Jimma University

College of Law and Governance

School of Law

LLM in Human Rights and Criminal Law

Examining Legislative and Regulatory Responses to The Evolving Cyber Criminality: Enforcement Challenges and Lessons for Ethiopia

A Thesis Submitted to the School of Law of Jimma University in Partial Fulfillment of the Requirements of LL.M in Human Rights and Criminal Law

By: - Zelalem Tadesse, ID No. RM/2770/12

Principal Advisor - Nega Ewunetie, Associate Professor of Law

Co Advisor - Yiheyis K. (LL. B, LL. M)

June 2022

Jimma, Ethiopia

Declaration

I, the undersigned, declare that this thesis entitled: “Examining Legislative and Regulatory Responses to The Evolving Cyber Criminality: Enforcement Challenges and Lessons for Ethiopia” is my original work, and has not been presented by any other person for an award of LL.M in Human Rights and Criminal Law in this or any other University, and all sources of material used for this thesis have to be duly acknowledged.

Zelalem Tadesse	_____	_____
Name of Author	Signature	Date

APPROVAL SHEET

As thesis research advisor, I hereby certify that I have read and evaluated this thesis prepared, under my guidance, by Zelalem Tadesse, entitled "Examining Legislative and Regulatory Responses to The Evolving Cyber Criminality: Enforcement Challenges and Lessons for Ethiopia". I recommend that it be submitted as fulfilling the thesis requirement.

Nega Ewunetie	_____	_____
Principal Advisor	Signature	Date
Yiheyis K.	_____	_____
Co-Advisor	Signature	Date

As members of the Board of Examiners the LL.M thesis open defense examination, we certify that we have read and evaluated the thesis prepared by Zelalem Tadesse. We recommended that the thesis be accepted as fulfilling the requirement for the degree of Master of Laws Degree (LL.M).

Yiheyis K.	_____	_____
Chairperson	Signature	Date
Abay A.	_____	_____
Internal examiner	Signature	Date
Dr. Marishet T.	_____	_____
External examiner	Signature	Date

LIST OF ABBREVIATIONS

AU	Africa Union
ICT	Information and Communication Technology
EU	European Union
INSA	Information Network Security Agency
GERD	Grand Ethiopian Renaissance Dam
CEI	Cybersecurity Exposure Index
GCI	Global Cybersecurity Index
NISP	National Information Security Policy
FPC	Federal Police Commission
ITU	International telecommunication union
CERT	Computer Emergency Response Team
EFCC	Economic and Financial Crime Commission
FDRE	Federal Democratic Republic of Ethiopia
DoS	Denial of Service
LEA	Law Enforcement Agency
NCRB	National Crime Records Bureau
FBI	Federal Bureau Investigation
AFF	Advance Fee Fraud
ITA	Information Technology Act
ITAA	Information Technology (Amendment) Act
MoIT	Minister of Information Technology
MoJ	Minister of Justice
MoHA	Minister of Home Affair
NISPG	National Information Security Policy & Guidelines
NFIU	Financial Intelligence Unit
ISP	Internet Service Provider
ONSA	Office of the National Security Adviser
FIC	Financial Intelligence Center
INTERPOL	International Criminal Police Organization
UNODC	United Nation Office of Drag and Crime
MLAT	Multilateral Legal Assistance Treaty

ACKNOWLEDGMENT

First of all, my endless thanks to almighty GOD for unwavering and lasting love he has upon me. Also, I would like to extend my gratitude to my advisor Associate Professor of Law Nega Ewunetie, for his indispensable guidance and continuous advice that helped me to successfully accomplish my study. Similarly, I am grateful to My co-advisor Mr. Yiheyis K. (LL. B & LL. M) for your follow up and invaluable feedback. Next to these I would like to provide my deep gratitude to the federal public prosecutors Mr. Getiye Belihu and Mrs. Tenay Abebe for your kind responses whenever I needed.

My deepest appreciation to my father Mr. Tadesse Seboka. I am pleased to have a father like you, your advice in every walk of my life has been invaluable. Likewise, it has been a blessing to have two mothers, Emebet Hailu and Addisalem Gashawu, with all the support and encouragement that you gave me throughout my study, you owe my heartfelt appreciation.

Finally, my special thanks go to all friends who stand beside me. It is my pleasure, if not for inconvenience, to mention the place I have for you in my heart. You owe my gratitude.

Thank You All!

Table of Content

Abstract

Internet and computer technologies provide limitless opportunities for commercial, communication, educational and industrial advancement, to say a few. Innovation of ICTs and Internet Technology has brought numerous advantages as it offers a virtual world over which one can conduct daily activities and easily interact without geographical and physical barriers. However, besides the plethora of advantages that the introduction of Internet and computer technology provides, its shortcoming has opened the door wider for cybercriminals to exploit or undermine confidentiality, integrity and availability of computer systems, data and networks. Thus, criminalizing and prohibiting cybercrime, and making timely review of legal measures to prevail over the cybercrime and ensure criminal justice system in the cybercrime case. Accordingly, to assess the case in Ethiopia, this study utilizes the combination of document analysis and empirical study research methodology to examine cybercrime legal and regulatory responses in the context of the ever-evolving cybercrime, and comparative approach to identify the strong sides and shortcomings. For empirical inquiry, semi-structured questionnaires were used to get relevant information and data were analyzed using qualitative data analysis techniques. Using this data collection method, relevant information has been collected from INSA, MoJ and FPC. Taking into account the knowledge and experience, the respondents were purposefully selected. Moreover, purposive sampling technique is preferred to have individuals that are proficient and knowledgeable with the subject of the study. The assessment showed that Ethiopia has developed comprehensive cybercrime specific law. But still Ethiopia lacks legal regulation on criminal activities committed over internet including revenge pornography, online blackmail, website and email scam and online crime committed through botnet. There is also a need for legal regulation on internet intermediaries (ISPs, Internet café operators, hotels and so forth) to limit the chance of their computer systems or networks being exploited for cybercrime purposes. Finally, Ethiopia needs to establish a cybercrime center that can organize and lead designing cybercrime related programs to produce technology savvy legal expertise, facilitate relevant information and technology sharing, forensic laboratory facilities and conduct research and development, and inter-sectoral collaboration and international cooperation.

Keywords: Cybercrime, Cyber criminality, Enforcement Challenges, Legislative Responses in Ethiopia.

Chapter One

Introduction

1.1 Background of the Study

Through science and technological advancement, a digital platform named 'cyberspace' was created and operates parallel to the physical world. Thus, virtual communication becomes possible and this is essentially happening because of the introduction of the internet. Internet and computer technology provides limitless opportunities for commercial, communication, educational and industrial advancement, to say few. Information and Communication Technology (hereinafter ICT) allow for information to be accessed, business conducted, professional and personal connections grown and maintained, and governments engaged and governance expanded.[1]

Nowadays interconnectivity across the world through the global network system/internet, which helps undertake various activities without even the need of physical presence, is exponentially growing. As reports indicate the worldwide internet users have reached 4.66 billion (59.5 % of the global population).[2] This is an illustration, how much the world's technological dependency is growing day by day. The reason for the daily traffic on the internet increases substantially because users are interested in having access to various websites to consume products/services offered at online avenues. Accessing information and knowledge from websites, the emergency of cloud computing to process and store data, massive reliance on ICTs by companies and government for their service are among things that impel dependence on digital technology.

As researches shown[3], in Ethiopia too, due to mass convergence to digitization which accompanying by the government's commitment manifested through the development of ICTs

[1] World Bank and United Nations, 'Combating Cybercrime: Tools and Capacity Building for Emerging Economies' (2017), Washington. DC p, 16

[2] Statista Report, April 7, 2021 available at <https://www.statista.com/statistics/617136/digital-population-worldwide/> accessed on July 17, 2021

[3] See Yohannes Mebrate, 'E-commerce and The Future Of Competition Regulation Under Ethiopian Law' (LLM thesis, Debre Berhan University, 2020); Iyasu Teketel, Cybercrime in Ethiopia: 'Lessons to be learned from International and Regional Experiences' (LLM Thesis, AAU 2018); Halefom H Abraha, The State Of Cybercrime Governance In Ethiopia (2015) <https://www.researchgate.net/publication/322234805>; Frehiwot Woldehanna al et, Legal Framework for Implementation of m-Government in Ethiopia: Best Practices and Lessons Learnt (2014), Vol. 32 Journal of EEA

infrastructure and telecommunication service expansion[4], which aims to increase internet bandwidth and connectivity speed, reliably over electronic technologies rising.[5] Owing to this awakening, banks have led to embrace electronic banking services, individuals and organizations leap to utilize cloud computers to automate their services. It also facilitates e-governance (one-stop-shop e-payment for phone, electric and water bills, online transport ticketing, e-procurement system[6]) as well.

However, 'as computers are responsible (directly or indirectly) for every aspects of our life, starting from the operation of our cars to our banking and 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'.[7] According to an International Business Machines Corp. (Hereinafter IMB) report, in 2020, 80 % of data breach incidents resulted in the exposure of customers' personal identification information.[8] So, many countries and international bodies have embraced the need to deal with cybercrimes. Typically, the EU Convention on Cybercrime and AU Convention on Cyber Security and Personal Data Protection are some of the international undertakings to pave the way for harmonization among domestic anti-cybercrime efforts.

Cybercrime is a sort of crime committed through the use of a computer or other smart device and using the help of the internet to connect to the target of the attack. It endangers the safety of users – their property or their personal data, organizations and government. Essentially, this is because, *inter alia,* the technologically illiterate of the vast majority of users and the far-reaching ability of criminals to circumvent technology for its malevolent activities – which even overreach countries'

[4] Ethiopian Monitor, February 4, 2020, Available at <https://ethiopianmonitor.com/2020/04/ethio-telecom-launches-lte-advanced-mobile-service/> Accessed on July 20, 2021; the Ethiopian government paid Huawei 173 million ($5.6 million) to install LTE network infrastructure in Addis Ababa as part of expansion plan; See also Ezega News, January 23, 2019, <https://www.ezega.com/News/NewsDetail/6913/Ethiopia-to-Increase-Internet-Gateway-Capacity> Accessed on July 20, 2021; Available at <https://www.ericsson.com/en/press-releases/1/2021ethi-telecom-and-ericsson-launch-4g-network-for-south-west-ethiopia-at-major-event-in-jimma> Accessed July 20, 2021

[5] See Abenezer B. Weldegiorgis, 'Developing National Cybersecurity Strategy For Ethiopia' (Master thesis, Tallinn University, 2019), the survey shows that among organizations respondent to the survey 60% are highly, 33% medium and the rest 7% less reliance on ICT

[6] Public Procurement and Property Administration Agency announce government e-procurement system will be introduced and piloting began in collaboration with selected federal offices, Available at <https://chilot.me/2021/07/06/electronic-procurement-to-be-operational-from-july-7/amp/> Accessed July 20, 2021

[7] James R. Richards, 'Transnational Criminal Organizations, Cybercrime and Money Laundering' (A Handbook for Law Enforcement Officers 1999) 88

[8] IMB Report, Aug 10,2020, Available at <https://www.dbta.com/Editorial.News-Fleshes/IBM-2020-Cost-of-Data-Breach-Study-True-Cost-of-Todays-Security-Glitches-142198.aspx Accessed on July 18, 2021

cyber security measures. The criminals may have committed it through the dissemination of malicious programs/software, making unauthorized access or system interference into computer systems, data, or networks. Such manipulation of ICT resources and online or computer operations for illegal activity will have undesirable consequences. Computer crimes or cybercrimes have various impacts on the national security of a given state, economy, privacy, public morals, and on life.[9] Moreover, cybercrime is a borderless crime that will be committed from elsewhere untraceable use of the advantage of anonymity that the internet gives. So, it is imperative to have a legal regime criminalize misbehavior involving computer systems or the internet. Having regulatory mechanisms carrying out successful detection, response, prevention, investigation, and punishment of cybercrime incidents is equally important. Also, undertaking such activities in coordination and cooperation at national level and adherence to international cooperation frameworks to deal with this boundless crime would lead to properly countering its consequences.

As Ethiopia delves into digitization with all effort in creating an enabling legal framework and technique that support the transformation, its vulnerability to cyber-involved attacks is unlikely impossible. Thus, at this point, it is unquestionably crucial to design and implement equivalent technical and legislative measures to remain on the top of the problem. Overtly, Ethiopia is dealing with the risk of cybercrime, as the country is no exception to this global problem. Information Network Security Agency's (hereinafter INSA) report indicates that, in 2019 cyber-attack has launched against financial institutions across the country which cause shut down of the internet for about thirty minutes to respond to the attack.[10] This incident has shown us how the country struggles to abort the attack through the existing legal frame and technical ability without shutting the internet as the country isn't yet built on legal and institutional readiness. Again, in the year 2020, Hacker groups based in Egypt, which identified as "Cyber Horus Group", "AnuBis.Haker" and "Security Bypassed" attempted cyber-attack against Grand Ethiopian Renaissance Dam (hereinafter GERD) aimed to disrupt the second water filling and operation of the dam and defaced thirteen government and four non-governmental institutions websites.[11] In the year 2020/2021

[9] Molalign Asmare, 'Computer Crimes in Ethiopia: An Appraisal of the Legal Framework' (2015) Vol. 3, Issue 1, International Journal of Social Science and Humanities Research, p, 96, Available at: <www.researchpublish.com>

[10] Ezega News, December 6, 2019, Available at <https://www.ezega.com/News/NewsDetails/7518INSA-Aborts-Cyber-Attacks-on-Financial-Institutions> Accessed July 19, 2021

[11] Available at <https://borkena.com/2020/06/22egypt-based-hackers-attemted-cyber-attacks-on-ethiopia-govt-sits/> Accessed on July 19, 2021

more than 2,800 cyber-attack had been attempted, that is more than (1080 incidents were recorded in 2019/2020) last year recorded incidents.[12] Thus INSA suggests that the organizations must strengthen their cyber security systems so as to resolve future attempts. Moreover, another survey also indicates that cyber-attack incidents have been on the rise and this is essentially due to growing ICTs reliance in Ethiopia.[13] It has been carried out against information systems/networks (to undermine confidentiality, integrity and availability of computer systems, network and data). This is, by making unauthorized access, illegal data interception and acquisition – offenders often use it for harvesting personal and financial data to cash out it at the black market. It may also be carried out to disrupt critical infrastructures that rely on ICTs; such as water and electric supply systems, bank systems, health facilities, telecom services, among others.

