penetration among the continents population and internet penetration is at 18 percent with 218 million internet users.[148]

With the expansion of mobile phones in the continent, associate technologies are being created and utilized that involve some kinds of vulnerability to cyber-attacks. For instance in Eastern African countries, mobile payment, are becoming so popular. According to The Economist, M-PESA, a mobile-phone-based money service that allows people to deposit, withdraw and transfer money, is the most successful scheme of its type on earth with 25% of the Kenyan gross national product flowing through it.[149]Hence an emerging threat that is particularly salient is the increasing vulnerability of mobile devices such as smart phones and tablets, as more and more people relay on mobile technologies; cybercriminals are developing their strategies to exploit

[142]Loucif Kharouni, cited above at note 140, p.2
[143]Nir Kshetri, cited above at note 3, 152
[144] Kenya Cyber Security Report 2016, p. 10, available at:http://www.serianu.com/downloads/KenyaCyberSecurityReport2016.pdf
[145]Nir Kshetri, cited above at note 3, p.12
[146]Eric Tamarkin, Cybercrime A Complex Problem Requiring a Multi-Faceted Response, Institute for Security Studies Policy Brief, p. 1, available at: http://www.fiels.ethz.ch/isn/177499/Polrief51Feb14.pdf
[147] Ibid.
[148] Available at: http://allafrica.com/stories/201704251054.html
[149] Available at: https://www.economist.com/blogs/economist-explains/2013/05/economist-explains-18

cybersecurity gabs.[150]Mobile money on Kenya has experienced numerous attacks through social engineering, use of malware and account Personification.[151]

East Africa got its first fiber optics submarine cable in June 2009 and this has made it possible for better connection and penetration across the region. Following such expansion, countries in the region have witnessed an increase amount of cybercrimes that have cost them millions of dollars. Kenya has recorded the highest losses- $171 million, Tanzania lost $85 million while Uganda has lost $35 million in 2016[152]

3.3.2 Institutional Hollowness

Generally speaking, digitalization in the global south is characterized by hollowness,[153]and this statement is particularly true when it comes to Africa. Hollowness is related to the lack of capacity to manage risks and vulnerabilities; technological, behavioral and policy related factors has contributed to the hollowness.[154]

Cybersecurity policies in most of Sub Saharan African (SSA) economies are developed in a random and haphazard manner without giving series thought and hence the gap between 'law on the books' and 'law in action' is substantial.[155] Most of the time, even if they have the laws and regulation on paper, it will be meaningless unless they have the means, capacity and the will to enforce them, which is not the case often.

There are figures that show the hollowness of African digitalization. For instance, according to a recent survey by the World Bank suggests that over 80 per cent of Sub Saharan Africa **(**SSA**)** lacks basic knowledge of information technology.[156]Most people access internet in such countries via internet cafes, which are unable to afford anti-virus systems and hence most of the computers are affected by viruses and worms which increase the risk to cyberattacks.

---

[150]Eric Tamarkin, cited above at note 146, p.11
[151] Kenya Cyber Security Report, cited above at note 144, p.11
[152] Available at: https://www.standardmedia.co.ke/business/article/2001235820/kenya-worest-hit-in-east-africa-by-cyber-crime last accessed on November 15/ 2017 3:00 pm

[153]Nir Kshetri, cited above at note 3, p.153
[154] Ibid.
[155] Id., p.160
[156] Id.,159

Most economies across the continent are characterized by an absence of laws that criminalize cybercrimes and serious deficiency in enforcement means, tools to investigate and prosecute such crimes, a lack of mechanisms to share information and scarcity of international collaboration.[157]

3.3.3 African Union Convention on Cyber Security and Personal Data Protection

3.3.3.1 Background

With all the current rapid expansion of infrastructures related to ICTs and the related vulnerability to cybercrime that comes with it, the AU has acknowledged that cybercrime is one of the biggest problems Africa has to face going to the twenty first century. As such, it has enacted a convention on cyber security and Personal data protection which was adopted on June 2014. As of November 2017, nine countries have signed the convention and only one has ratified it.[158]

3.3.3.2 Overview of the Convention

As the name of the Convention stresses, the Convention is not a typical cybercrime Convention like that of the Council of Europe Convention on Cybercrime, rather it tries to address a wide range of issues including Personal Electronic Transactions, Personal Data Protection and Cyber governance.

The Convention is part of a commitment of African countries at sub regional, regional and international level to build an information society.[159] From the start it acknowledges the protection of fundamental freedoms and human and people's rights contained in different declarations, conventions and international instruments that are adopted within the frame work of the AU and the UN.[160] The Convention sets the security rules essential for establishing a

[157] Ibid.,152

[158] http://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection,
Benin, Chad, Congo, Ghana, Guinea-Bissau, Mauritania, Sierra Leon, Sao Tome & Principe, Zambia has signed the Convention whereas Senegal is the only country that has ratified it so far.

[159] African Union Convention Cyber Security and Personal Data Protection, EX.CL/846(XXV) [Hereinafter AU Convention on Cyber Security], preamble, para. 2

[160] Id., para. 4.

credible digital space for electronic transactions, personal data protection and combating cybercrimes.[161]

Among other things, the aim of the Convention is to address the need for harmonized legislation in the area of cyber security in member states,[162] and it acknowledges that cybercrime poses 'a real threat to the security of computer networks and the development of the information society in Africa.'[163]

In terms of substantive criminal law, the Convention seeks to modernize instruments for the repression of cybercrime by formulating a policy for the adoption of new offense specific to ICTS, whereas in terms of criminal procedural law, it defines the framework for the adaptation of standard proceedings concerning information and telecommunication technologies and spells out the conditions for instituting proceedings specific to cybercrime.[164]

Article 1 of the Convention stipulates definition for key terms used in the Convention. However, Key definitions relating to procedural powers such as "*Service Provider*", "Traffic Data", and "*Subscribers Information*" are missing from the Convention. These concepts are essential for defining specific procedural powers to secure such data for criminal justice purposes.[165]

The first chapter of the Convention deals generally with Electronic transactions and discusses issues like *scope of applications of electronics in commerce,*[166] *contractual liability,*[167] and *advertising by electronic means,*[168]*contractual obligation in electronic form,*[169]*security of electronic transactions,*[170]

Chapter two of the Convention deals with Personal data protection. As such it stipulates the *Objectives of the Convention with respect to personal data protection,*[171]*Scope of*

[161]Id., para. 8.
[162]Id., para. 13
[163]Id., para. 15
[164]Id., para 16 & 17
[165] Zahid Jamil, Comparative Analysis of the Malabo Convention of the African Union and the Budapest Convention on Cybercrime(2016) p.4 available at www.coe.int/en/web/cybercrime/-/malabo-and-budapest-convention-towards-complementarity
[166] AU Convention on Cyber Security, art 2
[167]Id., art 3
[168]Id., art 4
[169]Id., art 5&6
[170]Id., art 7
[171]Id., art 8

applications,[172]*Preliminary personal data processing formalities,*[173]*Institutional framework for the protection of personal data,*[174]*Obligations relating to conditions governing personal data processing,*[175]*and The data subjects rights.*[176] (Article 16-23)

3.3.3.3 Cybercrime and the AU Convention

Chapter III of the Convention is the relevant portion of the convention to this paper as it addresses the issue of promoting cyber security and combating cybercrime.

Section 1 of the chapter discusses Cyber Security measures to be taken at national level. Article 24 stipulates national cyber security framework under *National policy*[177] and *National strategy.*[178] As such countries have the obligation to develop national cyber security policy and implement the policy.

As per the stipulation of article 25, countries are bound to adopt legislations and/or regulatory measures against criminal offences that affect the *integrity, confidentiality, availability and survival of ICTs.* Countries also have the duty to confer specific responsibility on institutions, either newly established or preexisting and on their officials a statutory authority and legal capacity to act in all aspects of cybersecurity application. But in doing so states should ensure that such measures do not infringe on the rights of citizens guaranteed under national regional and international Human right instruments; specifically the basic rights such as *freedom of expression, the right to privacy and the right to a fair hearing* among others.[179]

Each state party has also undertaken to promote the culture of cyber security among all stake holders namely, government, enterprises and the civil society, which develop, own, manage, operationalize and use information systems and networks.[180] The role of the government is to provide leadership for the development of the cyber security culture within its borders. And

[172]Id.,, art 9
[173]Id., art 10
[174]Id., art 11&12
[175]Id., art 13-15
[176]Id., art16-23
[177]Id., art 24(1)
[178]Id., art 24(2)
[179]Id., art 25(3)
[180]Id., art 26(1)

public-private partnership is the model to be engaged for the promotion and enhancement of a culture of cyber security.[181]

All member countries are bound to establish an appropriate institution responsible for cybersecurity governance,[182] doing so includes establishing a clear accountability in the matters of cyber security be defining the roles and responsibilities in a clear term,[183] and is able to respond to perceived challenges and all issues related with cyber security.[184]

One of the focuses of the Convention is to avoid double criminality and to this end it provides that states should make sure their efforts in fight against cybercrime could be harmonized regionally[185] and are encouraged to sign mutual assistance treaty if they don't already have one.[186] State parties also have the responsibility of establishing Computer Emergency Response Team (CERTs) or the computer Security Incidents Response Teams (CSIRTs)[187]and to this end states could use the already existing means of international cooperation to respond to cyber threats, improving cyber security and stimulating dialog between stake holders.