Obviously, weak anti-cybercrime measures have put the country in 115th position in the Global Cybersecurity Index (hereinafter GCI). In addition, in 2020 Cybersecurity Exposure Index (hereinafter CEI) listed Ethiopia next to Afghanistan and Myanmar as top most exposed country to cyber-attack.[14] Therefore, the challenge that encounters countries like Ethiopia is the question of how to combat the evolving tendency to cyber criminality and hence preserve many positive aspects of our interconnected world.

1.2 Statement of the Problem

As it is quite understandable from the government's strategy direction, Ethiopia is committed for technological change to back social development, productivity improvements and inclusive growth.[15] However, this transformation into the digital world does not come without a risk, it may cost the country in various aspects of economic, social and security. The threat of cybercrime has not been exacerbated; this is, by considering the country's effort for digitization that culminated with the rapid growth and expansion of ICTs infrastructures with nascence cyber-security strategy

[12] Xinhua News, 2021-09-07, 'Cyber-attack attempts more than double in Ethiopia this year: official', Available at fhttps://www.news.cn/english/african/2021-09/07/c_1310171963.htm> Accessed July 19, 2021

[13]Abenezer B. Weldegiorgis, 'Developing National Cybersecurity Strategy for Ethiopia' (n 5) p. 42-43, Tewodros Getaneh, 'Cyber Security Practice and Challenges at Selected Infrastructures in Ethiopia: Towards Tailoring Cyber Security Framework (Master thesis, AAU, 2018)', Halefom H. Abraha, 'The State of Cybercrime Governance in Ethiopia' (n 3)

[14] Cisomag News, Available at <https://cisomag.eccouncil.org/cybersecurity-exposure-index-2020-reveal-most-vulnerable-countries/amp/> Accessed on August 12, 2021

[15] FDRE, Digital Ethiopia 2025 A Strategy for Ethiopia Inclusive Prosperity

which isn't at the level to deter cybercriminals from exploit technological developments for their ill deed.[16] Ironically, as the technology based crimes are intensifying following the adoption of ICTs based services that have been underway throughout financial institutions, private and public sectors in the country. The government should have to take time and think about the security measures to combat cyber-security threats and cybercrime. Alongside the effort to develop ICTs enabling environment, it is indispensable to design legal and technical measures that mitigate the risks and boost users' trust in electronic based service and protect the whole computer systems (networks, data and information systems). Importantly, beside the work done in Ethiopia to support digitization, at the same time enacting a regulator regime, to reduce the adversity of such transformation, should be a top policy agenda.

Following this concern, Ethiopia has specifically cognized, by the time when the National Information Security Policy (hereinafter NISP) was enacted[17] vulnerability of its cyberspace to cyber-attack. Basically, its vulnerability is because of the country's decision to join global network systems and introduce internet service. Even before the adoption of NISP, technological advancement has taken as a major justification to amend the 1959 Ethiopia penal code by the FDRE Criminal Code 414/2004.[18] Nevertheless, the rules under criminal code provide scant regulation against threats posed on cyberspace or crimes carried out over the internet (i.e., cybercrime). Perhaps, this might be due to the nascence of the internet or little understanding on the nature and complexity of cybercrime by then time. At the end, in 2016, the computer crime proclamation which is the first of its kind was enacted and hence its rules outlaws unprecedentedly enormous types of cybercrimes.[19] Whereas, it is important to assess whether this cyber specific proclamation criminalizes as much online illegal activities to limit their effect. Activities such as production and dissemination of racist and xenophobic content data, intellectual-property related crimes, revenge pornography, and large-scale cyber-attacks through botnets that have been seen as a great threat to information society. In this sense, the Ethiopian cybercrime legal regime has

[16] Ibid, 42-43; Halefom H. Abraha 'The State Of Cybercrime Governance In Ethiopia', (n 13) 6-7
[17] FDRE National Information Security Policy, Available at <https://www.insa.gov.et/documents/20124/0/National+Informattion+Security+Policy.pdf/45e78efa-d671-4fbc-16c7-38eb1c70e35d?t=1600929143177&download=true> Accessed at July 26, 2021
[18] FDRE Criminal Code Proclamation No. 414/2004, entered into force May 9, 2005, under its preface par. 2
[19] Computer Crime Proclamation No. 958/2016 (Computer Crime Proclamation), entered into force 2016

been strictly probed under this study to examine its adequacy particularly computer crime proclamation in combating emerging cyber criminality.

Following the introduction of ICTs and the internet in Ethiopia, electronic transactions have been further promoted, facilitated and recognized by law.[20] Furthermore, e-commerce, e-governance, e-payment systems gain legal status and are imputed in the Ethiopian legal system. Recently, as part of the process of digitizing the economy, the country has signed an e-commerce agreement in 2019 with Alibaba Group for the establishment of the electronic world trade platform (eWTP) in Ethiopia.[21] Spectacularly, this is a step ahead to underpin e-commerce in the country with the aim to ensure and guarantee electronic transactions replacing paper-based transactions. Indeed, Ethiopia is heading, more widely than before, for mobile banking and e-financial service thus likely to face financial frauds and offenses. If not regulated properly to accommodate newly emerging criminal activities that are based on technological advancement with proactive institutional systems otherwise this will cost the country's economy.

Developments in information technology have also led to the recognition of online or digital identities. Hence, computer crime proclamation provides rules prohibiting illegal access, causing damage to personal information and identity theft to protect digital privacy invasion.[22] With the introduction of internet, pornographic related websites, magazines, photos, pictures, books and writings proliferated over internet and worldwide webs. So cyber pornography is become huge online business/industry with easy way to spoil societal value, moral and decency. Although pornography is not yet illegal in many countries including Ethiopia, save child pornography that is criminalized and made punishable under article 12 of computer crime proclamation. Generally, at this juncture, the question which needs an inquiry regarding Ethiopian cybercrime legal regime is whether it is adequate to prevent cybercrimes like data breach, identity theft, production and dissemination of illegal content data, online forgery and fraudulent *etcetera*.

[20] Electronic Signature Proclamation, Proclamation No. 1072/2018, enter into force 16th Feb, 2018; Electronic Transaction Proclamation, Proclamation No. 1205/2020, entered into force 30 June 2020

[21] Addis Standard, November 25/2019, Available at <https://addisstandard.com/news-alibaba-group-to-help-ethiopia-set-up-first-ewtp-hubthe-second-in-africa/> accessed on July 14, 2021

[22] Computer crime proclamation, Art. 3, 6 & 11

Regarding regulatory capacity in enforcing cybercrime law, Iyasu Takele, in his study indicate that the cyber unit under the Federal Police Commission (hereinafter FPC) 'has no capacity to investigate cybercrimes dealing with cybercrime per se such as hacking, spam, Denial of Service and the like at all'.[23] As he argued, even the legislative, regulatory and institutional frameworks have been overreached by the criminals due to the limited expertise, forensic technology equipment and lack of coordination among institutions empowered.[24] Having this in mind, this research pursued to assess, if any, the improvement with those institutions concerned about their human capital, relevant forensic technological and strengthen inter-sectoral coordination and cooperation to reinforce implementation of cybercrime law. To look at if there is any improvement enabled to carrying out effective enforcement of the law, detection, investigation and prosecution of cybercrimes. Obviously, enacting as much legislation alone would not effectively serve the purpose of crime control; rather it should be reinforced by strong regulatory and institutional mechanisms. Equally, creating strong protection and punishment in order to defend intrusion against information systems and undermine electronic communication is important.

As has been understood from the above, Ethiopia has been striving to integrate computer and internet technology for the digitization of areas related to commerce, communication and financial systems, most likely there is a growing negative impact of cybercrime. Therefore, it is highly important to inquire into the compatibility of the existing cybercrime legal and regulatory responses in terms of its capability to combat cybercrime and guarantee legality of online transactions in Ethiopia. Also, as a basis for understanding the challenges and strength in curbing technologies related crimes in Ethiopia, the research intended further to conduct comparative analysis with selected jurisdictions to get their best practice and experience for Ethiopia.

[23] Iyasu T., 'Cybercrime in Ethiopia' (n 3), 51

[24] Ethiopian Monitor, August 24, 2020, Available at <https://ethiopianmonitor.com/2020/08/24/insa-thwarts-787-cyber-attacks-on-ethiopia-in-2019-20-fy/> Accessed September 8, 2021. Deputy Director of INSA, Kefyalew Tefera affirmed that 'Over 90 percent of cyber-attack occurred due to lack of proper tech knowledge'

1.3 Research Objectives

1.3.1 General Objective

The general objective of the study is to examine the Ethiopian legal and regulatory frameworks in combating cybercrime, and upon comparison with other jurisdictions to identify the strength and shortcomings of cybercrime legal regime in Ethiopia thus to draw some best lessons.

1.3.2 Specific Objectives

- To examine Ethiopian cybercrime law in the context of the evolving cybercrimes whether it properly contemplates the concern and is capable of combating its effect.
- To review other jurisdictions' experience in the fight against cybercrime threats using the legal and regulatory measures and hence to import some best lessons for Ethiopia.
- To identify and analyze the challenges encountering the process of controlling cyber criminality and enforcement of cybercrime law in Ethiopia.

1.4 Research Questions

1.4.1 General Question

The general question of this study lies at the heart of examining whether the Ethiopian legal and regulatory frameworks are sufficiently designed to address cybercrime in the country, and can Ethiopia have some lessons from the selected jurisdiction?

1.4.2 Specific Questions

1. Is the Ethiopia cybercrime legal regime sufficiently contemplating the evolving cyber criminality and capable to combat cybercrime committed from inside or outside the country?
2. How do other jurisdictions approach the threat of cybercrime through their legal and regulatory measures and what lessons can Ethiopia draw from?
3. What challenges have encountered the process of controlling cyber criminality and enforcement of cybercrime law in Ethiopia?

1.5 Significance of the Study

As the objective of this study is to examine Ethiopian cybercrime legal regime in context of the evolving cyber criminality, this research's outcome is expected to have the importance of serving as literature for those interested to conduct their study in the same area. Also, it has brought relevant information that indicates legal gaps and challenges facing law enforcement to the attention of policy makers.

1.6 Scope of the Study

The focus of this study is on examining the legal and regulatory measures of cybercrime in Ethiopia. Thus, it is scope is limited to examine legal and organizational framework to address the research questions and objectives, among the five pillars set by ITU[25] (which are legal measures, technical and procedural measures, organizational structures, capacity building, and international cooperation).

1.7 Limitation of the Study

Noting the subject matter of the study which has been a recent phenomenon across the world particularly in Ethiopia, this fact has made the finding of literature as much as required for review and studying purposes hard. Alongside this difficulty, the tight bureaucracy from governmental bodies to be willing to share relevant information and other constraints such as time, resources, COVID 19 restrictions and security problems associated with law enforcement operations happening in the country were additional burdens to the researcher. These all, therefore, have their own contribution to limit the study from not going as per scheduled timeline.

1.8 Literature Review

The literature in this study has been reviewed based on the guide of its subject. But regarding the availability of academic, practical reports and writing on the issue, due to its steady growth over time coupled with having recent history, it is hard for the researcher to get as much literature as

[25] ITU Global Cybersecurity Agenda (GCA), 'Framework for International Cooperation in Cyber-security', Available at <www.itu/cybersecurity/gca/>

found on other fields of studies both at international and Ethiopian context. However, the researcher was able to access some of the following works and reviewed them as follows.

About how cybercrime is a growing challenge to the world, ITU in its report of 2012 titled '*Understanding cybercrime: Phenomena, challenges and legal response'* underscored that notwithstanding to the benefit of ICTs and the internet, there has been a growing concern of cybercrime to which especially developing countries should worry about.[26] Also the report stressed along with legal responses, cyber-security measures (protection technology) should be integrated while ICTs infrastructure or the internet bandwidth development efforts are undertaken and this is used to counter cybercrime. A study conducted by the Open-ended Intergovernmental Expert Group, a working group established under resolution 65/230, indicates how cybercrime has become an international threat that requires cooperation among countries.[27] The fast internet interconnectivity becomes a means to exploit the electronic technology for criminal opportunities that demand legal harmonization: harmonization in terms of criminalization, jurisdiction, national coordination and cooperation, electronic evidence gathering mechanism and international cooperation to strengthen legal and other responses to cybercrime.

Literature in the context of Ethiopia overall tells us how the cyber security threat and cybercrime are impacting the national economy, security, public interest and individual human rights and fundamental freedom. Accordingly, Abenezer B. Weldegiorgis,[28] argued that there is impelling ground to adopt a new policy in Ethiopia which shall be in tune with the current cyber security context of the country. He further states that the situation in the country has changed on information technology – as linking critical infrastructure to ICTs is massively underway – and economic and political ideology reform – to allow privatization of state-owned firms. Beyond this, ICTs and the internet resulted in a cyber-security threat and cybercrime that could not be responded to by the traditional justice system, so he urged for updating the existing policy. Emphasizing the importance of having comprehensive laws on digital technology in Ethiopia, Kinfe Micheal Yilma and Halefom Hailu Abraha in their article titled '*The Internet and Regulatory Responses in*

[26] ITU, 'Understanding cybercrime: phenomena, challenges and legal response', Available at: <www.itu.int/ITU-D/cyb/cybersecurity/legislation.html>

[27] United Nation Office of Drug and Crime (hereafter UNODC), 'Comprehensive Study on Cybercrime' (February 2013)

[28] Abenezer B Weldegiorgis, 'Developing National Cybersecurity Strategy for Ethiopia', (n 13)

Ethiopia: Telecoms, Cybercrimes, Privacy, E-commerce, and the New Media'[29], criticized the sector-specific approach and suggested sweep to coherent legal and regulatory responses. In this work they help us to understand the overall developments in convergence of telecommunication, broadcasting and information technology due to digital technology and the level of response in legal and regulatory means to this development. However, insofar as by the time computer crime proclamation was underway the drafting process, it does not become the point to be discussed as such and their discussion doesn't go more than highlighting the importance of the draft bill. In showing how much the Ethiopian legal system is in need of specific law deals with emerging technology-based crime, Molalign Asmare in his research entitled '*Computer Crimes in Ethiopia: An Appraisal of the Legal Framework'*[30], describe the situation along the international dimension. Based on this inquiry, he then concluded that the Ethiopia legal regime 'did not carefully and sufficiently criminalize according to their unique nature, impacts, and the provided punishments are disproportionately lenient'. But as the work dwelled in examining computer crime provisions under criminal code, fails to assess the perspective of cybercrime and measures taken afterward of computer crime proclamation.

Again, Kinfe Micheal Yilma in his article named *'Some Remarks on Ethiopia's New Cybercrime Legislation*' poses concern on the computer crime proclamation relating to its human rights implication and the practical challenge it will face at the time of its implementation.[31] Apart from his remark on computer crime law which brings a comprehensive and human right oriented approach, he states that the proclamation left too much to criminalize emerging cybercrimes and it is a missed opportunity. Regarding Ethiopia's state of information technology development and its ensuing cyber security related problems, Halefom Hailu Abraha under '*The State of Cybercrime Governance In Ethiopia'* wrote a well descriptive report.[32] Under this article, he depicts the picture of cyber security governance and conclusively proves the growing cybercrime incident has overreached the existing legal framework so that suggests further effort to be done. Insofar as, this report was written by the time when the computer crime law was under drafting stage, so it does

[29] Kinfe M. Yilma and Halefom H. Abraha, 'The Internet and Regulatory Responses in Ethiopia: Telecoms, Cybercrimes, Privacy, E-commerce, and the New Media', Available at <http://dx.doi.org/10.4314/mlr.v9i1.4>
[30] Molalign Asmare, 'Computer Crimes in Ethiopia: An Appraisal of the Legal Framework' (n 9)
[31] Kinfe M. Yilma, 'Some Remarks on Ethiopia's New Cybercrime Legislation' (2016), Vol. 10, No.2, Mizan Law Review, 455 DOI http://dx.doi.org/10.4314/mlr.v10i2.7
[32] Halefom H. Abraha, 'The State of Cybercrime Governance in Ethiopia', (n 16)

not examine the situation after the enactment of the enactment of the proclamation. And it does not also assess the functioning of the unit practically organized like Computer Emergency Response Team (hereinafter CERT) under INSA, cyber concerned department under Minister of Justice and Cyber Unit under Federal Police Commission (hereinafter FPC). The other reviewed literature is Iyasu Takele's research thesis titled *'Cybercrime in Ethiopia: Lessons to be learned from International and Regional Experiences'* which highlighted the current legal regime of Ethiopia along the international cybercrime instruments to examine its conformity to international standards.[33]

All the aforementioned works are the result of assessments done before the country enacted important instruments such as computer crime proclamation, hate speech and disinformation laws and other cybercrime implicated laws, which did not fit the current cybercrime context of the country. And the others are done with the intent of making a comparison of the Ethiopian cybercrime legal regime along with the standard of the international cybercrime regime. However, under this study, in a comparative perspective, the Ethiopian legal regime's adequacy will be assessed along with the evolving digitization, and ensuing cyber criminality.

1.9 Research Methodology

This study utilizes the blend of doctrinal and empirical research methodology to address research objectives and questions. A comparative approach has been employed to draw best practices to Ethiopia. To do so, both primary and secondary data collection tools were used. In analyzing the data, qualitative data analysis techniques were used to triangulate the respondents' opinion, attitude and experience along with subjects under study to reach relevant and supportive data.

1.9.1 Document Analysis

The study uses document analysis to have the required level of understanding on the subject matter. To do so, international legal documents such as the EU Convention on Cybercrime and AU Convention on Cyber Security and Personal Data Protection along with Computer Crime Proclamation of 958/2016 and other relevant national laws that have cybercrime implication have been examined. In addition, secondary sources such as books, reports, journal articles and website

[33] Iyasu T., Cybercrime in Ethiopia: 'Lessons to be Learned from International and Regional Experiences', (n 23)

sources were consulted to get as much relevant information. The study involves comparative analysis of literature and jurisprudence of other jurisdictions to examine the level of Ethiopian legislative and regulatory responses. The comparison has been made with India and Nigeria; these jurisdictions were selected upon accounting the following criteria.

First, based on prioritization that has been given to cyber-security at national level. Cyber-security has emerged as an area of priority for Indian lawmakers following repeated security lapses within existing information structures and policy direction for increasing digitization and access to the internet.[34] In Nigeria also due to the negative financial and economic consequences that cybercrime poses, the government had taken drastic measures, *inter alia*, by establishing a presidential committee on cybercrime to identify root causes and solutions to overtake the problem.[35]

The second criterion for the selection is the commitment to improve and take step ahead of the existing cybercrime governance measures in their respective jurisdiction. In terms of strength of cybercrime governance, Africa has been identified as a safe harbor for cyber criminals by TREND Micro Incorporated; this has been because of higher internet penetration rate, affordable internet access along lenient cybercrime law. In this respect, Nigeria is one of the countries where cybercriminals migrated into until it strengthened its anti-cybercrime measure as noted by the Nigerian Economic and Financial Crime Commission (hereinafter EFCC).[36] India also timely recognized its cyber vulnerability stem from national ambition for digitalization and hence the government takes measures to strengthen its legal regulatory and employ cyber readiness index to assess its readiness against potential cyber risks.[37]

The third justification lies at the countries' effort to set collaboration schemes among concerned national bodies, and a commitment to join and cooperate under an international framework to curb cyber-security threat and cybercrime. In this view, the Nigerian government has held partnership

[34] Divij Joshi, A comparison of legal and regulatory approaches to cyber security in India and the United Kingdom, The Center for Internet and Society, 8

[35] Muktar Bello, 'Investigating Cyber Criminals in Nigeria: A Comparative Study', (Doctoral Thesis, Business School College of Business and Law University of Sanford, UK. 2018) 45

[36] Nir Kshetri, 'Cybercrime and Cybersecurity in Africa' (2019), Vol. 22, No. 2, Journal of Global Information Technology Management, 78

[37] Melissa Hathaway et al, 'India Cyber Readiness at A Glance', (December 2016), see also GCI report 2020, India achieves 10th upon improved its previous position 37th in 2018 under Global Cybersecurity Index

with national private stakeholders to raise awareness in the fight against cybercrime and with Microsoft to tackle cybercrime and software piracy in Nigeria.[38] In this regard India had already taken numerous steps including signing 39 mutual legal assistance treaties with various countries and becoming a member of the Shanghai Cooperation Organization to reduce cybercrime.[39]

Lastly, the two legal systems have been selected because the researcher is able to access literature that concerns these jurisdictions' cybercrime context and cyberlaw to make this comparative study more than can be found in other jurisdictions on the same issue. Accordingly, as Ethiopia has strides to tackle the threat in its cyberspace to secure the benefit of information technology, there is a lot that the country will learn from these countries' progressive achievements. Therefore, these foreign jurisdictions' legal framework and experience were selected to draw best practice for Ethiopian in its endeavor to tackle cybercrime and benefited from electronic communication and information systems instead.

1.9.2 Empirical Study

For empirical inquiry, semi-structured questionnaire technique was selected. This method was opted as the other data collection method like observation and interview are difficult to employ considering institutions designed for such propose were hardly accessible in terms of time, resource and bureaucracy. Therefore, semi-structured questionnaire method preferable to get relevant information from concerned public offices and their experts. Its purpose (empirical work) is to provide explanations and understanding towards the legislative and regulatory responses against cybercrime in Ethiopia from the practical respect of practitioners and experts in the field. Furthermore, it is justified because it helps the researcher to gather in-depth information from respondents about the subject matter under study. More precisely, the researcher therefore is highly interested in this data collection method because it offers the chance to obtain experts' opinion and view in advance. In this scenario, the respondents also have the opportunity to add extra but relevant information which isn't within the knowledge of the researcher to ask. Moreover, if not for such a method the key points will be missed otherwise.

---

[38] Muktar Bello 'Investigating Cyber Criminals in Nigeria: A Comparative Study' (n 35), see also Maurice Ogbonnaya, 'Cybercrime in Nigeria demands public-private action', 2020, Available at <https://issafrica.org/iss-today/cybercrime-in-nigeria-demends-public-private-action> Accessed on August 15, 2021, Kshetri (n 37) 81

[39] Hathaway et al, India Cyber Readiness at A Glance, (n 38) 12

Using this data collection method, the researcher puts utmost effort to access, collect relevant information from experts of relevant government organs i.e., Information Network Security Agency (INSA), Minister of Justice (MoJ) and Federal Police Commission (FPC) Cyber Crime division. By taking into account the knowledge and experience, the respondents were purposefully selected. Based on such criteria that sample population (sampling) has been determined and respondents were selected from a specific division that is devoted to deal with cybercrime and related issues. Moreover, purposive sampling technique is preferred because it helps the identification and selection of individuals that are proficient and knowledgeable with the subject of the study. Regarding sample size, the total of 17 respondents were selected. The number of populations is limited to save time, energy, money and the researcher believes data that would have been collected from the entire population could have been extracted from the samples at such a required amount and quality. However, based on the variation of and out of the vast responsibility vested, 7 (seven) respondents were selected from INSA and MoJ respectively. And the remaining 3 (three) were from the FPC Cybercrime unit.

1.10 Ethical Consideration

The researcher has pursued this study with utmost care of the key ethical principles, among others, seeking informed consent of respondents, respecting confidentiality of the information and ensuring quality and genuineness of the research. In this vein, the researcher first seeks letters of cooperation from the School of Law and Governance Post-graduate Program Coordinator at Jimma University, to get access to selected institutions. Then the researcher submits the letter to secure their willingness and cooperation by describing the subject matter of the study. Specifically, they have said that their response is for this research only and vow for its confidentiality. To be most cautious, as the research seeks to obtain sensitive information from such targeted institutions, confidentiality is a matter of relevance, so it doesn't be negotiable. Thus, the researcher has put due effort to guarantee anonymity of information obtained through the interview, to do so, a pseudonym has been put in use while their responses is analyzed.

1.11 Organization of the Study

This study has been organized in five chapters. The first chapter is a research proposal. Chapter two is the discussion on the conceptualization of cybercrime. Chapter three presents comparative analysis of cybercrime law in context to examine Ethiopian legal and regulatory responses along with selected jurisdictions and to import the best practice for Ethiopia. Chapter four, under this chapter of the study, the challenges facing cybercrime control and enforcement of cybercrime law in Ethiopia are going to be discussed. The chapter also discusses the mechanisms in use to curtail cybercrime in Ethiopia. The final chapter, chapter five contains the conclusion and recommendation of the researcher based on the findings.

Chapter Two

Cybercrime: Definition and Conceptual Overview

Introduction

Firstly, the conceptualization of cybercrime is crucial in order to study the issue, most importantly, for lawmakers to design effective cybercrime law. If not, the attempt to enact the law appears futile and it becomes difficult for LEAs to implement the cybercrime law effectively.

Precisely, in the study of cybercrime, *inter alia,* one of the major problems is the lack of consistency in defining cybercrime, albeit there are some basic definitions provided by scholars and legal instruments that help us to understand the concept. Thus, under this chapter the study tries to grapple with the meaning of cybercrime, discussing the types of cyber or computer crimes focusing on those prevalent in Ethiopia. Followed by the sections examine the impact of cybercrime and the need for understanding cybercrime. Finally, we are discussing the technique utilized by cybercriminals and the anti-cybercrime strategy employed by state's LEAs.

2.1 Definition of Cybercrime

Cybercrime is a very broad term with various meanings. The definition can include everything from technology-enabled crimes to crimes committed against individual computers.[40] As a result, various terms have been used to describe cybercrime, including; computer crime, technological crime, high tech crime, online crime, internet crime, economic crime, electronic crime, digital crime. Although it is still the case that no one term has become truly pervasive.[41] It has been therefore reasonable to use the terms cybercrime, computer crime and computer related crime interchangeably as none of the terms is full-fledged to be used independently. Thus**,** these terms have also been used interchangeably in this research.

[40] Odumesi John Olayemi, 'socio-technological analysis of cybercrime and cybersecurity in Nigeria' (2014), Vol. 6(3), International Journal of Sociology and Anthropology, 118
[41] Jonathan Clough, 'Principles of Cybercrime' (Cambridge University Press, 2010) 9

Also, regarding the definition of cybercrime, there is no internationally recognized legal definition.[42] This has become a challenge in drawing all-encompassing legal norms in combating cybercrime that is trans-national in nature. Lack of uniformity in definition has negated the harmonizing effort of domestic cybercrime legislation to reinforce law enforcement and cooperation among countries. Insofar as criminals will be able to raid cyber-attack from elsewhere; from where they can access the internet, against information technology and computers systems undetectable, the countries must harmonize their domestic cybercrime law to promote cooperation among themselves and deter cyber criminals. Otherwise, this may cause difficulty to apprehend or timely collect relevant electronic evidence to conduct investigation and prosecution. Of the uniformity needed in fighting cybercrimes, the law is still lacking an adequate degree of uniformity. Moreover, the absence of consensus in defining cybercrime is contributory to the lack of related conceptions across jurisdictions that help to harmonize cybercrime law. In addition, this lack of definitional clarity is problematic as it impacts every facet of prevention and remedy.[43] Therefore, a considerable degree of legislative harmonization is vital if effective regulation is demanded to be achieved. Underline, by means of legal harmonization doesn't mean to have the same cybercrime law; instead, it means to have a similar concept of cybercrime across jurisdictions.