3.3.4 Sub-regional efforts

There are multiple Sub regional efforts in the African continent to legislate and bring about trans-national consensus and cooperation on the issue of cybercrime. For instance, East African Community (EAC) has a Draft Legal Framework for Cyberlaws (2008), whereas the Economic Community of West African States (ECOWAS) has enacted a Draft Directive on Fighting Cybercrime (2009),(Supplementary Act A/SA.2/01/10)Cybercrime Directive 1/08/11) and personal protection and personal data (Supplementary Act A/SA.1/01/10) The Common Market for Eastern and Southern Africa (COMESA) also have enacted Cyber Security Draft Model (2011), The Southern African Development Community (SADC) also have a Model Law on Computer Crime and Cybercrime.(2012)

Even if the level of development and the content of the instruments are different, almost all Regional Economic Communities (RECs) are working towards harmonizing their efforts to fight

[181]Id., art 26(3)
[182]Id., art 27(1)(a)
[183]Id., art 27(1)(b)(i)
[184]Id., art 27(1)(b)(ii)
[185]Id., art 28(1)
[186]Id., art 28(2)
[187]Id.,, art 28(3)

cybercrime at sub-regional level. Only the Directive of ECOWAS has a binding force to combat cybercrime as they are made part of the constitutive act of the ECOWAS but the others could still serve as reference for countries wishing to legislate on the area.

The East African Community was the first sub-regional economic organization to accept cyber law framework. According to this framework, the concept of cybersecurity in Africa is divided in to two phases, the first covers electronic transaction, electronic signatures and identification, cybercrime, data protection and privacy; the second covers intellectual property, competition, electronic taxation and information security.[188]

With regard to promotion of cooperation on cyber security, sub-regional organizations show more active and more flexible features than the regional organization (AU).[189] The spirit of CoE Convention is already reflected in sub-regional initiatives which increase the possibility of African countries joining the Convention. In fact, COMESA Cybersecurity Draft Model Bill (2011) is considered very detailed in terms of international cooperation and meets all the criteria of the CoE Convention.[190]

However, efforts by the RECs are not free from problems and criticism; rather regional and bilateral cybercrime instrument are criticized for creating a cooperation cluster that is unable to address the global nature of cybercrime.[191]

3.3.5 AU Convention vs. the Council of Europe Convention on Cybercrime

The AU Convention is broader than that of the Council of Europe Convention on Cybercrime in its scope as it addresses issues related to Electronic Transactions, Personal Data Protection as well as Cyber Security and Cybercrime whereas the Council of Europe Convention on Cybercrime mainly address issues related with Cybercrime.

The subsequent discussion will analyze point of consistency and divergence among the two Conventions with regard to offenses at the core of any cyber legislation and examine the effectiveness of the AU Convention on its own and the possible lessons both has to offer to the

[188] Xiao Yingying and Yuan Zhengqing, "A primary exploration on cyber security governance in Africa," China Academic Journal, 2015, p.8
[189] Id., p.14
[190] Id., 16
[191] Eric Tamarkin, , The AU Cybercrime Response, A positive start but substantial challenges ahead, Institute for Security Studies policy brief 73(January 2015), p.6

Ethiopian legal system as instruments of international acceptance (the CoE Convention) and an African Convention that has a probability of being ratified by Ethiopia.

3.3.5.1 Offenses against the Integrity of Computer System

The first issue of substance with regard to cybercrimes that is dealt under both Conventions is Offences *against the confidentiality, integrity and availability of computer data and systems.*[192]They are intended to protect the confidentiality, integrity and availability of computer systems or data and not to criminalize legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices.[193]

The CoE Convention under Article 2 and the AU Convention under article 29(1)(a)-(c) deals with Illegal access which covers 'the basic offence of dangerous threats to and attacks against the security (i.e. the confidentiality, integrity and availability) of computer system and data.[194]Accordingly**, '***access*[195] *to a whole or any part of a computer system'* is made an offence.

The CoE Convention under Article 3 and the AU Convention under article 29(2) (a) talks about Illegal interception and makes it an offence to *'intercept by technical means*[196] *of a non-public transmission of computer data.'* It aims to protect the right of privacy of data communications that are guaranteed under different international human rights instruments.[197]

The CoE Convention under Article 4 and the AU Convention under article 29(1)(e) & (f) deals with Data interference and aims to protect the integrity and proper functioning or use of stored computer data or computer programs. As such, it makes it an offence 'to *damage, deteriorate*[198]*, delete, alter*[199] *and suppress a computer data*'[200] In other words it extends the same type of

---

[192] Convention on Cybercrimes, *chapter II, Section 1*, art 2-8, AU Convention on Cyber Security art 29(1)(2)
[193] Explanatory Report, *Convention on Cybercrime, part III*, para.43
[194] Explanatory Report, *Convention on Cybercrime, part III*, para.44
[195]Access comprises the entering of the whole or any part of a computer system and includes the entering of another computer system, where it is connected via public telecommunication networks, or to a computer system on the same network, such as LAN (local area network) or internet within an organization. (see Explanatory Report, *Convention on Cybercrime, part III*, para.46)
[196]Interception by "technical means" relates to listing to, monitoring or surveillance of the content of communications, to the procuring of the content of data either directly or through access and use of the computer system, or indirectly, through the use of electronic eavesdropping or taping devices. (see Explanatory Report, *Convention on Cybercrime, part III*, para.53)
[197] Explanatory Report, *Convention on Cybercrime, part III*, para. 51
[198]'Damaging' and 'deteriorating' refers to the alteration of computer programs or data whereas deletion is equated with destruction of corporeal things since deletion makes data useless or unrecognizable.
[199]Alteration on the other hand refers to the modification of existing data and would include the addition of viruses, Trojan horse and logic bombes and the like.

protection given to corporeal objects against intentional infliction of damage to compute data and computer programs.[201]

The CoE Convention under Article 5 and the AU Convention under art 29(1)(d), deals with system interference in general and makes '*a series hindrance*[202] *of a computer system* an offense. The purpose of these articles is to criminalize the international sabotage which prevents the lawful use of a computer system, including telecommunication facilities.[203]The protected legal interest is the interest of operators and users of computer or telecommunication systems being able to have them function properly.[204]

3.3.5.2 Misuse of Devices

Misuse of devices under article 6 of The CoE Convention or attack on computer system under art 29(1)(h) of the AU Convention is another form of cybercrime. It is established as a separate and independent criminal offence of the 'production, sale, procurement for use, import, distribution[205] or making available[206] of a devise, including computer programs that are primarily designed or adapted for the purpose of committing crimes stipulated under art 2-5 of the Council of Europe Convention. The commission of these offences often requires the possession of means of access (hacker tools) or other tools, there is a strong incentive to acquire them for criminal purposes which may lead to the creation of a kind of black market in their production and distribution. To combat such dangers more effectively, the criminal law should prohibit specific potentially dangerous acts at the source preceding the commission of offences under article 2-5.[207]

Under the CoE Convention the creation of a virus becomes an offense the same way as the distribution of any virus. Interestingly, even a hyperlink to a virus entails prosecution for

---

[200]Suppressing data means making the data unavailable for legitimate users.
[201]Mohamed Chawki and others, cited above at note 2, p.48
[202]The term "hindering" refers to any and all actions that interfere with the proper functioning of the system. This could be anything from inputting, transmitting, damaging, deleting, alerting or suppressing computer data. (see Explanatory Report, *Convention on Cybercrime, part III*, para.66)
[203]Mohamed Chawki and others, cited above at note 2, p.49
[204] Explanatory Report, *Convention on Cybercrime, part III*, para. 54
[205]Distribution refers to the act of forwarding data to others
[206]Making available refers to the act of making available by the placing of the said devices online for others to download and use. (see Explanatory Report, *Convention on Cybercrime, part III*, para.72)
[207] Explanatory Report, *Convention on Cybercrime, part III*, para. 71

distribution.[208] In other words linking to a material becomes an offense and no one knows where the border stops; a person replying to an anonymous email or browsing nude pictures in the internet could potentially be an offender if the files are infected with viruses even if he actually did not do anything wrong. This area is a grey area where the Convention is open for interpretation and could potentially restrict the freedom of individuals unless states put some distinctions when they incorporate the Convention in to their domestic laws.

3.3.5.3 Computer Related Offences

These are ordinary crimes that are frequently committed through the use of a computer system. Hence this category covers the situation where the computer is used as a tool for commission of a crime. Under this sub title the addressed offences are computer related fraud and forgery.[209]

Computer related forgery is discussed under article 7of the CoE Convention. It is also described as computerized data breach under art 29(2)(b) of the AU Convention. Both stipulations aim at creating a parallel offence to the forgery of a tangible document.[210]It is made an offence to make 'unauthorized creation or alteration of a stored data so that they acquired a different evidentiary value in the course of legal transactions, which relies on the authenticity of information contained in the data.

Article 8 of the CoE Convention and article 29(2)(d) of the AU Convention address computer related fraud, which are becoming more and more common by the day owing to the expansion of technology. These crimes mainly consist of input manipulations, where incorrect data is fed into the computer or by program manipulations and other interference with the course of data processing. The aim of this article is to criminalize any undue manipulations in the course of data processing with the intention to affect an illegal transfer of property.[211]

The computer fraud manipulations are criminalized if they produce a direct economic or possessory loss of another person's property and the perpetrator acted with the intent of producing unlawful economic gain for himself or for another person.[212]

[208]Igor Bernik, cited above at note 51, p.51
[209] Convention on Cybercrimes, *chapter II, Section 1*, art 7 & 8
[210] Explanatory Report, *Convention on Cybercrime, part III*, para. 81
[211]Id., para. 86
[212]Id., para. 88

3.3.5.4 Content Related Offenses

Content related offenses most of the time would mean one thing, offences related to child pornography. Both Conventions address the issue of child pornography in detail and make it an offense using unequivocal terms. Article 9 of the CoE Convention and article 29(3) of the AU Convention addresses the issue. The provisions seeks to strengthen protective measures for children, including their protection against sexual exploitation, by modernizing criminal law provisions to more effectively circumscribe the use of computer systems in the commission of sexual offences against children.[213]

These provisions criminalize various aspects of the '*electronic production, possession, making available*[214]*, transmitting*[215] *and distribution*[216] *of child pornography.'* Most states already criminalize the traditional production and physical distribution of child pornography, but with the ever-increasing use of the internet as the primary instrument for trading such materials, it was strongly felt that specific provisions in an international legal instrument were essential to combat this new form of sexual exploitation and endangerment of children.[217]

Therefore, as the forgoing discussion illustrates, the AU Convention has several provisions that are consistent with the Council of Europe Convention even if the wording and degree of elaboration of the concept is different. In this regard most of the Substantive Criminal provisions of the Council of Europe's Convention are covered by the AU Convention in one way or the other.