Hereunder, based on such a motive, we are going to examine literature and try to understand the conception of cybercrime dictated therein. To start with, some were conceived as a computer crime as criminal activity involves computers as a subject, tools/means and source of criminal activities. For Z. Okemuyiwa[44] Computer crime is a criminal activity that targets computers or uses computers as a means of committing a crime. However, nowadays with the introduction of the internet, computer crimes have changed their attribute as the online interconnection of computers enables other ways of commission by using networked computers, for example, illegal access, email spoofing and business email compromise. And also, a method that presents new means to commit traditional crimes has proliferated. On the other hand, for McGuire and Dowling, "Cyber-

[42] Roberto Flor, 'Cyber-Criminality: Finding a Balance between Freedom and Security'; S. Manacorda (ed), ISPAC, (Milano, 2012) 13

[43] Hamid Jahankhani et al, 'Cybercrime classification and characteristics' (2014) 152, Available at <https://www.researchgate.net/publication/280488873>

[44] Adedeji Akeem Z. Okemuyiwa and Ibraheem Ohinoyi Akeem, 'Cyber Crime and Policing in Nigeria: Issues, Challenges and Prospects'

dependent crimes are offenses that can only be committed by using a computer, computer networks, or other forms of ICT" such as creation or/and distribution of malwares/viruses,[45] whereas cyber enabled crimes "can still be committed without the use of ICT" such as cyber fraud.[46] In their part, Animesh Sarmah *et al*[47] define cybercrime as an illegal activity that takes place over electronic communication or information technology which involves computers and networks for its commission. In the same manner, Ufuoma V. Awhefeada1 & Ohwomeregwa O Bernice, define cybercrime 'as a commission of clandestine and criminal activities in a cyberspace using a computer which is connected to a type of network as enabled by network provider'.[48]

Some others consider "Cybercrime" and "Computer crime" differently.[49] The former is narrower than the latter and it has been used to describe illegal activities involving computer networks or the internet.[50] On the other hand, 'Computer crimes' cover those offenses that bear no relation to a network, but only affect stand-alone computer systems.[51] Therefore, in its narrower sense, cybercrime means an act of illegal nature committed against computer systems using electronic devices interconnected through the internet. Whereas in its broader meaning, it encompasses any misuse of information systems to commit crime against computers (i.e., computer system as target), or using computer operation as a tool to carry out even conventional crimes (i.e., this time computer network or system is used as a tool). In defining computer crime, Doris Karina[52] classified it into criminal activity in abusive use of physical ICTs resources without authorization from the owner, namely "Computer crime" and offense which is committed in the virtual environment using computer and the internet i.e., Cybercrime.

---

[45] As quoted by Suleman Ibrahim, 'Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals' (2016), Vol 47 International Journal of Law, Crime and Justice, 45

[46] Ibid

[47] Animesh S. et al, 'A brief study on Cyber Crime and Cyber Laws of India' (2017) Vol 04 Issue 6, IRJET 1633.

[48] Ufuoma V. Awhefeada & Ohwomeregwa Ogechi Bernice, 'Appraising the Laws Governing the Control of Cybercrime in Nigeria' (2020), Vol. 8, No. 1, Journal of Law and Criminal Justice, 32

[49] Kabiru H. Mohammed, *et al*, Cybercrime and Digital Forensics: 'Bridging the gap in Legislation, Investigation and Prosecution of Cybercrime in Nigeria' (2019), Vol. 2 Issue. 1, International Journal of Cybersecurity Intelligence & Cybercrime, 56-57

[50] Grercke, Marco, Understanding Cyber Crime: Phenomena, Challenges and Legal Responses, ITU Publication, (2012) 11, Available at <www.itu.int/ITU-D/cyb/cybersecurity/legislation.html>

[51] Ibid

[52] Doris Karina, 'Thea Vulnerability of Cyberspace - The Cyber Crime' (2017), Vol 2 Issue 1, J Forensic Sci & Criminal Inves, 2

Beside the above discussion in the literature about the meaning and definition of cybercrime, there is also a legal definition that has mentioned what constitutes cyber or computer crime. The definition proposed by the US Department of Justice refers cybercrime as 'criminals use mobile phones, laptop computers, and network servers in the course of committing their crimes, in some cases, computers provide the means of committing crime…in other cases, computers merely serve as convenient storage devices for evidence of the crime.'[53] This definition has accommodated the dynamic nature of technology while grappling with the concept; it considers the fact of growing use of mobile phones in the commission of cybercrime. Again, it classified computer crime based on the involvement of computers into three categories. These are, computers as a target of computer crime, computers as tools (means of commission) and computers as instruments to commit criminal activities. Again, the Council of Europe *Convention on Cybercrime*[54] provides a model definition that may help the attempt of harmonization. This definition encompasses four categories of offenses; i.e. '*offenses against the confidentiality, integrity and availability of computer data and systems, traditional computer-related offenses, content related offenses and copyright infringement and related rights'*.[55] Besides, the endeavors made by academicians, and various international and domestic documents to define cybercrime and its constitutive elements, many countries, including India and Nigeria, fail to define in their law that is initial as well fundamental in the work to prevent and control the problem. Moreover, lack of defining the subject matter that is at the core of labeling offense and prescribing punishment to defend individual, organization and national interest from cybercrime will considerably hamper the effort of tackling cybercrime.

Contrarily, in the case of Ethiopia, the Computer Crime Proclamation of 2016 has provided the definition of computer crime unlike the FDRE criminal code which provides rules regarding computer crime for the first time in the country. The proclamation defines computer crime under its article 1(1) as *"Crime committed against a computer, computer system, computer data or computer network; a conventional crime committed by means…or Illegal computer content data disseminated through a computer, computer system, or computer network".* From this definition,

[53] Ed Hagen & Nathan Judish, Searching and Seizing Computer and Obtaining Electronic Evidence in Criminal Investigations, (Office of Legal Education Executive Office for United States Attorneys, 2009) 9
[54] Council of Europe, *Convention on Cybercrime* ETS No. 185, (Budapest, 2001)
[55] Jonathan Clough, 'Principles of Cybercrime', (n 42) 23

we can understand that computer crime, in Ethiopia law, is classified into three basic categories, this is, criminal activity which takes computers as a target, as means to commit other crime and content related crime. As Molalign A. argued that these classifications by the Ethiopian computer crime proclamation are seemingly similar with the typology of computer crimes set by the US Department of Justice.[56] Clearly, the proclamation has mentioned intention as the element required in the criminalization of computer crimes and left negligence as mental element. To the understanding of the researcher due to the substantial technology illiteracy manifested over electronic technology users in the country making activity which resulted from negligence/ignorance criminal offense would not serve criminal control purpose. Thus, presumably this is why the proclamation took intention as the only mental element required in the computer crime cases.

The computer crime proclamation states criminal offenses respectively with the appropriate punishments. The proclamation mentioned illegal access, illegal interception, illegal interference with computer systems, DoS attack, and creating and disseminating computer virus or malicious programs as criminal activities targeting computers.[57] Illegal access that has been committed against computer integrity is punishable based on the gravity of the offense from the range of 3 years of simple imprisonment to 5 years and fine ranging from 30,000 – 100,000 ETB or both. Committing interception to computer data or critical infrastructure is a crime and punishable upon conviction from rigorous imprisonment from 5 - 15 years and fine from 10,000 – 200,000 ETB based on the gravity of the case. Interference with a computer system to cause damage to the system or disrupt operation is punishable, depending on the nature and seriousness of the case, from rigorous imprisonment of 5 – 20 years and fine 50,000 – 500,000 ETB. Article 6 seems the replica of article 5 of the proclamation except the variation in punishment, as they both prohibit DoS attack among the crimes' elements listed therein. The punishment for causing damage to computer data by alteration, deletion, suppression to render it meaningless, useless or inaccessible under article 6 has been ranging from 3 – 10 years of imprisonment and fine from 30,000 – 100,000 ETB on the basis of seriousness of the case. With regard to the fact that criminals create and distribute malicious or infectious computer programs that are capable of causing damage to a

[56] Molalign Asmara, 'Computer Crimes in Ethiopia: An Appraisal of the Legal Framework' (n 31) 95

[57] See article 3 - 8 of the computer crime proclamation, it has listed them under the caption of crimes against computer system and computer data.

computer system, computer network or data, the proclamation is more elaborate to address such issues. These criminal activities have been punishable upon conviction by imprisonment from 1–5 years and fine from 5,000 – 30,000 ETB or fine only based on the circumstance of the crime.

Regarding the second category of computer crimes among the three mentioned, the proclamation identified three sets of crimes; computer related forgery, fraud and identity theft.[58] Under this category, computers have been seen as a means used to commit conventional crimes in new and innovative ways that complicate crime investigation and prosecution undertaken by LEAs. Counterfeiting electronic documents or any electronic data to procure undue advantage for oneself or others or injure the interest or rights of others made punishable under the proclamation with simple imprisonment not more than 3 years and fine not more than 30,000 or in a serious case with rigorous imprisonment not more than ten years and fine from Birr 10,000 to 100,000. Fraudulent activity to mislead the other party to accrue undue advantage using different methods including email scam and compromising business emails or to cause economic loss to others is prohibited. And punishable with rigorous imprisonment not more than 5 years and fine not more than 50,000 ETB or in serious cases with rigorous imprisonment not exceeding ten years and fine from Birr 10,000 to 100,000. Identity theft and impersonation has also been criminalized and made punishable upon conviction with simple imprisonment not exceeding five years or fine not exceeding 50,000 ETB.

The last category of computer crime under the proclamation, that is, illegal content data which constitute produce, transmit, dissemination or possess obscene material through computer systems against minor, cyber stalking, cyber defamation, cyber terrorism and unsolicited electronic advertisement.[59] Abundance of the internet and easy access of websites from mobile phones enable minors to browse various web pages without making a judgment no matter whether malicious or legitimate. Even more, they are more curious to know things, using this fact, criminals exploit to online technologies to inject minors with morally unacceptable characters – this could be done to recruit them to engage on sexual activities, redirect them to pornographic sites or sending erotic materials to expose minors to early sexuality. To mitigate these and other activities that will be committed against children in Ethiopia, the law prohibits the act of produce, transmits, sales,

[58] Ibid art. 9-12
[59] Ibid art. 13-15

distributes, makes available or possesses without authorization any picture, poster, video or image through a computer system. It has been punishable with rigorous imprisonment of 3–10 years as the seriousness of the case may be. The act of intimidation, threatening, causing fear and psychological strain against a victim or his/her family or relatives through computer systems is considered a crime under the proclamation with the punishment of simple imprisonment of 3-5 years or in serious case rigorous imprisonment from 5-10 years. Defamatory activities that are committed through the computer system upon dissemination of any writing, video, audio or any other image prohibited and made punishable, upon complaint, with simple imprisonment not exceeding three years or fine not exceeding 30,000 ETB or both. To mention computer crimes listed on the basis of the three classifications identified, the aforementioned activities are prohibited and punishable under the proclamation.

To sum it up, either of the definitions, which is broader or narrower, has its own consequences. Defining things means by itself is to delimit the scope. While defining cybercrime, if it goes broader by including any online activity as cybercrimes, it may cause the danger of lacking specificity against the criminal law principle (*nullum crimen sine lege or nullu poena sine lege*). In addition, the narrow definition may also cause the prohibition to fewer activities thus enabling offenders to be let free to go using a legal loophole. Thus, legislative definition needs to accommodate to the best extent the aforementioned concerns in order to facilitate endeavors in taking down the ever-growing cybercrime threats.

2.2 Classification and Types of Cybercrime

Certainly, to understand and define the concept, classifying cybercrime into different categories has become essential and this has been done considering the means used, nature and target of the criminal activity. And it is important to take note that overlapping occurs in many cases and it is impossible to have a perfect classification system.[60] Beside this general fact, there is a categorization as '*active*' and '*passive'* computer crimes.[61] An active crime is when someone uses a computer environment or telecommunications device without authorization (hacking).[62] A

[60] Longe O.B, 'Internet Service Providers and Cybercrime in Nigeria –Balancing Services and ICT Development', 3
[61] Hamid Jahankhani et al, 'Cybercrime classification and characteristics', (n 43) 154
[62] Ibid

passive computer crime occurs when someone uses a computer to both support and advance an illegal activity, an example is when a narcotics suspect uses a computer to track drug shipments and profits.[63] Pati, on the other hand, classified cybercrimes based upon types of entities targeted for cybercriminal activity. Accordingly, he classified cybercrime into three groups; 'cybercrime against individuals', 'against individuals' property', 'against organization and society'. There, also the categorization of computer crime into computers 'as a target', 'as a tool to cause damage', 'as online or offline cybercrime' and 'incidental cybercrime'.[64] This has been based on the involvement of computers in the commission of computer crimes or other crimes.

To come to discuss the types of cybercrimes, it is difficult to exhaustively list out cybercrime as technology advances progressively and hence adds opportunity for criminals to find new ways to commit crimes. Although some of the prominent cybercrimes will be discussed hereunder to understand its nature and complexity associated with. Accordingly, for the purpose of this study, the discussion mainly focuses on those cybercrimes prevalent in Ethiopian cyberspace.

2.2.1 Hacking

Hacking is an act of breaking into computer systems or information technologies without authorization but the act of hacking isn't usually illegal as there are ethical professionals involved in hacking called 'white hat hackers' who use their ability to defend the digital environment from hackers with a wicked motive named 'black hat hackers'.[65] Literally, hacking has been committed using different techniques among other installing computer viruses, phishing and network scanning.[66] Such offenses have been committed against confidentiality, availability and integrity of computer systems or networks.[67] Moreover, offenders use illegal accessing of commercial computers and personal computers to gain secret information such as industrial design, intellectual property and sensitive financial data or to commit data mining by taking advantage of technology illiteracy of users or upon deploying technical capability to circumvent digital technologies. To deter its negative consequence, it has been labeled a crime and punishable upon conviction as it

[63] Ibid
[64] Arun B. Prasad, 'Cyber Crime in India: Time Series Study of State Level data' (Manakin Press, 2017) 4
[65] Jagnarine, Amit Anand, "The Role of White Hat Hackers in Information Security" (2005), Honors College Theses, Paper 14 < http://digitalcommons.pace.edu/honorscollege_theses/14 >
[66] Ibid
[67] Ibid, 1

committed against computers to access sensitive information stored therein without permit or in excess of authorization.[68] According to Clough, the need for unauthorized access to computers has steamed depending on the type of data found in the computer; it may be to access information, modification or deletion of data and use of computers to commit other crimes by its support.[69] The main motive in commission of unauthorized access is to gain income in exchange of information obtained from the legitimate owner. After accessing, the offender encrypts the computer system to deny the owner accessing its own computer or threatens to modify, alter or delete the data unless the ransom has been paid. Again, such information that has been obtained illegally may be used to facilitate commission of other crimes such as identity theft, cyber stalking, electronic fraud and denial of service attack (DoS). In general, for the increase of hacking offenses, three main factors have been counted: inadequate and incomplete protection of computer systems, development of software tools that automate the attacks, and the growing role of private computers as a target of hacking attacks.[70]

In Ethiopia too, the report has indicated that the act of hacking has become rampant from time to time. For example, in 2019, a hacking attempt targeting financial institutions by a group of more than 200 hackers has been committed even if it can be foiled by INSA. [71] Surprisingly, one report shows that 142 INSA agents' email accounts were hacked because of the lenient password they have used, this has even led the hacker to break into the agency's email server.[72] Even though the other time, groups based in Egypt manage to hack government web pages to misrepresent the information about GERD.[73]

2.2.2 Denial of Service Attack (DoS)

DoS attack is another form of cybercrime that has been committed against computer systems. It has been attempted or committed against computer systems and information infrastructure by

[68] See Computer Crime Proclamation, Art. 3, Nigerian Cybercrime Act, s 6 (1&2), India ITAA, s 66 cum s 43 a
[69] Jonathan Clough, 'Principles of Cybercrime', (n 56) 28-32
[70] ITU, 'Understanding cybercrime: phenomena, challenges, legal response', (n 26) 17
[71] Xinhua News, Dec 7, 2020, 'Ethiopia foils mass cyber hacking attempt', Available at <http://www.xinhuanet.com/english/2019-12/07/c_138613947.htm > Accessed on Dec 16, 2021
[72] ECADF Ethiopian News, May 30, 2019, Available at <https://ecadforum.com/2019/05/30/ethiopian-insa-agents-hacked/> accessed on Nov 04, 2021
[73] Africa Center for Strategic Studies, by Nathaniel Allen, January 19, 2021, 'Africa's Evolving Cyber Threats', Available at <https://africacenter.org/spotlight/africa-evolving-cyber-threats/> Accessed on Nov 04, 2021

disseminating infectious programs that are deliberately to interfere with computer systems and disrupt its properly functioning to cause the service unavailable. A similar effect may be observed when a website is unable to cope with the number of requests it is receiving, for example when tickets go on sale for a popular concert and the system is overwhelmed by the number of simultaneous requests.[74] It may also be caused by sending bulk of traffic data or large number of email or self-replicating computer program[75] to interrupt the network and hence shutdown availability of certain services. With this regard, Ethiopia has experienced cyber incidents that hit computer operations, one of INSA's reports revealed that in 2019, the hacker attempted DoS attack against financial institutions to immobilize the financial infrastructure in Ethiopia.[76] Furthermore, the Agency in its report of 2020 that revealed 787 cyber incidents has mentioned cybercrime that causes infrastructure disruption has been among attacks carried out in Ethiopia.[77] Most recently, in 2021 also the same cyber-attack that hit various institutions including Development Bank of Ethiopia, Minister of Defense, and Minister of Education that disrupted operation and made the service inaccessible for clients was committed.[78]

2.2.3 Ransomware Attack

Ransomware, it is a form of malicious programs, which has been committed through various techniques such as social engineering and email scam in order to deceive users to download malicious websites/links deliberately created to infect computers. Criminals use these techniques in an attempt to install the ransomware on the victim's computer to successfully manipulate information contained therein and encrypt files. Once the data has been encrypted, the cybercriminals may ask the data owner to pay ransom to recover the data and threaten to delete, alter or modify if the payment isn't made right away. Even after the ransom is paid, the victim does not have a guarantee whether he will get the file decrypted or no being asked for the second payment.

---

[74] Ibid 37
[75] Ibid 20
[76] Xinhua News, 'Ethiopia foils mass cyber hacking attempt' (n 69)
[77] Ethiopia Monitor News, Available at <https://ethiopianmonitor.com/2020/08/24/insa-thwarts-787-cyber-attacks-on-ethiopia-in-2019-20-fy/> accessed Dec 3, 2021
[78] Addis fortune, 'Red Alert Over Cyber Attacks', available at <https://addisfortune.net/columns/red-alert-over-cyber-attacks > accessed on Dec, 16 2021

In 2020, the Federal Bureau of Investigation (hereinafter FBI) report indicates that among the complaints received through Internet Crime Complaint Center (hereinafter IC3) 2,474 were identified as ransomware causing loss over $29.1 million.[79] Ethiopia was also hit by WannaCry Ransomware (the other species of ransomware) which first occurred in 2016 and attacked over 300,000 computers, as the attack targets various state-owned and private institutions, but the level of its damage in Ethiopia remains unrevealed by INSA.[80]

2.2.4 Malicious software

In the commission of crime against integrity of computer systems, data or network offenders use malicious computer programs. Hence, they installed malicious programs through the use of techniques, like deceiving the user to download contaminated files to easily get control of the victim computer. In this way, computer viruses and worms are used to cause unauthorized access into information stored in computer systems either to modify, delete data or facilitate the commission of conventional crime such as fraud, counterfeit documents etc. For example, the customer's computer may be infected with malware in the form of computer viruses or implanted malicious programs that run in the backdoor of the system in order to allow perpetrators to covertly obtain financial data of remote (online /distantly) users without authorization.

Generally, malicious software or malwares are utilized to commit criminal activity targeting computer systems or information technologies. Basically, this is used to infect computer systems and monitor the computer remotely to facilitate the commission of other crimes including collecting sensitive and financial data, DoS attack, identity theft and impersonation or content related crimes. In Ethiopia, INSA's report of 2020 reveals among 787 cyber-attacks the large portion of malware attacks during this period was committed through malicious software named Ransomware and Crypto-currency miner.[81]

2.2.5 Phishing

[79] Federal Bureau of Investigation, Internet Crime Report, 2021, 14

[80] Ezega News, Dec 6, 2019, Available at <https://www.ezega.com/News/NewsDetails/7518/INSA-Aborts-Cyber-attacks-on-Finanacial-Institutions > Accessed Dec 16, 2020; Addis fortune 'Red Alert Over Cyber Attacks' (n 76)

[81] Ethiopia Monitor News (n 75)

Phishing has been described as a form of social engineering in which an attacker, also known as a phisher, attempts to fraudulently retrieve legitimate users' confidential or sensitive credentials by mimicking electronic communications from a trustworthy or public organization in an automated fashion.[82]A typical phishing email will appear to come from a legitimate organization, such as a bank, and will state that the organization requires the recipient to verify their account information.[83] Phishers designed a fake website or email to defraud unsuspected victims to disclose her/his secret personal and financial information believing that the request has actually come from the legitimate service provider. Once the target clicks to the mimic website or opens an email sent out to its address, secret password and detained financial information might enter the hand of the offender. Fraudsters may use it to commit crimes of identity theft, data mining for sale or prevent victims from accessing the computer or encrypting files until the requested ransom has been paid.

2.2.6 Spamming

Spam, like phishing, used to trick the victim to make him/her believe the dealing that is offered by the offender is genuine. The spammer may communicate the victim through email, phone message or any other electronic communication method to illegally obtain personal information. Perpetrators may send e-mail messages to credit institutions' customers inviting them, under various pretexts (like technical upgrading, database reconciliation or updating), to enter the provided code manually via a computer keyboard into the screen forms in course of online sessions initiated by perpetrators (using, for example, a fake website).[84] Thus, based on such faith earned because of hitherto activity, the targeted victim asked to transfer money to take the relationship into another level. Once the victim transfers the requested money or secret information, the scammer does not reappear or say a word to the victim; rather he/she blocks the communication. On the other hand, scammers create malicious websites and send it through email to a company or an individual to have them click a link in order to infect the computer with malware and to have

[82] Shi J., Saleem S., 'Phishing' Computer Security Research Reports, University of Arizona, Available at <http://www.cs.arizona.edu/~collberg/Teaching/466-566/2014/Resources/presentations/2012/topic5final/report.pdf> Accessed on October 1, 2021

[83] Jonathan Clough, 'Principles Of Cybercrime', (n 67) 192

[84] Eurasian Group on Combating Money Laundering and Financing of Terrorism 'Cybercrime and Money Laundering' (2014) 16

access to the computer system. Hence, this malicious website may support the spammer to have access to sensitive and personal information contained within the victim's computer.[85]

Obviously, the emergency of coronavirus has forced the world to rely on electronic communication and technology more than before because of the lockdown order.[86] This fact has provided an opportunity for cyber criminals to exploit it and the most prevalent fraudulent scheme seen during this time is government impersonation.[87] Through the process of impersonation, the fraudster may compromise business email and utilize the information obtained in an attempt to pretend to be a company or government officer to spoof the victims. Considering the international reach of email and other electronic communication through the internet, spam attacks are not an unusual incident in Ethiopia. Against the consent of the recipient bulk of unsolicited or unauthorized emails have been sent and that is abusing the available electronic communication means. Though, beside such a fact, the Ethiopian computer crime proclamation merely prohibits making email or any electronic communication that contain advertisements for products and services without prior consent of the recipient. Amid the existence of the problem the law left out to deal expressly with spamming by defining the word in advance and regulating to curtail its effect.

2.2.7 Online Financial Crimes

Alongside the expansion of electronic and computer technology, banks and financial institutions are attracted to online banking and electronic money transfer systems. This has brought for cybercriminals an opportunity to exploit online banking and financial services to commit cybercrimes such as credit card fraud, internet auction fraud, and money laundering. The report from McAfee indicates that financial crime through Internet Protocol (hereinafter IP) accounted for 75% of losses in 2021 and pose the greatest threat to companies.[88] Internet auction fraud is when items offered for sale are fake or stolen goods, or when a seller advertises nonexistent items for sale which means goods are paid for but never arrive.[89] In an online auction fraud, in their own respect both seller and buyer might be deceived, for instance, the seller who expects payment upon

[85] See Hamid Jahankhani, *et al*, 'Cybercrime classification and characteristics' (2014), 158
[86] Internet Crime Report (n 77)
[87] Ibid, 9
[88] McAfee Report, Available at <https://www.businesswire.com/news/home/20201206005011/en/New-McAfee-Report-Estimates-Global-Cybercrime-Losses-to-Exceed-1-Trillion> Accessed on October 10, 2021
[89] Hamid Jahankhani et al, 'Cybercrime classification and characteristics' (n 62) 160

full delivery of the product to the auction winner though he may lose the payment.[90] On the other hand, the winner of the auction will deny delivery of the product after the whole payment is made or the buyer might deceive to submit a bid for a non-existing product.

Certainly, the proliferation of online banking and digital currency provide a wide opportunity for criminals to launder illegally obtained money through electronic money transfer. Furthermore, electronic money transfer schemes that are accompanied with high speed and available at low expenses may decrease the cost required for money laundering and in turn encourage criminals to seek new sources of illegal proceeds.[91] Moreover, the development of technology such as crypto-currency, digital currency and electronic money transfer technology provide new opportunities for cybercriminals to commit financial crimes, for example, they can transfer ill-gotten money through online money transferring without leaving any tracks. One of the reports from National Intelligence and Security Service (NISS) of Ethiopia reveals that six criminals and one of them are Nigerian caught while trying to steal 110M USD using electronic transfer, though they only manage to withdraw 1.8M USD.[92]

2.2.8 Computer Fraud and Forgery

With the rapid expansion of computer technology and the internet, online business interaction increases exponentially. At the same time, such development creates opportunities to misuse computer technology for fraudulent activity. Impersonation is one of the most popular computer related crimes. The offender who can compromise the business email account of one of the company's employees may use it to send out misleading information to the customer as though it is from the company and request the customer to respond by sending secret code and other relevant personal information under the threat of losing the service. Again, offenders of fraudulent activity create infected web, email or malicious code into the recipient email address which appears to be the normal one. But, as soon as the victim unsuspiciously opens or downloads it, like in the case of phishing or scam, he/she may lose control of its own computer system or data unless he/she does what has been requested to do. In the same manner, parallel to forgery committed in document

[90] Ibid
[91] Eurasian Group, 'Cybercrime and Money Laundering', (n 82) 14
[92] Further Africa, May 12, 2020, Available at <https://furtherafrica.com/2020/05/12/ethiopia-intelligence-intercepts-us110m-cyber-fraud/> Accessed on Nov 16, 2021

format, falsifying electronic documents or data contained in electronic form has become possible with the help of computers. Thus, it has also become another form of cybercrime committed through the help of computers.