3.3.5.5 Point of difference between the two Conventions

The substantive criminal provisions of both Conventions are consistent. However when it comes to the procedural provisions and international cooperation, there is a huge difference in terms of obligations they impose on state parties and the mechanism of enforcement of the Conventions. For instance, almost all offences under the AU Convention are missing appropriate *mens rea*

[213]Id., para. 91
[214]Making available is intended to cover the placing of child pornography on line for the use of others like by means of crating websites.(see Explanatory Report, *Convention on Cybercrime, part III*, para.95)
[215] Transmitting refers to Sending child pornography through a computer system to another person(see Explanatory Report, *Convention on Cybercrime, part III*, para.96)
[216] Distribution is the active dissemination of the material (see Explanatory Report, *Convention on Cybercrime, part III*, para.96)
[217] Explanatory Report, *Convention on Cybercrime, part III*, para. 93

elements and therefore appear to criminalize legitimate conduct of law enforcement authorities and other conduct that should be lawful under international best practices.[218]

For an act to be an offense under the CoE Convention it must be done "*without right"* and it must be "*intentional."* However, the AU Convention provisions do not have the phrase "*without right*" which makes most offences a strict liability offences without any *mens rea* which could apply to conducts that are legal. On the other hand some provisions of the AU Convention provide for fraudulent intent which is a higher requirement than the CoE Convention which stipulates "*without right and intent.*" Hence opening a possibility for acts to be unlawful under the latter to be lawful under the former as one has to prove deceit or deception in case of the provisions of the AU Convention.[219]

With regard to specific provisions that are dealt under both Conventions, the AU Convention lacks most of the procedural aspects that are stipulated under the CoE Convention. As such, it does not include concepts like *Scope of procedural provisions, Conditions and Safeguards, Expedite preservation and partial disclosure of traffic data, real time collection of traffic data* as well as the concept of *Jurisdiction.*

The most important aspect relating to an international or regional instrument in cybercrime is to create a functional framework for criminal justice cooperation between parties, whereas the CoE provides for an effective and fully functional mechanism for international cooperation between state parties, the AU Convention does not have provision dealing with *International Cooperation* except for trans-border access to stored computer data with consent or where publicly available.[220] Hence on its own the AU Convention cannot assist its member states achieve their stated objective of harmonizing cybercrime domestic law and enabling cooperation against cybercrime between parties.[221]

So now, few important questions need to be raised, why did the African Union resort to its own Convention when member countries could simply join the CoE Convention? What are the reasons behind such divergence between the two Conventions? Given the fact that the AU

[218] Zahid Jamil, cited above at not 165, p.4
[219] Ibid.
[220] Ibid.
[221] Ibid.

Convention comes later in time than that of the CoE Convention, why did it omit the procedural and international cooperation part that are the pillars of the later?

An effort to legislate on Cybercrime in the African level has been surrounded by critics before during and after the Convention was enacted. For a longer period of time, before any effort to legislate on the matter was started, Africa was described as a continent in the dark when it comes to cybercrime legislation and that there need to be an effort to legislate on the matter. Once the AU took an initiative to adopt a Convention on it and enacted a draft legislation, it was fiercely criticized especially by Non-Governmental Organizations (NGOs) and Civil Society Organizations as an instrument that repress human rights especially the freedom of speech and the right to privacy.[222] Even after the adoption of the Convention, various criticisms are raised on its contents, especially in its deficiencies that will be discussed later on.

The reasons why the AU resort to its own Convention, instead of encouraging member countries to simply join the Council of Europe Convention could be explained in two ways; First of all reasons why the rest of the word is reluctant to join the Convention could also apply for Africans. Secondly there are also reasons that are peculiar to Africa.

The fact that CoE Convention was prepared by Council of Europe and not the UN and as such not all countries of the world were part of its negotiations has affected some countries' decision not to be part of the Convention.[223]

One of the reasons why many countries did not join the CoE Convention yet has to do with procedural measures stipulated in the Convention. Which would mean that, when a country wants to join the Convention, not only does it needs to amend its Criminal Code but also its Criminal Procedure Code.[224]

On the other hand, when we consider reasons that are specific to Africa, one of the reasons Africans choose to adopt their own Convention instead of just resorting to the Council of Europe Convention has to do with resource allocation. Even if countries have the political will to take a stance against cybercrime, it is often difficult to justify allocating resources for it, when the

[222] Eric Tamarkin, cited above at note 146, p.4
[223] Alexander Seger, The Budapest Convention on Cybercrime 10 years on: Lessons learnt or the web is a web, (2012), p. 5
[224] Ibid.

beneficiaries will not be that of the states' own citizens but those of other countries.[225] This is especially true since the majority of African countries are busy with more pressing issues like poverty, AIDS, energy crisis, political instability, ethnic conflicts, and traditional crimes, there are fewer resources left to combat cybercrime.[226]

The difference in social and legal values of states also plays an important role for Africans to resort to their own Convention instead of joining the Council of Europe Convention. One major issue is that the European Union is known for much stricter privacy laws than that of other countries including that of the United States.[227]On the other hand, Privacy is considered as a foreign culture that is alien to Africans as it has its roots in individualism whereas the African society is perceived to be communal, as such the AU Convention does not provide a comprehensive model frame work to be followed by countries.[228]

When it comes to the omissions by the AU Convention with regard to procedural and international cooperation, it is difficult to conclude with absolute certainty as the Convention does not have an Explanatory Report explaining the justifications why the Conventions chooses to do so. Nor does it set up a body that is responsible for its implementation. However, one of the most important aspects relating to an international or regional instrument in cybercrime is to create a functional framework for criminal justice cooperation between parties.[229]Provisions dealing with procedural and international cooperation are vital in this regard. And it is actually one of the problems associated with the AU Convention.

3.3.5.6 Gaps in the AU Convention

There are a number of problems that could one way or the other affect the effectiveness of the AU Convention. First of all, the scope of the Convention is extremely broad as it encompasses three separate areas that need specific legislations in to one instrument. It was an effort to address all the ICT problems of Africa in one legislation and doing so has made it unnecessarily broad.

---

[225] Mohamed Chawki and others, cited above at note 2, p.116
[226] Xiao Yingying and Yuan Zhengqing, cited above at note 188, p.10
[227] Mohamed Chawki and others, cited above at note 2, p.117
[228]Cynthia Rich, Privacy Laws in Africa and the Middle East, privacy and Security Law Report, 2015, p.3 available at: https://media2.mofo.com/documents/150615bloombergprivacyafricamiddleeast.pdf , last accessed on January 06/ 2018

[229] Zahid Jamil, cited above at not 165, p.4

Secondly, the Convention does not establish a supervisory body at regional level, except for encouraging states to work together and cooperate. Article 32 provides that the AU chairperson is responsible for implementing the Convention but it does not go beyond that, which will be next to impossible for a single person to effectively ensure the implementation of the Convention.

Thirdly, as the scope of the Convention is wide, it is not clear if a state wants to be a party to one of the issue addressed in the Convention without committing to the others. However the possible way out of this lays in reservation as the instrument does not prohibit reservations.

Fourthly, the Convention make use of terms that are broad, in a form of giving discretions to states, such as those *that are deemed necessary*, *appropriate* and *effective*, which are open for interpretation and could be abused by undemocratic African leaders.[230]

Many elements of the AU Convention "transplant" the laws and regulations of Western countries which are beyond the existing law enforcement capacity of the African countries and bring them difficulties to ratify and implement the Convention.

3.6 The way forward

Without the appropriate provisions dealing with procedural law and international cooperation on the mater, the AU Convention could hardly be of any value as an instrument of serving criminal justice in the continent. With all its deficiencies, it is the right step in a crucial direction to avert the problem faced by the continent as a whole, owing to the necessary advancement in ICTs. But the level of enthusiasm shown by African countries, including Ethiopia, to be part of this region-wise effort or any other international effort is worrying and more need to be done both at Regional and Sub-regional level in the continent as the problem of cybercrime does not abide by the artificial boundary line drawn between states.

The provisions of the AU regarding cybercrime are not in conflict with the Council of Europe Convention. However, problems may arise if a country were to implement limited or vague provisions of the AU Convention only.[231] It would be better if countries use the Council of Europe Convention on Cybercrime as model to legislate on their domestic law. Moreover,

[230] For instance see, AU Convention on Cyber Security, art 32
[231] Zahid Jamil, cited above at not 165, p.4

African countries need to cooperate with the authorities of countries in other regions of the world where electronic evidence is often stored or where service providers are located. The most relevant states in this respect are already parties to the Council of Europe Convention, joining this treaty would offer a legal framework for African Countries to engage in cooperation with these countries.[232]

The forgoing discussion in this chapter has pointed out the features of CoE Convention as well as the AU Convention. As the most widely accepted and comprehensive instrument on the area, the CoE Convention has laid down the minimum standards that should be followed by countries while drafting their legislation. A legislation on cybercrime needs to meet a few criteria; first, it should be sufficiently technology neutral so as to enable it to entertain development in the fields of technology, secondly, law enforcement powers must be subject to safeguards to ensure that the rule of law and human rights requirements are met, and finally it must be sufficiently harmonized or compatible with the laws of other countries to permit international cooperation's.[233]

The CoE Convention is formulated while taking these criteria in to consideration. It is enacted in technology neutral terms so as to enable it to encompass technological developments and sixteen years after its adoption, it is still relevant and serving its intended purpose despite technological development in the field.