2.2.9 Cyber Pornography

This rapid expansion of the internet has facilitated electronic communication such as e-mail, websites, SMS text, webcams, chat rooms and social media platforms. In turn, such electronic communication provides a chance to make online solicit and recruitment for sexual activity so easier and with less risk of being caught. Availability and affordability of the internet has led to the growing number of websites created to offer production, possession and distribution of pornographic and related materials online. At the same time, criminals have exploited this online communication technology to harass, recruit and invite children to trend online sexual activity or accept the bid to take part as porn actor.

Recently, the global online porn industry's worth is estimated to be $97 billion.[93] Popularity of the internet makes uploading and downloading any videos, nude pictures, articles and obscene material very easier which enables the porn industry to grow successfully. Conversely, such development attributes cyber porn a borderless crime thus it being a challenge to effect investigation to curtail its consequence and punishing perpetrators. Since its transnational nature involves different LEAs in different jurisdictions, detecting and punishing suspects working under secure networks which guarantee benefit of anonymity cause difficulty to tackle the problem unless international cooperation has been made among nations to such specific cases.

2.2.10 Cyber Stalking or Harassment

Cyber stalking is a technological-based "attack" against a person who has been targeted specifically for reasons of anger, revenge or control.[94] In the commission of cyber stalking, the offender uses the Internet, e-mail or other electronic communication device as a means to intimidate, threaten or harass the victim or his/her relatives. Unlike real world stalking, cyber

[93] Fight The New Drug, Nov 24, 2020, Available at <https://fightthenewdrug.org/how-does-the-porn-industry-actually-make-money-today/> Accessed on October 12, 2021

[94] V. Karamchand Gandhi, 'An Overview Study on Cybercrimes in Internet', (2012), Vol 2, No.1, Journal of Information Engineering and Applications, 1

stalking doesn't require the physical presence of a stalker to threaten or harass the victim; rather, the stalker uses electronic communication and benefits from anonymity of this technology to keep itself unidentified. Like other cybercrimes, the offender of cyber stalking commits it with the aim to control the victim and to do whatever he asks. If not, the stalker threatens to disseminate or publish personal information he had against the interest or reputation of the victim/ his family/relative.

2.2.11 Hate Speech and Xenophobia

Without a doubt, global communication of interconnected network systems has provided easy access and affordability of communication from anywhere and at any time. But this has not been without shortcomings as some malevolent users utilize such electronic communication platforms to disseminate fake news considering its global reach. Stat obtained from Datareportal has shown that internet users in Ethiopia have shown an increase by 2.8 million as it reached 23.96 million in January 2021.[95] The same report has also revealed that in the same year social media users have reached 6.7 million with an increasing rate of 8.1% between 2020 and 2021.[96] As of April 2021 the report reveals that 7.2 million are Facebook users in Ethiopia, among which users with the age of 25-34 counted as large portions with 4 million.[97] Most users considering the level of age and maturity they aren't much concerned for what they have written on social media rather they disseminate sensitive and fake information to instigate violence.

Various reports show how violently electronic communication was used in Ethiopia to result in social unrest.[98] Hate speech and disinformation through the use of world wide web (WWW) browsers and social media platforms have been surging in Ethiopia over a period.[99] Quite clearly

[95] Datareportal, 2021, Available at <https://datareportal.com/reports/digital-2021-ethiopia> Accessed Nov 7, 2021
[96] Ibid
[97] NapoleonCat Stat, Available at <https://napoleoncat.com/stats/facebook-users-in-ethiopia/2021/04/> Accessed on Nov 7, 2021
[98] See European Institute of Peace, 'Fake news misinformation and hate speech in Ethiopia: A vulnerability assessment', Apr 21, 2021, available online at <https://www.eip.org/wp-content/uploads/2021/04/Fake-News-Misinformation-and-Hate-Speech-in-Ethiopia.pdf>; Martin Plaut, Dec 18, 2021, Available at <https://martinplaut.com/2021/12/18/the-use-of-social-media-to-promote-hate-speech-in-ethiopias-tigray-war/; Addiszeybe, Aug 1, 2021, Available at <https://addiszeybe.com/featured/politics/currentaffairs/analysis/does-social-media-intensify-the-conflict-in-northern-ethiopia> Accessed on Nov 10, 2021
[99] Rest of world, Available at <https://restofworld.org/2021/why-facebook-keeps-failing-in-ethiopia/> Accessed on Nov 12, 2021

the problem of epidemic fake news, hate speech and disinformation observed circulating and videos viral over social media in Ethiopia have been the result of electronic communication mediums operated without a proper controlling mechanism. The proclamation provides to suppress and control hate speech and disinformation of Ethiopia is not in equal pace with the problem posed using these electronic mediums to tackle it and even institutional capability is at its embryo.

2.3 Impact of Cybercrime: Economic, Social and Technological Scenarios

In order to understand why cybercrime has been prevalent especially since recent years, one must consider its causes with its rigorous consequences from the outset. High rate of unemployment, poverty, lack of information security awareness, negligence, cybercriminals far reaching technological skill and knowledge are among factors that causes the commission of computer crimes at its apex. Moreover, study shows that cybercrime has steadily increasing, *inter alia,* due to users' lack of information security awareness to enable oneself protected from crimes committed through information technologies and due to LEAs outpaced by cybercriminals in terms of technical tools and technologies. And such factors further exacerbate the increase of cybercrime with huge economic and sociocultural impact across the countries. One survey report in 2021 projected that global economic losses from cybercrime were over $1 trillion, which accounted for a more than 50% increase from 2018.[100]

Besides, an argument stated that cybercriminals require access to the internet, level of skill and be technology savvy more than what an average person could possess to commit cybercrimes.[101] However, the proliferation of mobile phones at the least cost to do what could be done only using desktop or personal computers some years back and simplistic presence of online technologies with tips enable anyone to commit technology-enabling crimes irrespective of technology experts. Internet's easy accessibility in affordable cost and having little technological knowledge, through use of mobile devices which could be possessed by least cost can pose psychosocial adversity by distributing content related crimes over internet or WWWs. For example, children those could access internet likely exposed to websites created with the aim to produce and distribute pornographic and obscene material, thus it will lead them to early sexuality.

[100] McAfee Report (n 85)
[101] Hamid Jahankhani et al, 'Cybercrime classification and characteristics', (n 86) 153

At present, considering worldwide growing dependence on digital technology in effect of modernizing and keeping pace with globalization, as ITU report suggested, this reliance makes systems and services prone to attack against critical infrastructure.[102] Similarly, criminals manipulate and interfere with the systems to commit DoS attacks, hack into bank systems to transfer money, illegally access financial institution's client information or disrupt companies' operation/production that could cost financial losses. Moreover, cybercrime has adverse consequences on technological growth, innovation and transformation aimed to support productivity and socio-economic development. Altogether, considering all these consequences against individuals, companies and government the impact of cybercrime doesn't be overstated.

2.4 The Need for Understand Cybercrime

These days as discussed above, easy availability and affordability of the internet and presence of networked computers; digital technologies have integrated in almost every aspect of modern life. Advances in ICTs enable individuals and organizations to utilize computer technologies to store their valuable information. While overwhelmingly positive, there has also been a dark side to these developments.[103]It creates an easy way for cybercriminals to commit crime at low cost and little/no risk of being identified. Cybercriminals have taken advantage of techniques related to social engineering— such as phishing—that target employees having direct access to databases containing confidential business information, as well as pharming, credit card fraud, dedicated denial-of-service (DDOS) attacks, identity theft and data theft.[104]

Essential question at this juncture is, should the countries need rules or principles that regulate such online misconducts? For sound mind it is unquestionably, legal framework and strategic measures to reverse the effect it may have on nation, organization and individual is imperative. Notwithstanding this importance, understanding the concept of cybercrime has become the most important and prior thing to design appropriate and effective preventive and protective measures. Altogether, this has invaluable importance to enable laws and policy makers to draft suitable law

[102] ITU, 'Understanding cybercrime', (n 68) 75

[103] Mahboob Usman, 'Cyber Crimes: A Case Study of Legislation in Pakistan in The Light of Other Jurisdictions' (LL. M Thesis, International Islamic University Islamabad, 2015) 'Cyber Crime', 3

[104] World Bank and United Nations, 'Combating Cybercrime: Tools and Capacity Building for Emerging Economies' (2017) 11

and policy, organize effective LEAs, intelligence and security apparatus to enforce and oversee laws and information security measures. Again, it has been crucial to initiate education and awareness creation programs to educate users about information security threats thus making them take protective measures. Grappling with causes and consequences of cybercrime is an insight to the nature and prevalence of cybercrime. This is a way to come through effective and efficient legal and technical strategies to fight cybercrime. Just as it is important to understand the characteristics of the criminals in order to understand the motives behind crime and subsequently develop and deploy crime prevention strategies, it is also important to understand victims, i.e., the characteristics of the users of computer systems in order to understand the way these users fall victim to cybercrime.[105] It is also needed to understand cybercrime from this perspective.

To know its prevalence, the actual rate of cybercrime incidents remains unreported because of the absence of awareness on the part of the public at large and the fear of organizations for the negative effect of publicity of cyber incidents they are faced with. In turn, this has the negative implication to take adequate legal and regulatory response which the situation requires to respond. Perhaps, understanding the nature of cybercrime and the degree of its occurrence helps lawmakers, judiciary and law enforcement authorities to understand the complexity of cybercrime and hence to equivalent legal measures and efficiently enforce and monitoring measures put in place.

In summary, it is essential to first understand the concept, nature and complexity of cybercrime to develop a robust legislative and institutional framework to combat cybercrime consequences on e-commerce, electronic privacy and national interest. In addition, in the view of the researcher, understanding cybercrime and its repercussions is a fundamental and initial step that helps the process undertaken to bring capacity building and awareness creation initiatives.

2.5 Cybercrimes and Techniques of Cyber Criminals

If not properly handled, the development of ICTs that might reinforce new methods/technologies to advance opens the opportunity for cybercriminals to exploit cyberspace. Thus, concrete measures should be taken to ensure that technology wouldn't outpace legislative effort and ability of LEAs to tackle cybercrime. In use of digital technologies for undesired purposes, various

[105] Hamid Jahankhani et al, 'Cybercrime classification and characteristics', (n 97) 149

methods have been developed over time. Advancement in computer and internet technologies, provide an opportunity for criminals to remain anonymous and offenders may conceal their identity using proxy servers, spoofed email or IP addresses or anonymous emailers.[106] Accordingly, anonymity and global reach of the internet, fraction of second as sufficient to commit cybercrime, volatility of evidence and high cost of investigation have amplified the chance of its commission in turn criminals might get away with its deeds unfounded. Meantime, this has increased the challenge of law enforcement institutions while detecting and investigating the crime. The report by ITU states that as criminals control more powerful computer systems and networks, the gap between the capacities of investigating authorities and those under control of criminals is getting wider.[107]

In conclusion, in this era when networked computers are increasingly available, criminals attempting to access computers that contain information has been presented as a mile easier than committing traditional crimes. It could be committed through dissemination of malware and other techniques such as spam to manipulate the systems. Thus, criminals no longer need to brainwash their "targets" and have personal contact with their potential victims.[108] Instead, the criminal uses the techniques, *inter alia*, botnet, encryption, anonymous communication and automation which brought a lot of opportunities for cybercriminals so does it being a challenge to law enforcers.[109]

[106] Jonathan Clough, 'Principles of Cybercrime', (n 81) 6
[107] Ibid
[108] Eurasian Group, 'Cybercrime and Money Laundering', (n 87) 3
[109] ITU, 'Understanding cybercrime', (n 98) 78-81

Chapter Three

Legislative and Regulatory Framework of Cybercrime: Comparative Analysis among Ethiopia, India and Nigeria

Introduction

It is quite understandable how cybercrime and its repercussions cost the world economically and technologically, therefore, knowing this fact is an initial driving force in the fight against cybercrime. Beyond this, it is imperative to examine legislative and institutional responses available in each of the selected jurisdictions in halting the effect of cybercrime in their respective context.

Therefore, in this chapter the discussions are made in three different parts. The first part is devoted to discussing and analyzing the international legal framework on cybercrime. The second part is a comparative part that would examine conception and context of cybercrime in each jurisdiction. The discussion in this part also devotes more attention in examining legal and regulatory frameworks used to prevent cybercrime, in a comparative perspective. Finally, the third part by focusing on Ethiopia, probe the issue and draw the best lessons Ethiopia could get from the comparators.

Part I. International Legal Framework in Combating Cybercrime and Cyber-criminality

At present, the rapid expansion and prevalently dependency on ICTs along with advantage of anonymity and global reach of the internet led cybercrime to be the most complicated global concern that required international cooperation to overcome its effect. Specifically, considering the fact that activity which has been criminalized in one country might be regarded as lawful in the other country from where the cyber-attack emanated, evidence or victim has been found. In the field of cybercrime, as it is for all cross-border crimes, the main advantage of harmonizing the law perhaps enables the prevention of cyberspace safe havens for perpetrators.[110] Noteworthy, to

[110] UNODC, 'Comprehensive Study on Cybercrime' (n 28) 60

harmonize domestic cybercrime legislation, international legal framework plays a key role by underlying minimum standard in criminalization and influencing the country's national legislation. In a scenario where cooperation to enforce cybercrime laws, effect extradition or help the investigation process upon expedite preservation of electronic data is not properly handled, this may hurdle prevention and investigation of cybercrime.