For any cyber legislation to be effective in prevention and mitigation of the problem, effective procedural rules play a vital role. Clearly stipulated procedural rules not only guarantee the basic human rights of citizens, but they will also enable law enforcement agencies to effectively act within the boundaries provided therein.

The problem of cybercrime is an international one and no single country could single handedly solve the problem irrespective of the size of its economy or its technological advancement. The core for effective investigation and prosecution of cybercrime lays in international cooperation. The CoE Convention lays down detailed rules that could assist member countries in achieving

[232]Ibid.
[233] The state of cybercrime legislation in Africa-an overview, Council of Europe/project cybercrime @octopus ,p.2 available at: https://rm.coe.int/16806b8a79

this goal. The fact that the AU Convention lacks such rules contributes to its ineffectiveness to assist member countries to fight cybercrime on its own.

Sub-regional efforts by different RECs in the continent are moves in the right direction in the fight against cybercrime and a stepping stone for countries to bring about continent wide and international cooperation. The fact that the spirit of the drafts by the RECs is in line with CoE Convention would make it easier for African countries to join the CoE Convention. Doing so would have tremendous benefits. Countries will be able to join an existing and operational framework; they could also participate in the operation of the treaty and further developments in the form of protocols. Being part of the Convention would mean working together with countries and organizations with a large share of ICT infrastructure, internet industry and internet users.[234]

Hence, with all its deficiencies, The AU Convention should help create a political momentum for stronger legislations and the CoE Convention could serve as a guideline to legislate on the matter. Ethiopia has a lot to take away from such experiences. So far the country has been dormant when it comes to any international effort that has to do with cybercrime. As the next chapter will discuss, it has enacted a computer crime proclamation on domestic level, while it is a step in the right direction, domestic cybercrime legislation alone is not an answer to the problem of cybercrime.

[234] Alexander Seger, cited above at note 220, p.5

Chapter Four: Cybercrime in Ethiopia

4.1 Introduction

Ethiopia has one of the lowest percentages of internet penetration in the world and in Africa. Still the number of internet users and the percentage of penetration in the country are rising by the day. At the beginning of the twenty first century, the number of internet users in the country was around 10,000 people, but as of June 2017, this number has raised to 16,037,811 with an internet penetration rate of 15.4% and an overall growth of 160,278.1% from the year 2000.[235]

This development is largely attributed to the vast expansion on infrastructure undertaken by the government in the last decade or so. Since the year 2010, the government has started formulating a five year Growth and Transformation Plans, (hereinafter GTP) the first phase of which cover the year 2010/11-2014/15.

One of the pillars of the GTP I was to enhance the expansion and quality of infrastructure development.[236]As such, the program, *inter alia* focuses on building a high capacity fiber optics transmission line which enables full utilization of latest information and communication technologies and via neighboring countries links it with worldwide marine cables and enhances the global gateway capacity of the country.[237]

During the GTP I period, huge investment has been made so as to acquire the latest technology and expand the services in the telecom sector. As a result accessibility and quality of telecommunication services have improved. With regard to accessibility the number of customers of all kinds of telecom services increased from 7.7 million in 2009/20 to 39.8 million by 2014/15, the number of mobile subscription increased from 6.7 million to 38.8 million in the same time interval, and 3.75G and 4G internet networks with the capacity to provide services to 60 million people has been completed in the GTP I period.[238]

---

[235]See www.internetworldstats.com/stats1.htm, last accessed on December 5, 2017

[236]Growth and Transformation Plan (GTP) 2010/11-2014-15, Ministry of Finance and Economic Development (MoFED) 2010, (hereinafter GTP I) p.8

[237] Id., P. 39

[238]Growth and Transformation Plan II (GTP II) 2015/16-2019-20, Volume 1, National Planning Commission, May 2016 (hereinafter GTP II), P37

During GTP II, which covers the year 2015/16-2019/20, it is planned to complete the ICT Park which have been under establishment during GTP I period. Once the park is completed, it is believed that modern telecom services will be provided at reasonable prices from the park and as a result of which costs of production and services will be reduced, which will ultimately increase productivity and enhance competitiveness.[239]

In light of the above achievements, there are plans under the GTP II to further expand the ICT sector with a major target of increasing computer users, improve the equitable distribution of computer users and expand ICT manufacturing industry. It is planned to increase mobile penetration rate from 43.9% to 100%, increase telecom density from 10.5% to 54%, increase internet and data density from 3.3% to 10%, increase international link capacity from 27.9Gbs to 1485Gbs and maintain mobile coverage at its current level which is around 81%.[240]

However, such vast expansion of internet access and penetration in the country is not without any consequence. In fact given the short period of time it took for its expansion and the fact that many of the users are new to the technology, it has made Ethiopia a fertile target for cybercriminals.

According to US-CERT, 150 countries around the world have been affected by a computer virus called "WannaCry" which affected more than 200,000 people.[241] Ethiopia is among the victims and telecommunications, financial institutions, electronic companies, industries and hospitals are among the infrastructure targets, even though the amount of damage is not disclosed by INSA.[242]Ethiopia has been hit by more than 256 cyber-attacks during the last six months of 2016.[243]

According to a report by Kaspersky Lab, a Russian multinational cybersecurity and anti-virus provider, Ethiopia is among four African countries that have been under attack by a North Korean linked hackers group called Lazarus hackers.[244] The group is believed to be behind the

[239] Id., P.180
[240] Id., 181
[241] Available at https://www.us-cert.gov/ncas/alerts/TA17-132A last accessed on December 5, 2017
[242]Available at: http://news.xinhuanet.com/english/2017-05/18/c_136292912.htm, last accessed on December 5, 2017
[243]Available at: http://www.sudantribune.com/spip.php?article62497 last accessed on December 5, 2017
[244]Available at: http://www.thereporterethiopia.com/content/north-korea-linked-hackers-target-ethiopian-banks last accessed on December 5, 2017

attack on Bangladesh Bank, which stole 81 million dollars and the famous attack on Sony pictures back in 2014.[245]Nowadays more and more experienced hackers are shifting their attentions and directing their attacks on the developing world which have little or no form of protection against such attacks and Ethiopia is no exception to this.

INSA was able to prevent more than 400 cyber-attacks that have originated from domestic and outside sources in 2012.[246]INSA has stated that, it had put in place an integrated cyber-security solution which could prevent banks from attacks, which will be able to detect threats before and after attacks in July 20, 2016.[247]Still there are reports of ongoing attempts of cybercrime on various institutions and the treat is nowhere near to be solved.[248]

So the problem of cyberattacks is not a possibility of the future in Ethiopia but rather it is a reality that is happening on a daily basis and with more people logging online every day, the risk of being a prey to cyber criminals keeps on increasing. According to one report, there are around 4.5 million Facebook users in Ethiopia and more and more people keep joining similar social networks every day.[249] Given the fact that most of the users are new to the technology; many people did not contemplate the risk of putting personal information online, including travel plans, personal contact information and living addresses. It is becoming easier to know a lot about a stranger, using a computer just with a few clicks of a button and the danger associated with such recklessness is begging to be felt in the country.

According to an interview the researcher conducted with an investigator in the cybercrime unit division of the Federal Police Commission, one of the most common complaint lodged with the unit by private individuals had to do with revenge porn which is related with social media. People that used to date and exchange nude pictures and videos using social media will either threaten to publish it online or publish it online when they broke up. According to the Sergeant, a lot of people come with similar complaints even though the unit does not investigate

[245] Ibid.
[246]Available at: http://ethiopianbusinessreview.net/index.php/focus/item/176-cyber-attack-when-the-war-goes-digital-growing-threat-to-ethiopia) last accessed on December 5, 2017
[247]Available at: http://www.fanabc.com/english/index.php/news/item/6434) last accessed on December 5, 2017
[248]Available at: http://www.thereporterethiopia.com/content/north-korea-linked-hackers-target-ethiopian-banks last accessed on December 5, 2017
[249]Available at: www.internetworldstats.com/stats1.htm, last accessed on December 5, 2017

complaints made by individuals owing to limited capacity of the unit. Further discussions on the function of the Unit will be made in subsequent part.

With this in mind it will be good to discuss the institutional set up in the country that are endowed with the power to follow up, investigate, and prosecute cybercrime in Ethiopia.

4.2 Institutional Setup

4.2.1 Ministry of Communication and Information Technology

The government of Ethiopia has re-established and established its Ministries as new in 2010. Among the newly established Ministries, the Ministry of Communication and Information Technology (hereinafter MCIT) is one of them.[250]All the ministries among others have the obligation to initiate policies and laws on their respective fields and hence the MCIT has the obligation to do so with respect of information and communication technology.[251] Among the specific duties given to it by law, promoting the expansion of communication services and the development of information technology, setting standards to ensure the provision of quality, reliable and safe communication and information technology services, ensure the integration and interoperability of operational and forth coming computer networks and application and support of the coordination and secure information flow and exchange between government institutions are some of them.[252] In short, the Ethiopian government has established the MCIT by recognizing the critical role of ICT to national development and gave the MCIT a compressive mandate to promote the expansion and development of ICT.[253]Therefore, MCIT has the broader obligation of dealing with information technology, including insuring its safety from cyber-attacks.

4.2.2 Information Network Security Agency

The Information Network Security Agency (hereinafter the Agency) was established as a primary organ dealing with the issue of cybersecurity and entrusted with the task of protecting the country from cyber-attacks of both domestic and international source.

---

[250] Definition of Powers and Duties of the Executive Organs of the Federal Democratic Republic of Ethiopia, 2010, Art.9(12), Proc.No. 691, Fed. Neg. Gaz., year 17, no.1
[251] Id., Art. 10(1)
[252]Id., Art. 24(a)(b)(i)&(m)
[253]The National Information and Communication Technology (ICT) policy and strategy, final draft 2016, p. 4 (hereinafter ICT Draft Policy)

The Agency is accountable to the prime minister[254]and among others, has the power to; draft national policies, laws, standards and strategies that enable to ensure information and computer based key infrastructures[255] and take all necessary counter measures to defend any cyber or electromagnetic attacks on information and computer based infrastructures or systems on citizens' psychology.[256]It also Organize and administer a national computer emergency responding center[257], provide assistance and support, in respect of preventing and investigating cybercrimes, to police and other organs empowered by the law.[258]Furthermore, it Conduct forensic investigation without physical presence or conduct same with physical presence upon court warrant and in collaboration with the police.[259] The Agency also has the power to Control the import and export of information technology, information sensor and information attacking technologies[260]establish international collaboration, when it is necessary, to implement its mission.[261]

The Director General has also been given with a wide range of responsibilities, among which some of them are controversial to say the least. For instance, he could make certain financial documents, equipment, methods, work outputs and plan and strategy documents as top secret inaccessible to anybody when he has reason to believe that national security will be at stake[262] including to the Auditor General.[263] Finally, the Agency has the power to issue directives necessary for the effective implementation of the Proclamation.[264]

4.2.3 Federal Police Commission

The Federal Police is the primary institution with the power to investigate crimes in Ethiopia. Among the investigatory powers vested to it, one of them is to investigate crimes relating to information network and computer system.[265]In fact, the Computer Crime Proclamation also

[254] Information Network Security Agency Reestablishment Proclamation, 2013, Art.3 (2), Proc. No.808, Fed. Neg. Gaz. Year 20, no. 6
[255] Id., Art. 6(2)
[256] Id., Art. 6(4)
[257] Id., Art. 6(6)
[258] Id., Art. 6(7)
[259] Id., Art. 6(8)
[260] Id., Art. 6(11)
[261] Id., Art. 6(18)
[262] Id., Art. 8(2)(e)
[263] Id., Art. 10(2)
[264] Id., Art. 11(2)
[265] Ethiopian Federal Police Establishment Proclamation, 2011, Art.6 (5) (b), Proc. No. 720, Fed. Neg. Gaz. Year 18, no.2

designates the Federal Police as one of the chief institution with regard to investigating computer crimes, in collaboration with the Attorney General.[266]

The researcher has conducted interviews with experts in the Cyber Unit Division of the Federal Police Commission. The Unit was established in 2004 with the help of the American Federal Bureau of Investigation (FBI). The Unit is the only cyber division in the country and all investigations by the police that have connection with cybercrime will go through them. They conduct investigations when they are either asked by the Federal Police or State Police who needs their expertise on the matter. Contrary to the researcher's expectation, when asked the most common types of crimes they investigate often, they said most of them have to deal with forgery of document, verifying and tracing telephone communications, fake news and revenge porn investigation and the like.

The Unit has no capacity to investigate cybercrimes dealing with cybercrime *per sea* such as hacking, spam, Denial of Service and the like at all. Given it is one of the most relevant divisions in the police unit dealing with a number of technology related crimes that increase every day, the capacity and the Human Resource, which is only four individuals, is very lacking.

The Unit members have told the researcher that some trainings has been set for them by the help of US Embassy in Addis Ababa, United Nation Economic Commission for Africa (UNECA) and the Interpol, that ranges from a couple of days to two weeks in a couple of African countries, and that is all, as far as updating their capacity is concerned.

With respect to Cooperation in the international arena, the Unit has never conducted any joint investigations with intelligence agencies of foreign counties or Interpol. INSA provides technical assistance every now and then, but in their opinion, the country has a long way to go to effectively address the problem of cybercrime, which starts by addressing different technical and material needs of the Unit.

The software's used by the Unit to investigate crimes are bought from abroad and they need constant updates as they expire every three years. Updating the software constantly requires

[266] Computer Crime Proclamation, 2016, Art.38, Proc. No. 958, Fed. Neg. Gaz. Year 22, no.83 (hereinafter Computer Crime Proclamation)

foreign currency, which the government does not have readily whenever it is needed and hence, it is one of the constraints the unit has to face.

Therefore, as a unit entrusted with one of the most important job in the country, the cybercrime Unit of the Federal Police is nowhere close to where it should be. As it will be discussed later, INSA is the primary organ when it comes to cybercrime; however, both the Federal Police Commission Establishment Proclamation and the Computer Crime Proclamation have also given the Federal Police the task of investigating cybercrimes. If it is to discharge its obligation in a manner required by the law, then the Unit needs to be restructured with the necessary man power and equipment that is up to the international standard, as the country face cyber threats not only from domestic sources but international sources as well.

4.2.4 The National Intelligence and Security Service

The National Intelligence and Security Service (NISS) is also vested with powers that have some cybercrime implication. For instance, among the powers given to it, one is to lead the work of intelligence and security service both inside and outside the country in a responsible manner.[267] This could include cybercrimes as they have international dimensions. Besides, it has also a power to follow up and collect intelligence evidence on other serious crimes which are threats to the national interest and security, in collaboration with other relevant organs[268]which clearly includes cybercrimes.

Finally, when it comes to the Courts that has jurisdiction to adjudicate cases involving cybercrime, It is interesting to note that the Court of venue with first instance jurisdiction has been changed from Federal First Instance Court, which was provided for by the Federal Courts Establishments Proclamation,[269] to Federal High Court by the Computer Crime Proclamation.[270]

[267]National Intelligence and Security Service Reestablishment Proclamation, 2013, Art. 7(1) Proc. 804, Fed. Neg. Gaz. Year 19, no. 55
[268] Id., Art. 8(6)
[269] Federal Courts Proclamation, 1996, Art.4 (7) & 15, Proc. No. 25, Fed. Neg. Gaz., Year 2, no. 13
[270] Computer Crime Proclamation, cited above at note 266, Art. 40

4.3 The Policy Framework

4.3.1 The National Information and Communication Technology (ICT) Policy and Strategy 2009

As far as the policy front is concerned, the Ethiopian government has acknowledged that cybercrime is a threat to the country and formulated a policy back in 2009. According to the 2009 National Information and Communication Technology Policy, the government will give priority to the creation of a safe and secure ICT environment as well as appropriate standards.[271] As such some of the objectives of ICT security are: to prevent, detect and respond to cybercrime and misuse of ICT so as to contribute to the fight against national, regional and international crimes such as prostitution, fraud, organized crimes and terrorism.[272]

The strategies to achieve this objectives are to facilitate the necessary laws and legislation instruments to govern and regulate cyber related activities, introduce and enforce appropriate legal measures against misuse of systems, protect networks, data and information systems against attacks and unauthorized access, and protect the right of citizens, introduce measures for protecting the Ethiopian public against the negative and undesirable impacts of ICT such as *cybercrimes*, digital frauds and pornography.[273]

With respect to standards, the objective is to adopt regional and international standards and best practices in the development of ICT rules, guidelines and regulations, promote cooperative endeavors between national security agencies and similar agencies in other countries for collaboration and for sharing best practices.[274]Ensuring the protection of Intellectual property rights in ICT is one of the objectives of the legal and regulatory environment.[275]

The government has updated this policy in 2016 still keeping the above pillars and objectives as they are with added emphasis on the vital importance of ICT for the development of the country. Hence, the government has made the development of ICT one of its strategic priorities and has placed a significant emphasis on its role for economic transformation.[276]

---

[271]The National Information and Communication Technology (ICT) Policy and Strategy 2009, p.1

[272] Id., p. 11
[273] Ibid.
[274] Id., p.24
[275] Id., p. 25
[276]ICT Draft Policy, cited above at note 253, p.4

4.3.2 The Criminal Justice Policy

The criminal justice policy acknowledges the need for new techniques of criminal investigation other than those that are already stipulated by the 1961Criminal Procedure Code in order to cope up with the complex and difficult crimes that have international dimensions. As such the use of electronic devises so as to gather evidence is taken as one area where legislation is needed. Furthermore, it stipulates conditions where electronic surveillance could be undertaken with or without court warrant in emergency situations and the need to legislate on such areas.[277]

4.4 The Legal Framework

4.4.1 The Criminal Code

The Criminal Code of Ethiopia is the first instrument to ever legislate on cybercrime. As it is stipulated in the preamble of the Code, a number of reasons have necessitated the revision of the Penal Code that was enacted in 1957. The various social, political and economic changes that have taken place in the country and a major shift with regard to equality between religions, nations, nationalities and peoples and Human Rights recognized by the Constitution and International Human Right Instruments ratified by Ethiopia are the general reasons. In particular, *inter alia* failure of the Penal Code to properly address crimes born out of advances in technology and complexities of modern life such as hijacking of aircrafts, *Computer Crimes* and money laundering are some of them.[278]

The Criminal Code discusses computer crimes under chapter III, which broadly deal with crimes against Rights in property. Section II of the chapter comprises of six articles and all deal with computer crimes. The entire issue as far as the Criminal Code is concerned is discussed under these six articles.

For the crimes stipulated under the Code to be punishable, they must be committed 'without authorization' and 'intentionally.' However, the expression "without authorization" is somewhat problematic as it seems to indicate 'potentially punishable acts, but made just by exceeding authorization [that] was already given are not punishable under the Code'.[279]

---

[277] The Federal Democratic Republic of Ethiopia Criminal Justice Policy, Ministry of Justice, 2011, Amharic, p.17 & 18 (*translation mine*)
[278] The Criminal Code of the Federal Democratic Republic of Ethiopia, Proclamation 2004, preamble para. 2, Proc. No. 414, Fed. Neg. Gaz. 9 May 2005 (hereinafter The Criminal Code)
[279]Kinfe Micheal Yilma, cited at note 8 above, p. 725,

Despite being relatively recent and a result of necessity to legislate on matters that are significantly increasing as technology and modern means of communications increases, the Criminal Code does not provide for a comprehensive coverage of cybercrime. Rather, it is full of flaws that necessitate further legislation on the matter. It is too narrow in scope as it only covers three types of cybercrimes, it still uses procedural laws of the 1961Criminal Procedure Code which are out dated for cybercrimes, it is silent about international cooperation, and it does not provide definition of key terms and provides for minimal punishments in case of indictment.