As of yet, there is no comprehensive and binding international mechanism or instrument developed to deals with cybercrime,[111] save for the proposal recently submitted by Russia for adoption of a comprehensive international cybercrime treaty which has been in the process of drafting after resolution made by UNGA in Dec 2019.[112] But, there are international organizations working on cybercrime by taking it as part of their transnational crime control and prevention agenda. INTERPOL for its member of 194 countries provide support to the effort of combating one of the transnational criminal activities, cybercrime, upon facilitating LEAs to get capacity building and cooperation in electronic data collection and access institution's databases.[113] UNODC is also another organization that promotes international effort in combating cybercrime by providing technical assistance for capacity building, awareness, works on awareness rising, international cooperation, data collection, research and analysis on cybercrime.[114] In addition, the office assigned by General Assembly resolution 65/230 to organize open-ended intergovernmental expert group to conduct comprehensive study on cybercrime.[115]

Parallel, there are regional efforts to regulate use of ICTs and confront the effects of cybercrime in respective regions. In Europe, to assist the effort to tackle cybercrime by the member states, the Council of Europe adopted the Convention on Cybercrime in 2001. The other is the Commonwealth of Independent States' Organization, which adopts the Agreement on Cooperation in Combating offenses related to Computer Information of 2001, which calls for harmonized

[111] S. Daultrey, Cybercrime: 'Invisible problems, imperfect solutions' (2017) 7

[112] By Deborah Brown, Available at <https://www.hrw.org/news/2021/08/13/cybercrime-dangerous-new-un-treaty-could-be-worse-rights> Accessed on Dec 5, 2021

[113] See INTERPOL,<https://www.interpol.int/>; <https://law.stanford.edu/education/only-at-sls/law-policy lab/practicums-2019-2020/supporting-interpols-efforts-to-combat-transnational-crime-805z/> Accessed Dec 10, 2021

[114] UNODC, Available at <https://www.unodc.org/unodc/en/cybercrime/index.html> Accessed on Dec 10, 2021

[115] Available at: <https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html> Accessed on Dec 10, 2021

cybercrime laws. The Arab League adopted the Arab Convention on Combating Information Technology Offenses in 2010 under the auspices of creating strong cooperation among member states. Shanghai Cooperation Organization's Agreement on Cooperation in the Field of International Information Security, adopted in 2010. The African Union also adopted the Convention on Cyber Security and Personal Data Protection in 2014.

Council of Europe Convention on Cybercrime (hereinafter Budapest Convention) has been taken as a robust and model instrument. It is the only most effective convention to help the effort by presenting robust legislative and regulatory means. The Budapest Convention combines a comprehensive set of rules on different aspects of cybercrime including substantive, procedural, jurisdictional and international cooperation issues.[116] Above all, it has been opened even for non-European states to join membership with the aim to reinforce the cooperation to speed up the fight underneath the problem of cybercrime. It has been quite clear that the process of domestication is encouraged to enable states to join hands in the fight and secure dual criminality which becomes a precondition to undertake both MLAT and extradition. Particularly, to meet this requirement 'the convention comprehensively covers those actions that parties are to criminalize in their domestic law as cybercrimes'.[117] Also, considering fluidity of electronic evidence, the convention requires the 24/7 contact network for effective cooperation in preserving evidence and effective investigation of computer crimes. By doing so, the convention provides cooperation frameworks for effective fight against cybercrime upon creating threads of national efforts together. Generally, its binding nature on state parties has increased its efficacy and suits its aspirational goal of harmonization.[118] In addition, EU Council has adopted other instruments such as directive to combat sexual abuse and sexual exploitation of children and child pornography (2011/92/EU), directive against information systems (2013/40/EU), directive combating fraud and counterfeiting of non-cash means of payment of 2001, e-commerce directive (Directive 2000/31/EU), e-privacy directive of 2002. The treaty on child sexual exploitation and pornography to protect the safety of children from online malpractice, it urges member states to take measures to ensure immediate removal of such contents related to pornography in their jurisdiction. The Union of Europe Council

[116] UNODC, 'Comprehensive Study on Cybercrime' (n 174) 197
[117] Ibid 202
[118] Ibid 204

has also pursued it effort and adopted Additional Protocol[119] to the Budapest Convention to regulate hate speech and xenophobia carried out through electronic communication medium. This instrument requires state parties to legislate law that criminalize hate speech and xenophobia through computer system to bring uniformity of application that has the implication to restrain the occurrence of such activities through electronic technology.

Given the fact that continent Africa's higher dependency on ICTs and increased Internet penetration rate (accounting 28%) to integrate economic, political and social development along fast-tracking technologies and globalization, it faces challenges of cyber-security and cyber-attacks. To cope with, disintegrated domestic effort wouldn't be as helpful to tackle cyber-security threats at national or regional level. Considering this reality, in 2014, under the auspices of AU the Convention on Cybersecurity and Personal Data Protection was adopted at Malabo. It set forth rules to secure the information environment and to strengthen legislative effort by member states and regional economic communities. Like the Budapest Convention, the Malabo Convention has provided a cooperation platform among member states to support regional and international efforts to combat cybercrime and cyber-security threats. Even prior to the Malabo Convention there are sub-regional treaties with the effect of bringing inter-regional harmonization in the fight against cybercrime. Southern Africa Development Community (SADC) Model Law on Computer Crime and Cybercrime adopted in 2012, the Economic Community of West African States (ECOWAS) Directive on Fighting Cybercrime of 2011, IGAD also sponsored an effort in East Africa to tackle cybercrime as a part of its Security Sector Program. Looking at the cooperation platforms, even though there are such international initiatives to create and promote legal assistance to harmonize legislation and bring cooperation means in jointly fighting extraterritorial cybercrime cases, none of them are successfully enforceable to achieve their objective. However, there is no doubt on the search for such international instruments since cybercrime and its effect is not subject to geographical and territorial limits for certain countries to deal with it. Therefore, whether or not the countries are interested or not for the sake of their cyberspace security, they are forced to join and strengthen bilateral or multilateral cooperation mechanisms. This is what justifies that Ethiopia

[119] Council of Europe, Additional Protocol to the Convention on Cybercrime, Concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems, 28 January 2003<http://conventions.coe.int/Treaty/en/Treaties/Word/189.doc>

has to think over seriously if it needs to secure the safety of its information system and enforce cybercrime law against perpetrators.

Part II. Comparative Study on Legislative and Regulatory Framework of Cybercrime

Here, under this specific part of this chapter the objective is to find out best practice and experience from the selected jurisdictions. And the comparisons have been undertaken in respect of conception and context of cybercrime. Examining the legal and regulatory frameworks used to prevent cybercrime as devices by the respective jurisdictions have also been made in comparative perspective.

1. Conception and Context of Cybercrime in India, Nigeria and Ethiopia

As discussed under the previous chapter, cybercrime has caused worldwide socioeconomic, psycho-social and political problems. However, what is difficult is to know the actual rate and prevalence of cybercrime across the world because of lack of data available and the absence of measuring tools and control of cybercrime.[120] Amid several legislative and technical methods that have been introduced to control and prevent cybercrime, countries are still facing these problems. So, in this section, the context of cybercrime and legislative effort taken to suppress its effect by the India, Nigeria and Ethiopia government has been discussed respectively. Particularly, the discussion was made with a view to understand the context and prevalence of cybercrime in these jurisdictions in accordance.

To begin the case with India, like many other countries, the introduction and development of internet and digital technologies that inspired the digitization of the country has been responsible for the birth of cybercrime. It has grown at an alarming rate. Unsurprisingly, cybercrime incidents has shown rapid growth over the years, for example, in the year 2020, the cases of cybercrime rose to 50,035 from 44,735 of the previous year in an increasing rate of 11.8% based on the report

[120] SciDevNet, 07/07/16 'Cybercrime in Africa: Facts and Figures' Available at <https://www.scidev.net/sub-saharan-african/features/cybercrime-africa-facts-features/> Accessed on October 26, 2021

from National Crime Records Bureau (NCRB).[121] With this increasing rate, the leading motive behind cybercrimes was fraud which accounted for 30,142 or 60% of 50,035 cases, followed by sexual exploitation with 3,293 (7%), extortion 2,440 and causing disrepute 1,470 respectively.[122] Besides this increase in cybercrime cases, the government of India has taken outstanding measures that enable the country to stand 10th in 2020 from its previous position of 37th in 2018 at GCI.

The next comparator is Nigeria, which is one of the largest economies and most populated countries in Africa and has been featured by the expansion of ICTs and internet users bases. Regarding the level of Internet penetration, the report from Statista revealed that it has reached 51.44% with users of 108.75 million in 2021, and projected to reach 59.92% with 143.26 million users in 2026.[123] Besides such growth in the use of electronic technologies to drive the digital economy in Nigeria, the country has an international reputation for being one of the biggest cybercrime hotspots in the world.[124] Understandingly, the report from the FBI reveals in 2020 Nigeria ranked 16th among the countries most affected by internet crime in the world.[125] And fraudulent electronic mails, identity theft, hacking, cyber harassment, spamming and Automated Teller Machine spoofing are the most popular forms of cybercrime.[126] Among electronic fraud, advance fee fraud which is known as 419 or 'Yahoo Yahoo' is the most prevalent in Nigeria. According to the Nigerian Electronic Fraud Forum, in 2018, commercial banks in Nigeria lost a cumulative N15 billion (US$39 million) to electronic fraud and cybercrime, this was a 537% increase on the N2.37 billion loss recorded in 2017.[127] These are some illustrative shows how cybercrime is prevalent in Nigeria. However, to stand against this booming cost of cybercrime, particularly, Advance Fee Fraud (hereinafter AFF) scams, the Nigerian government enacted the AFF Act in 2006 and in strengthening the effort Cybercrime Act was also enacted in 2015. In

[121] Available at <https://www.hindustantimes.com/india-news/cyber-crimes-registred-11-8-increase-last-year-ncrb-101631731021285.html> Accessed on November 3, 2021

[122] Available at <https://www.moneycontrol.com/news/india/heres-the-reason-behind-60-of-the-cyber-crimes-committed-in-2020-7489071.html. > Accessed on November 3, 2021

[123] Statista Report, Sep 29, 2021, Available at <https://www.statsta.com/statistics/183849/internet-user-nigeria/> Accessed on Oct 29, 2021

[124] The Guardian, Aug 27, 2019, Available at <https://guardia.ng/news/is-nigeria-really-the-headquarters-of-cybercrime-in-the-world/> Accessed on Oct 26, 2021

[125] The Cable, March 18, 2021, 'Nigeria Ranked 16th in FBI global cybercrime victims report', Available at https://www.thecable.ng/nigeria-ranked-16th-in-fbi-global-cyberime-victims-report/amp> Accessed on Oct 26, 2021

[126] The Guardian's report (n 110)

[127] Enact Observer, Oct 07, 2020, Available at <https://enactafrica.org/enact-observer/nigerias-financial-institutions-vulnerability-to-cybercrime> Accessed on Oct 26, 2021

quelling cybercriminals who immigrated to Nigeria to use the weak point in cyber-café to raid cyber-attacks, Nigerian undertake strong measures through its regulatory bodies as reported by EFCC.[128]

In Ethiopia too the reality isn't different. About the context, Halefom H. argued that Ethiopia could be a safe harbor for cybercrime, considering the country's experiencing a massive increase in availability of internet which is accompanied by nascent cyber-security governance.[129] Thus far, this argument remains true as various reports suggest the same about Ethiopia's current cyber governance reality.[130] Even though the government of Ethiopia has strived to strengthen its legal and institutional measures to prevent cybercrime, it is mounting. The report proves that cyber-attack has alarmingly increasing from 479 and 576 to 791 in the successive three years from 2017, 2018 to 2019 respectively,[131] much worse, in 2021 it has reached 2,800 incidents.[132] In 2019, the then INSA's Deputy Director-General Engineer Worku Gachena stressed that as 'cybercrime is alarmingly increasing in Ethiopia the swift action needed to thwart the attack'.[133] Furthermore, the same message has been convey by the current INSA Deputy Director, Kefyalew Tefera, claiming that trends of cyber-attacks is increasing every years.[134] This has been beside the effort that the government of Ethiopia has taken to further legal and institutional measures to curb the problem of cybercrime from its very occurrence.

Yet, the country doesn't enact a law that criminalizes the act of produces, possesses and disseminates nude pictures, pornographic videos (include revenge pornography), and obscene material through the internet. Besides the absence of laws that prohibit such cybercrimes, studies

---

[128] Nir Kshetri, 'Cybercrime and Cybersecurity in Africa' (n 37)

[129] Halefom H. 'The State Of Cybercrime Governance In Ethiopia', (n 33) 6-7

[130] See Waltainfo, Available at <https://waltainfo.com/ethiopia-encounters-2,800-cyber-attack-attempts/>; Cyber Security Intelligence, Available on <https://www.cybersecurityintellegence.com/blog/cyber-attacks-on-africas-are-soaring-4709.html>; Commander Abebe Muluneh, Director of IGAD SSP, describe Ethiopia's cybersecurity governance as it is in its infant stage, in turn the could cause Ethiopia the safe harbor of cybercrime, Available on <https://igad.int/divisions/peace-and-security/2668-igad-ssp-conducted-ethiopia-national-traning-on-investigation-and-prosecuting-cybercrime>, Accessed on November 7, 2021

[131] Ezega News, Available at <https://www.ezega.com/News/NewsDetails/7518/INSA-Aborts-Cyber-Attacks-on-Financial-Institutions> Accessed on Nov 20, 2021

[132] Walta News, Oct 20, 2021, Available at <https://waltainfo.com/insa-urges-media-institutions-to-enhance-capacity-to-prevent-cyber-attacks/accessed> Accessed on Dec 17, 2021

[133] Ezega News (n 117)

[134] Available at <https://ethiopianmonitor.com/2020/08/24/insa-thwarts-787-cyber-attacks-on-ethiopia-in-2019-20-fy/> Accessed on Dec 17, 2021

show that most complaints that are brought to the FPC Cyber Unit are related to revenge porn, blackmail, threatening the victim for distribution or publishing video or nicked pictures online when the love relation has broken.[135] The same study underlines that the Unit is not successful in investigating the complaints due to limited expertise and technical capacity.[136] Overall, this is a cybercrime trend in Ethiopia as can be understood from the past reports and researches undertaken on the field as have illustrated.