4.4.2 The Computer Crime Proclamation

The Computer Crime proclamation has been drafted by INSA and has been a subject of debate for a while. INSA claims that various stakeholders including the society have a chance to see and debate on the draft before it was sent to the parliament. Indeed, there has been some changes made to the proclamation that were fiercely debated in the draft and it is a step in the right direction to legislate on a matter that is a growing concern not just for the country but the whole world, and yet few actions has been taken so far at the national arena.

The Proclamation in the preamble part acknowledges cybercrime as a threat and if it's not managed properly it could hinder the economic development of the country and the existing laws are not sufficient to deal with the problem *per sea.*[280]Hence, it has become necessary to incorporate new legal mechanisms and procedures in order to prevent, control, investigate and prosecute cybercrimes. However, it is interesting to note that unlike international best practices that are found both in Council of Europe Convention on Cybercrime and the AU Convention, the preamble has no stipulation that it should be interpreted in accordance with International Human Rights instruments so as to not infringe fundamental rights and freedoms, especially right to privacy and freedom of expression, which are the most likely to be infringed by such laws.

Part I of the proclamation has two articles, article 1 stating short title and article 2 providing for definition of key terms. Article 2 provides for a number of key definitions including "computer crimes" "content data", "access", "critical infrastructure," "service provider" and the like. By

[280] Computer Crime Proclamation, cited above at note 266, preamble para. 2&3

doing so, the Proclamation remedies one major gab of the Criminal Code provisions, which are devoid of such key term definitions.

Part II of the Proclamation has two sections and section I deals with crimes against computer system and computer data.[281]It includes *Illegal Access, Illegal Interception, Interference with Computer System, Causing Damage to Computer Data and Criminal Acts Related to Usage of Computer Devices and Data.* The final article of the section deals with aggravated cases of the crimes discussed above. This section of the Proclamation is more or less consistent with international practices, especially the Council of Europe Convention on Cybercrime except for a few variations.

Article 3 of the Proclamation talks about Illegal Access and stipulate for punishment with simple imprisonment not exceeding three years or fine ranging from 30,000-50,000 birr. And if the act is committed against a legal person the punishment will rise to rigorous imprisonment three to five years, and it will even rise to rigorous imprisonment from five to ten years if committed against critical infrastructure. The Council of Europe Convention provides that countries could require *dishonest intent* to make the act punishable but the proclamation does not have such requirements. Article 4 of the Proclamation criminalizes Illegal Interception in the same manner of aggravated punishment if it is committed against legal person or critical infrastructure. Again, it does not require any *dishonest intent* for the act to be punishable, which is optional under Council of Europe Convention on Cybercrime.

Interference with Computer System and Causing Damage to Computer Data are discussed under article 5 and 6 of the Proclamation respectively and just like the previous articles they did not provide for dishonest intent or series harms to be caused before a criminal liability is attached to the act, as such stipulation are provide as optional requirements in international best practices.

Article 7 of the Proclamation deals with cases related to Criminal acts related to the usage of computer devices and data and knowingly transmitting computer program that is exclusively designed for causing to computer system or data or network is punishable with a simple imprisonment not exceeding five years or fine up to 30,000 birr. Knowingly importing, producing, distributing or offering for sell of such programs that could be used to commit crimes

[281] Id., Art. 3-8

under article 3-6 of the proclamation is punishable with rigorous imprisonment up to five years and fine 10,000 to 50,000 birr.

Interestingly, under article 7(4) of the Proclamation intentional disclosure of computer program, secret code, key password or any other similar data for gaining access to a computer is punishable with simple imprisonment up to five years or in serious cases with rigorous imprisonment up to five years even if there is no harm what so ever done with the action or there is minimal harm done to a person. The punishment provided for the act and the act that could potentially lead to such an action is not proportional. Finally, under article 7(5) of the Proclamation negligent act is also punishable with a simple imprisonment up to one year and fine up to 10,000 birr. Not only there is no such stipulation in international and regional best practices, but also in a country like Ethiopia where the population is new to ICT, the probability of someone unknowingly disclosing such data is high and punishing such person for negligent acts where there is no intention and possibly no harm done is highly controversial.

Section II of the Proclamation mainly focuses on Computer Related Forgery, Fraud and Theft. Computer related forgery is discussed under article 9 of the Proclamation and it is more or less in line with Council of Europe Convention on Cybercrime even the later provides for optional inclusion of *fraudulent intent*, which the former did not include. On the other hand Computer related fraud under article10 of the Proclamation is consistent with Council of Europe Convention as it requires fraudulent intent. The final article of the section deals with Electronic Identity Theft, which is a new concept, as far as international best practices are concerned and provides for a simple imprisonment not exceeding five years or fine up to 50,000 birr.

Section III of the Proclamation deals with Illegal content data and as far as best international practices are conserved, the only content data restrictions imposed is child pornography which is dealt under article 12 of the Proclamation. However, the Proclamation has added additional crimes in this regard. Article 13 criminalizes Intimidating or threatening a person by disseminating any writing, video, or any other image through a computer system. However, there are legitimate concerns that are raised against such stipulation as the Proclamation does not define “intimidation” and hence, legitimate journalistic works could be included in such

restriction.[282]Besides, article 13(3) of the Proclamation provides for criminal defamation as punishable act, which has been a condemned action by the International Human Right courts.[283]

Article 14 of the Proclamation deals with crimes against Public Security and criminalize intentional dissemination of any written documents, videos, audios, or any other pictures that incites violence, chaos or conflict among people through a computer system. Still, the concern with this provision is that, it does not provide for an exception where journalistic activities are concerned and it could possibly punish legitimate reporting.

In principle, Service providers are not criminally liable for third party content. The Proclamation acknowledges this fact. However it also provides exceptional circumstances where they could still be liable. Service providers could be liable if they are directly involved in dissemination or edition of the content f they failed to take action up on obtaining of the actual knowledge that the content data is illegal and if they failed to take action upon receiving notice from competent authorities. There are people like the researchers of Article 19 that argue service providers should be absolutely exempted from criminal liability. They assert that intentional best practice does not support any restriction or liability on service providers. The researcher however, is of the opinion that the restrictions impose by the Proclamation are sound and necessary. First of all it acknowledges that in principle they are not liable and only in exceptional circumstances would they be liable. Secondly, the exceptions are reasonable as they require some form of knowledge or involvement on the part of the service provider in the content. Thirdly, despite the argument forwarded by researchers of Article 19, the international best practice nowadays is favoring such restrictions on service providers. The recent action the American Senate took on companies of Silicon Valley including Google, Facebook and Twitter as a result of their role in assisting in Russian meddling in the 2016 US presidential election supports such assertion.[284]

Interestingly, the Proclamation is silent on offense related to Infringement of copyrights and related rights unlike international best practices, even if the ICT policy clearly stipulates such protection as one of the goals of the policy, as discussed above. Given that this is the most

[282]Ethiopia: Computer Crime Proclamation, Article 19, (2016), p. 15, available at: https://www.article19.org/data/files/medialibrary/38450/Ethiopia-Computer-Crime-Proclamation-Legal-Analysis-July-(1).pdf

[283] Ibid.

[284] See https://www.theverge.com/platorm/amp/2017/11/1/16591646/facebook-senate-hearing-feinstein-russia-google-twitter

comprehensive legislation on the issue so far, and copyrights and other related rights are likely to be infringed using a computer, the researcher is of the opinion that the issue should have been addressed here.

Section Four of the Proclamation under Other Offenses penalizes failure to cooperate and hindrance of Investigation.[285] Furthermore, it provide for concurrent application of laws where any of the act under the proclamation resulted in a commission of another crime under the Criminal Code or other special laws.[286]The Public Prosecutor and the Police are given the investigative role, when necessary they could be assisted by the Agency.[287] The service provider has a duty to retain computer data that flows through its system for up to one year.[288]

With regard to Real time collection of computer data, two scenarios are provided. In the first scenario, real time collection data could only be resorted to as a last measure up on the decision of the Attorney General and approval of a warrant by a Court.[289]In the second scenario, the Attorney General could authorize interception without a Court warrant where there are grounds to believe that computer crime could damage critical infrastructure. In such case the Attorney General should present the reasons before the president of the Federal High Court within 48 hours, and the president will give the appropriate order immediately. The question is what would happen to the operation and the data gathered if the president of the High Court disagrees with the decision of the attorney general? It looks like in case the president of the Court finds the reasons for interception insufficient or unreasonable, then he could order the discontinuation of the operation and the destruction of the data gathered. But what if the Attorney General wants to appeal such decisions? The Proclamation is silent on this issue and it looks like, at least from the way the provision is framed, that the decision of the president is a final one.

The Proclamation provides for duty to report on any service provider or government organ that has the knowledge about commission of computer crime to the agency immediately.[290]It also provides that arrest should be conducted as per the provision of the Criminal Procedure Code, provided that the overall remand period does not exceed four months. One could argue that four

[285] Computer Crime Proclamation, cited above at note 266, Art. 17
[286] Id., Art. 19
[287] Id., Art. 23
[288] Id., Art. 24
[289] Id., Art. 25(1)(2)
[290] Id., Art. 27

months is a very long time for an investigation to take place, but given the international dimension of cybercrime and the failure of the Criminal Procedure Code to stipulate for an upper limit for remand, the four months maximum period provided by the Proclamation is both reasonable and a step in the right direction.

Part Four of the Proclamation provides detailed rules with regard to Evidentiary and Procedural Provisions. Accordingly, the investigatory organ has the power to order preservation of data for three months when he has reason to believe that the data is vulnerable to loss or modification and such order could be extended once for additional three months.[291]

The investigators should apply to a Court warrant before they want to search a computer data of a suspect.[292] But while conducting the search, the investigators, *inter alia,* are given a power to render inaccessible the stored data from the computer system on their own. Such powers are not made conditioned up on approval of the Court and it seems that it is totally left for the discretion of the investigators, which is open for abuse.[293] Interestingly they have to seek Courts approval to render a data inaccessible or restricted or blocked if they found out the function of a computer system is in violation of the provisos of the Proclamation[294], hence for a stronger reason, they should have to apply for Courts approval in the first scenario as well.

In the course of their investigation, the investigators could order *any person* that has knowledge to provide the necessary information or computer data that could facilitate the search or access.[295] Here, it is controversial whether such person could include the accused himself, as the Proclamation, unlike international best practices, did not include unequivocal statement ensuring that it is subject to conditions and safeguards provided under international instruments. However, one still could argue that, since the principle provided under article 21 of the Proclamation guarantying that this section as a whole should be subjected to Human and Democratic Rights provided under the Constitution, and International Instruments, it would be safe to conclude that the accused himself could not be forced to provide information as it could be self-incrimination which is protected under the Constitution and International Instruments ratified by Ethiopia.

[291] Id., Art. 30
[292] Id., Art. 31
[293] Id., Art. 31(3)(d)
[294] Id., Art. 31(5)
[295] Id., Art. 32(4)

Electronic evidences are made admissible under the Proclamation, provided that they are authenticated and the burden of proving their authenticity rest up on the party that produces them.[296]Under article 37(1) of the Proclamation it is provided that the public prosecutor has the burden of proving material facts, which is logical, but sub article 2 provide the Court could shift the burden of proving to the accused once the basic facts are proved, this stipulation is controversial as to why such burden of prove need to be shifted when there is a Constitutional guarantee of presumption of innocence until proven guilty.

Part Five of the Proclamation deals with institutions that follow up cases of computer crimes, and the Attorney General and Police have the power to set up a specialized task units and the agency has the duty to establish online computer crimes investigation system and provide assistance to the Police and Attorney General when needed.[297]The establishment of a National Executive Task Force comprising of the Federal Attorney General, Federal Police Commission, and other relevant bodies is provided for under article 41of the Proclamation , the researcher has made an inquiry both in the Federal Police Commission and the Attorney General Office whether such task force is established or not and it has not been yet established, owing to the fact that the Proclamation is new and the Attorney General Office was also established recently.

In Part Six which is the final section of the Proclamation, the Federal Attorney General is authorized to engage in International cooperation agreements with competent authorities of another countries, which as of yet, it has not.[298] The Council of Ministers and the Agency are given the power to issue regulations for the effective implementation of the Proclamation,[299]and finally the Proclamation rightly repeals all the Criminal Code provisions dealing with cybercrime as they cannot be effective in the fight against cybercrimes.[300]

[296] Id., Art. 33 & 34
[297] Id., Art. 38 & 39
[298] Id., Art. 42
[299] Id., Art. 44
[300] Id., Art. 45

Chapter Five Conclusion and Recommendation

5.1 Conclusion

Cybercrime is one of the most increasing security threats the world has to face as more and more portion of the world's society is logging online every day. The expansion of technology and reliance by the population to carry out their daily activities is inevitable fact, but a lot should be done to mitigate the effect of cybercrime that could potentially disrupt people's everyday life or even set the human civilization back in time.

As an emerging economy in Africa, Ethiopia is doing a lot of expansion in its infrastructure including the telecom sector and that will inevitable enable more and more people to conduct their daily activities online by using the internet. Such reliance is a good thing if the country is to keep up with the rest of the world and compete in the international market including in terms of attracting investors.

However, the threat of cybercrime is the necessary evil Ethiopia has to face just like any country in the world and it has a lot to do in this respect even if it is in the right track of doing so. The Council of Europe Convention on Cybercrime is one of the most comprehensive pieces of legislation at the international level when it comes to cybercrime and the major economies of the world are part of it including the United States and Japan. Enacting a legislation that is in line with such international 'standards' will make it easier to Ethiopia to join the Convention when the need arises to do so, but more importantly, it will enable the country to have a comprehensive legislation to deal with the issue of cybercrime that is up to the international standard.

There are various efforts in the African continent to address the issue of cybercrime both at sub-regional and regional levels. The sub-regional efforts are in the right track in manifesting the spirit of the CoE Convention even though most of them are still drafts. The AU Convention on Cyber Security and Personal Data Protection among other things tries to achieve comprehensive cyber legislation throughout the continent but it lacks the essential procedural parts that will assist each member countries to cooperate in the investigation and prosecution of cybercrime in the continent.

For a long time the need for cybersecurity has not been felt in Ethiopia owing to both low development of ICT infrastructures and more pressing matters that occupy the attention of the

government. The one piece of legislation that was meant to rectify the problem and stipulate a comprehensive rule on the matter, the Criminal Code, is full of shortcomings and could not serve the intended purpose. Even if the ICT policy of the country has long acknowledged the need for a comprehensive legislation on cybercrime, it has taken years to come up with such legislation. Finally a Proclamation has been enacted to govern the issue and it is a step in the right direction, as it is framed in a technology neutral terms and including guarantees to basic human rights and freedoms. According to the drafter of the proclamation, the CoE Convention on Cybercrime was taken as a guideline but domestic legislation alone is not the answer to cybercrime as it is an international problem that needs international cooperation. The Proclamation has authorized the Attorney General to engage in such cooperation but it needs more commitment and effort as a country on the part of Ethiopia in order to effectively make use of the available international mechanisms. There are still some gaps that needs improvement with regard to the Proclamation, especially when it comes to trying to strike a balance between the individual interests including the right to privacy and the interest of the society as whole to be protected from cybercrime.

5.2 Recommendation

Despite the introduction of new Computer Crime Proclamation and the establishment of INSA to primarily deal with the matter of cybersecurity, there is still a lot that could and should be done in order to give better protection to the Ethiopian public from cybercrime and ensure a safe and smooth business transaction that depends on and make use of the appropriate technology.

5.2.1 Concerning International and Regional Agreements

Despite the fact that cybercrime is a problem that is common to all countries of the world irrespective of their economic status, the measures taken by African countries to protect themselves from such threats is not that great. Despite the enactment of a Convention which specifically deals with the problem of cybercrime, so far only a couple of countries has signed and adopted the Convention. Sadly, Ethiopia is not a party of it yet, in fact Ethiopia is dormant when it comes to any international cooperation on cybercrime so far. It has not participated in any sub-regional, regional or international cooperation in the fight against cybercrime. With all its flaws the AU Convention is a step in the right direction and it will help bring the issue in the continental radar and hence is helpful to be a part of. Therefore, Ethiopia should sign and ratify

the AU Convention and encourage other African countries to do the same so that the Convention could enter into force.

On the other hand the Council of Europe Convention on Cybercrime is one of the most comprehensive legislation on the matter that is open for every country in the world. And has as its members, the most of the strongest economies of the world where the big ICT related service providers are situated. Ethiopia should follow the example of countries like South Africa, Seychelles and Senegal and join the Council of Europe Convention so that it could easily get technical and other assistance from such member countries and effectively investigate and prosecute cyber-attacks including those from the outside.

5.2.2 Concerning the Federal Police Cybercrime Unit

The Federal Police Cybercrime Unit is one of the most important stakeholders in the fight against cybercrime. It has been given joint mandate together with the Attorney General Office to investigate cybercrimes. However, at its current stage, its composition and status is nowhere close to where it should be. It does not have the necessary man power; equipment's and training in order to fully engage and discharge its duties. Hence, it needs a great deal of attention and assistance from the government if it is to be fully operational and keep the Ethiopian public safe.

5.2.3 Concerning the Computer Crime Proclamation

The enactment of the Computer Crime Proclamation is a long awaited and long overdue process. But even if it took quite a time, the enactment by itself is a move in the right direction. The Proclamation tries to strike a balance between the interest of individuals' vis-à-vis protection of the right to privacy and freedom of information and the interest of the society at large. However, there are still some stipulations that cast shadow on such efforts either by being vague or give a wider power to the executive branch. One of the criteria to be a member to the CoE Convention is to have a law that is consistent with the Convention. If Ethiopia aspires to be a member and reap the benefits associate with it, the following provisions of the Proclamation need to be aligned with the spirit of the CoE Convention.

Article 7(4) of the Proclamation provides for a simple or rigorous punishment of up to five years for disclosure of pass word, key, secret code and the like without taking into consideration the harm done as a result of such action, thereby making acts with simple or no effect punishable un proportionally. Moreover, article 7(5) also punish negligent act, still without considering the

harm done and hence run the risk of punishing unsuspecting innocents in a country like Ethiopia where the society is new to the technology.

Article 13 of the Proclamation criminalizes Intimidating or threatening a person by disseminating any writing, video, or any other image through a computer system. On the other hand, article 14 of the Proclamation deals with crimes against Public Security and criminalize intentional dissemination through a computer system any written video, audio, or any other picture that incites violence, chaos or conflict among people. However, both provisions do not provide for any exception to protect legitimate journalistic reporting there by run the risk of jailing journalist for doing their works.

Article 25 of the Proclamation that talks about real time collection of data is vague, to say the list as it is not clear if the judge decide against the stipulation of the Attorney General, whether the later would have recourse to appeal or not. The provision is draft in a way that suggests the judge would likely agree with the Attorney General and it needs redrafting.

Article 31 of the Proclamation provides for unreasonable power given to investigators to render inaccessible the stored data from the computer system on their own, without any oversight by the Courts. Such power is not only unreasonable but is open for abuse by the investigators either to force the accused to cooperate with them or derive unnecessary benefit under the disguise of investigation.

Finally article 32(4) of the Proclamation is not clear whether the stipulation "any person" to cooperate will include the accused himself. At the very least the stipulation is vague and open for interpretation, which could ultimately infringe the Constitutional right of the accused against self-incrimination.

Therefore, the researcher provides the above as recommendations that could be taken in to consideration in order to align the Computer Crime Proclamation with CoE Convention.

Bibliography

Books

Bernadette H. Schell and Clemens Martin, *Cybercrime A Reference Handbook (*ABC-CLIO, Inc. 2004)

Bryan A. Garner (ed.) *Black's Law Dictionary*, (9th *ed.,2011) p.443*

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

George Curtis, *The Law of Cybercrimes and Their Investigation*, (CRC Press 2012)

Igor Bernik, *Cybercrime and Cyberwarfare*, (ISTE Ltd and John Wiley & Sons. Inc. 2014)

James R. Richards, *Transnational Criminal Organizations, Cybercrime and Money Laundering, A Handbook for Law Enforcement Officers, (CRC Press* 1999)

Jonathan Clough, *Principles of Cybercrime*, (Cambridge University Press, 2010)

Majid Yar, *Cybercrime and Society*, (Sage Publications Ltd 2006)

Mohamed Chawki, Ashraf Darwish, Mohamed Ayoub Khan, Sapna Tyagi, *Cybercrime, Digital Forensics and Jurisdiction*, (Springer International Publisher Switzerland 2015)

Nir Kshetri, *Cybercrime and Cybersecurity in the Global South*, (Palgrave MacMillan Publisher 2013)

Nir Kshetri, *The Global Cybercrime Industry, Economic, Institutional and Strategic Perspectives*, (Springer International Publisher, 2010)

Parker Donn., *Fighting Computer Crime: A New Framework for Protecting Information*, (1998) p.72

Samuel C. McQuade III, (ed.) *Encyclopedia of Cybercrime*, (Greenwood press 2009),

Stein Schjolberg and Solange Ghernaouti-Helie, *A Global Treaty on Cybersecurity and Cybercrime*, (AiTOslo Publisher, 2011)

Susan W. Brenner, *Cybercrime Criminal Threats from Cyberspace, (an imprint of ABC-CLIO,LLC, 2010)*

Will Gragido, Daniel Molina John Pric, Nick Selby, Blackhatonomics An Inside Look at the Economics of Cybercrime, (Elsevier 2013)

Journals and Articles

*"*Comprehensive Study on Cybercrime,*"* United Nations Office on Drugs and Crime, February 2013, United Nations, New York

"Ethiopia: Computer Crime Proclamation," Article 19, (2016), p. 15, available at: https://www.article19.org/data/files/medialibrary/38450/Ethiopia-Computer-Crime-Proclamation-Legal-Analysis-July-(1).pdf

Alexander Seger, "The Budapest Convention on Cybercrime 10 years on: Lessons learnt or the web is a web", (2012)

Dr. Dejo Olowu, "Cybercrimes and Boundaries of Domestic Legal Responses: case for Inclusionary Framework for Africa*," Journal of Information, Law and Technology*, May 2009

Dr. Nick Nykodym and Robert Tyler, "Control of cybercrime: the World's Current Legislative Efforts against Cybercrime," *Computer Law and Security Report* Vol.20 No. 5 (2004)

Eric Tamarkin, "The AU Cybercrime Response, A positive start but substantial challenges ahead," *Institute for Security Studies Policy Brief* 73(January 2015)

Eric Tamarkin, "Cybercrime A Complex Problem Requiring a Multi-Faceted Response" *Institute for Security Studies Policy Brief*, available at: http://www.fiels.ethz.ch/isn/177499/Polrief51Feb14.pdf

Gardachew Worku, "Electronic-Banking in Ethiopia- Practices, Opportunities and Challenges," *Journal of Internet Banking and Commerce*, vol. 15, no.2, (August 2010)

Haleform Hailu, "The State of Cybercrime Governance in Ethiopia", (2015)

Joan Ruttenberg, Paige von Mehren, Julie Yen, "The OPIA Insider's Guide to Intellectual Property and Cyberlaw," Harvard Law School *(*2013)

Jonathan Clough, "A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonization*", (Monash University Law Review (Vol. 40, No. 3)*

Kenya Cyber Security Report 2016, p. 10, available at: http://www.serianu.com/downloads/KenyaCyberSecurityReport2016.pdf

Kinfe Micheal Yilma, "Developments in Cybercrime Law and Practice in Ethiopia," *Journal of Computer Law & Security Review* (2014)

Kristen E. Eichensher, "The Cyber-Law of Nations*", The Georgetown Law Journal*, Vol. 103:317

Loucif Kharouni, "Africa A new Safe Harbor for Cybercriminals*?",* (Trend Micro Incorporated Research Paper 2013)

Mary Ellen O'Connell, "Cyber Security and International Law*", University of Notre Dame Law School, US*, May 2012

Mesifin Belachew, "Investment in Broadband Infrastructure in Ethiopia", available at http://unohrlls.org/custom-content/uploads/2017/03/presentation-on-BB-in-Ethiopia.pdf

Molalign Asmare, "Computer Crimes in Ethiopia: An Appraisal of the Legal Framework," *International Journal of Social Science and Humanities Research*. , vol. 3,(2015),

National Bank of Ethiopia, Annual Report 2014/15, available at http://www.nbebank.com/pdf/annualbulletin/Annual%20Report%202014-15/Annual%20Report%202014-15.pdf

Rajlakshmi Wagh, "International Comparative Analysis of Trends of Cybercrime Laws in USA and India*" Journal of Advanced Computer Science and Information Technology*, 2013, vol.2,

Stein Schjolberg, *A Geneva Declaration for Cyberspace, January 2016, available at www.cybercrimelaw.net*

Xiao Yingying and Yuan Zhengqing, "A primary exploration on cyber security governance in Africa," *China Academic Journal,* 2015

Zahid Jamil, Comparative Analysis of the Malabo Convention of the African Union and the Budapest Convention on Cybercrime (2016) p.4 available at www.coe.int/en/web/cybercrime/-/malabo-and-budapest-convention-towards-complementarity

International Instruments

AU Convention on Cybersecurity and Personal Data Protection (EX.CL/846(XXV))

Council of Europe Convention on Cybercrime 2001(ETS No.185)

East African Community (EAC) Draft Legal Framework for Cyberlaws (2008),

Economic Community of West African States (ECOWAS) Draft Directive on Fighting Cybercrime (2009), (Supplementary Act A/SA.2/01/10)Cybercrime Directive 1/08/11) and personal protection and personal data (Supplementary Act A/SA.1/01/10)

Explanatory Report to the Council of Europe Convention on Cybercrime 2001, (ETS No.185),

The Common Market for Eastern and Southern Africa (COMESA) Cyber Security Draft Model (2011)

The Southern African Development Community (SADC) Model Law on Computer Crime and Cybercrime (2012)

Domestic Legislations

Computer Crime Proclamation, 2016, Art.38, Proc. No. 958, Fed. Neg. Gaz. Year 22, no.83

Definition of Powers and Duties of the Executive Organs of the Federal Democratic Republic of Ethiopia, 2010, Art.9(12), Proc.No. 691, Fed. Neg. Gaz., year 17, no.1

Ethiopian Federal Police Establishment Proclamation, 2011, Art.6 (5) (b), Proc. No. 720, Fed. Neg. Gaz. Year 18, no.2

Federal Courts Proclamation, 1996Proc. No. 25, Fed. Neg. Gaz., Year 2, no. 13

Information Network Security Agency Reestablishment Proclamation, 2013, Art.3 (2), Proc. No.808, Fed. Neg. Gaz. Year 20, no. 6

National Intelligence and Security Service Reestablishment Proclamation, 2013, Proc. 804, Fed. Neg. Gaz. Year 19, no. 55

The Criminal Code of the Federal Democratic Republic of Ethiopia, Proclamation 2004, preamble para. 2, Proc. No. 414, Fed. Neg. Gaz. 9 May 2005

The Federal Democratic Republic of Ethiopia Criminal Justice Policy, Ministry of Justice, 2011, Amharic

The National Information and Communication Technology (ICT) policy and strategy, final draft 2016,

The National Information and Communication Technology (ICT) Policy and Strategy 2009, p.1

Websites

www.itu.int/net/press_releses/2015/17.aspx

https://www.itu.int/net4/itu/icteye/CountryProfileReport.aspx?countryID=77

www.history.com/topics/inventions/invention-of-the-internet

http://www.telegraph.co.uk/tecnology/microsoft/11577364/Web-browsers-a-brief-history.html

https://www.cnbc.com/2017/02/07/cybercrime-costs-the-global-economy-450-billion-ceo.html

http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=KDnvg84D

http://allafrica.com/stories/201704251054.html

https://www.economist.com/blogs/economist-explains/2013/05/economist-explains-18

https://www.standardmedia.co.ke/business/article/2001235820/kenya-worest-hit-in-east-africa-by-cyber-crime

http://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

www.internetworldstats.com/stats1.htm

http://news.xinhuanet.com/english/2017-05/18/c_136292912.htm

http://www.sudantribune.com/spip.php?article62497

http://www.thereporterethiopia.com/content/north-korea-linked-hackers-target-ethiopian-banks

http://ethiopianbusinessreview.net/index.php/focus/item/176-cyber-attack-when-the-war-goes-digital-growing-threat-to-ethiopia

http://www.fanabc.com/english/index.php/news/item/6434

http://www.thereporterethiopia.com/content/north-korea-linked-hackers-target-ethiopian-banks

www.internetworldstats.com/stats1.htm