2. Legal and Regulatory Frameworks to Prevent Cybercrime in India, Nigeria and Ethiopia

Altogether, countries have enacted cybercrime laws and deployed strategic methods to control and prevent cybercrime, even though they could not yet overpower the steadily growing cybercrime and risks associated with. Most specifically, hereunder we are going to discuss and compare cybercrime legal regimes in India, Nigeria along Ethiopia.

A. India

As discussed above, in India cybercrime has been surging over the years as the stats rightly shows. Alike trended in most jurisdictions, the government of India has taken laws and other relevant measures to halt the spread of cybercrimes. Of the steps taken to prevent cybercrime, measures of legislation and regulation have been discussed as follows.

i. Legislative Measure

The country has enacted the Information Technology Act (hereinafter ITA) in 2000, which is the first of its kind to deal with information and technology.[137] It enacted with the objectives to provide legal recognition for transactions carried out through electronic means, to facilitate the electronic filing of documents with government agencies, and to amend certain Acts, *inter alia*, the Indian Penal Code 1860, Indian Evidence Act 1872.[138] But with the advancement of technologies, many loopholes of the ITA were noticed that led to the passage of the IT (Amendment) Act 2008

[135] Iyasu T. 'Cybercrime in Ethiopia: Lessons to be learned from International and Regional Experiences' (n 34) 48
[136] Ibid
[137] Y. Karali et al, 'Cyber Crime: An Analytical Study of Cyber Crime Cases at the Most Vulnerable States and Cities in India.' (2015), Vol. 5 Issue. 2, International Journal of Engineering and Management Research, 43
[138] Ibid, 44

(hereinafter ITAA) which was made effective from 27 October 2009.[139] The Protection of Children from Sexual Offences Act, 2012 was also enacted to protect children from being used for sexual purposes and to further strengthen the provisions stipulated under the ITAA.

As stated above there are developments in cyber law in India, but we are specifically concerned to examine such a legal regime related to cybercrime. The ITAA lists out cyber offenses with respective penalties to prevent cybercrime and deter cyber criminality to ensure information security of users. For example, an act of tampering with a computer source document entails 3 years of imprisonment or a fine of 2 lakh Rupees or both.[140] Acts of hacking, dissemination of malicious programs to cause damage to computer systems or networks and DoS attack has been punishable by 3 years of imprisonment or fine of 5 lakh Rupees or with both.[141] Including cyber stalking, identity theft, impersonation, breach of confidentiality and privacy, distribution of obscene material and child pornography, online fraud, are among online criminal activities criminalized and punishable under the Act.[142] Furthermore, aiming to protect confidentiality and privacy of personal data and to deter insiders from committing data breach, the Act prohibits and penalizes acts of causing loss against the persons by intermediaries or its employees using their position.

In addition, pursuant to s 87(zg) of ITAA the central government enacted information technology intermediary and cybercafé guideline rules.[143] Information technology intermediary guidelines have imposed a duty on intermediaries to have rules, regulations and private policy to monitor users from engaging in content-related crimes using ISPs or Cybercafe operators computer systems and networks.[144] Furthermore, the intermediaries shall report cyber security incidents and share cyber security incidents related information with the Indian Computer Emergency Response Team (hereinafter CERT-In).[145] Concerning internet café operators, the Information Technology

[139] Ibid
[140] The Information Technology ACT 2008 (as amended) of India, s 65
[141] Ibid, s 66
[142] Ibid, s 66A, C, D, E, 67, 67 A-C, 71, 72
[143] Eze Kenneth Uzor, 'A Review of The Problems in Regulating the Internet Use: Enforcement Mechanisms Against Cybercrimes Under International Law', (PhD Thesis, Nnamdi Azikiwe University, 2016) 243
[144] Information Technology (Intermediaries guidelines and Digital Media Ethics Code) Amended Rules, 2021, Rule 3 (1) (2) (a) - (i).
[145] Ibid, Rule 3 (9)

(Guidelines for Cyber Cafe) Rules requires service providers to keep record of users' identification, in addition to obtaining the photograph of users using a web-camera installed on the computers in the cyber-café and immediately to notify police upon reasonable suspicion.[146] Generally, in India there are ITAA, IT intermediary guideline and Cyber cafe operator guideline rule as a primary cybercrime concerning laws that are used to tackle cybercrime.

ii. Regulatory Mechanisms Device to Enforce Cybercrime Laws

Equally, alongside the long lists of cyber offenses to criminalize misuse of computer technologies and the Internet, the ITAA has established institutions to effect implementation of the law, conduct effective detection, investigation, prosecution and punishment of cybercriminals and assert information security and safety in India. In this context, CERT-In was formed to undertake functions that have been mentioned under s 70B. The CERT-In has been mandated, among others, to forecasts and alerts of cyber security incidents, emergency measures for handling cyber security incidents, and coordination of cyber incidents response activities. To put this in effect, service providers, intermediaries, data centers, body corporate and any other person shall provide the information requested to the CERT-In and non-compliance will entail punishment by virtue of s 70(B,7).

Pursuant to s 69A of the Act, the Minister of Information Technology (hereinafter MoIT) is empowered to issue directions for blocking from public access of any information generated, transmitted, received, stored or hosted through computer resources following the instruction from CERT-In.[147] Minister of Home Affair (hereinafter MoHA) is another organization established to combating cybercrime in India, it deals with matters related to cyber security, cybercrime, design and implement National Information Security Policy & Guidelines (hereinafter NISPG) and grants states permit to set up forensic labs require to conduct computer crime investigation in India.[148] Police officers not below the rank of inspector, upon reasonably suspected of having committed or committing computer related crimes, have the power to effect search and arrest the suspect (s

[146] Information Technology (Guidelines for Cyber Cafe) Rules, 2011. Rule 4 (2) (3) (6)
[147] Dr. Karnika Seth, 'Combating Cybercrime in India' (2019) 41
[148] Ibid

80(1) of the Act). These aforementioned institutions are put in place to deal with cybercrime and enforce the law in order to control and prevent cybercrime in India.

B. Nigeria

Here, Nigeria's legislative and regulatory frameworks that have employed in effect control and prevention of cybercrime would be dealt with. The Nigerian experience of cybercrime and computer – related offenses assumed a terrifying dimension in the late 90s and early 2000 and is still on the rise with the advent of GSM phones, sophisticated computers and an influx of network providers which affords everyone equal opportunity to access the internet.[149] Cybercrime has been one of the eluding issues in the online global transactions in Nigeria because of the endemic nature of computer related frauds and crimes.[150] As discussed above, due to the growing tendency towards cyber criminality that undermines the country's reputation, the government of Nigeria has taken legislative and regulatory measures and promoted relationships with the private sector and global cybercrime enforcement agencies to limit its consequences. Accordingly, as illuminated by Muktar Bello, the government of Nigeria has taken drastic measures in creating central agency to enforce criminal laws, regulation of cybercafés, enactment of cyber laws and government partnership with international electronic service providers like Microsoft to overcome the negative financial and economic consequence of cybercrime in the country.[151]

i. Legislative Measure

Criminal Code Act of 1990, EFCC Act of 2004, AFF and Other Fraud Related Offenses Act of 2006, Evidence Act of 2011 (as amended) and Money Launder Act (as amended) are some of the laws that have had cybercrime implication in Nigeria. But the effort through such a legal regime remains incomparable to the increasing tendency of cyber criminality within the country.[152] Whereas, this was inspired cybercrime specific law, named the Nigerian Cybercrime (Prohibition and Prevention) Act of 2015[153] to be enacted on May 15, 2015. Before the enactment of the

[149] Ufuoma V. Awhefeada & Ohwomeregwa Ogechi Bernice, 'Appraising the Laws Governing the Control of Cybercrime in Nigeria' (n 49) 31
[150] Muktar Bello, 'Investigating Cyber Criminals in Nigeria: A Comparative Study', (n 96) 21
[151] Ibid
[152] Ibid; Awhefeada, 'Appraising the Laws Governing the Control of Cybercrime in Nigeria' (n 135)
[153] Cybercrimes (Prohibition and Prevention) Act, 2015, s 6, 8-10, 12-14, 16, 23-26

Cybercrime Act in 2015, there was the Nigerian Criminal Code Act of 1990, this Act has relevance regarding cybercrime.[154] As Olubukola S. Adesina argued that 'the specific provisions relating to cybercrime is s 419, while s 418 gave a definition of what constitutes an offense under the Act'.[155] Also, as quoted by Muktar Bello, Chawki et al. argues that under the Nigerian Criminal Code, advance fee fraud qualifies false pretense while an internet scam would amount to crime under s 419 of Criminal Code.[156] It read as;

> *"Any person who by any false pretense, and with intent to defraud, obtains from any other person anything capable of being stolen, or induces any other person to deliver to any person anything capable of being stolen, is guilty of a felony, and is liable to imprisonment for three years".*

EFCC Act 2004 (as amended) is also another law that has cybercrime implications;[157] as it regulates economic and financial crimes. By virtue of s 1(1) of EFCC Act, EFCC (hereinafter the Commission) established to discharge the functions and responsibilities stated under s. 6& 7(1) of the Act and enforce the legislations mentioned under this Act (s. 7(2)). Accordingly, the Commission is a leading Nigerian law enforcement agency that investigates economic and financial crimes such as AFF (419 fraud) and money laundering.[158] It also serves as Nigeria's designated Financial Intelligence Unit (hereinafter NFIU) and is charged with 'preventing, investigating, prosecuting, and penalizing financial and economic crimes such as … cybercrime, advance fee fraud (419 or advance obtained through different fraudulent schemes), banking fraud and economic governance fraud.[159] In addition, it has the power to monitor and raid internet cafes, and in most cases, stop night browsing at the cafes.[160] Furthermore, the commission shall initiate, develop and improve specific training programs to boost enforcement and other personal charges to overwhelm tools and techniques used for cybercrime commission.

---

[154] R. Abubakar, *et al,* 'Appraising Institutional Capacity for Implementation of the Nigerian Cybercrime Act 2015' (2017), Vol. 2, Proceedings on Big Data Analytics & Innovation (Peer-Reviewed) 64

[155] Olubukola S. Adesina, 'Cybercrime and Poverty in Nigeria' (2017) Vol. 13, No. 4, Canadian Social Science, 25

[156] Muktar Bello, Investigating Cyber Criminals in Nigeria: A Comparative Study' (n 136) 48

[157] Economic and Financial Crimes Commission (Establishment) Act 2004

[158] Muktar Bello, Investigating Cyber Criminals in Nigeria: A Comparative Study' (n 142) 26

[159] Obuah (2010) as quoted by Muktar Bellom 'Investigating Cyber Criminals in Nigeria: A Comparative Study' (142), 49

[160] Olubukola S. Adesina, 'Cybercrime and Poverty in Nigeria' (n 141) 27

The AFF Act 2006[161] was a deliberate and concerted effort by the Nigerian government to tackle effectively the menace of advance fee scams.[162] The Act define AFF pursuant to s 23 as; '*A representation, whether deliberate or reckless, made by word, in writing or by conduct, of a matter of fact or law, either past or present, which representation is false in fact or law, and which the person making it knows to be false or does not believe to be true'*. Moreover, through its s. 1 to 10 the Act mentioned offenses of AFF and prescribed a proportionate penalty. Telecommunication, ISPs and internet cafés are bound to enforce the AFF Act by virtue of s. 13 of the same Act and required to retain a record of traffic data and handover it to EFCC upon request.

As all the above legislation has proven ineffective in curbing cybercrimes as it is on its rise.[163] To put a robust legal regime in place in turn to take away ineffectiveness and gaps, the Nigerian Cybercrime Act has been enacted with the objective to fill the loophole left by the preexisting laws. The Act provides an effective and comprehensive regulatory, legal and institutional framework for effective detection, prevention, prohibition and prosecution of cybercrimes in Nigeria. It has served two fundamental objectives as mentioned under s. 1 of Act. These are to ensure protection of critical infrastructure and to promote cybersecurity in order to protect computer systems and networks, electronic communications, intellectual property, and privacy rights. Considering the rate of prevalence in fraud and cybercrimes within the country, the Act becomes more concerned with these problems and prescribes lists of cybercrime offenses along with appropriate penalties to tackle its effect and prevalence. These offenses have ranged from the act of tempering against national information infrastructure, illegal access, system interference and interception to computer related and content related crimes. To curtail the vulnerability of financial institutions for cybercrimes, the government also imposes certain responsibilities on financial service providers. Accordingly, s 37 (1a, b) and 2 of the Cybercrime Act provides a duty on financial institutions to verify the identity of customers carrying out electronic financial transactions, requiring the apply principle of knowing your customers and documenting customers' electronic transfer, payment, debit and issuance orders. This is basically to prevent cybercrime money laundering.

[161] Advance Fee Fraud and Other Fraud Related Offence Act 2006 as amended
[162] Muktar Bello, 'Investigating Cyber Criminals in Nigeria: A Comparative Study' (n 145) 49
[163] Olubukola S. Adesina, 'Cybercrime and Poverty in Nigeria' (n 146) 26

ii. Regulatory Mechanisms Device to Enforce Cybercrime Laws

Nigeria has established and empowered the EFCC to discharge the functions and responsibilities given under the establishment Act (EFCA) in order to tackle cybercrime in Nigeria. In addition, the cybercrime Act under s 41 (1) has established the Office of the National Security Adviser (ONSA) as a coordinating body for the administration and enforcement of all LEAs and security agencies under the Act. And to provide support to relevant agencies in combat cybercrime, establish and maintain the National Computer Emergency Response Team (CERT-Ng), establish appropriate platforms for public private partnership, and establish and maintain a National Computer Forensic Laboratory are amongst others.

Significantly, all these legislative and regulatory efforts have helped Nigeria to score significant improvement in dismantling cybercrime activities which have been prevalent in the country.[164]

C. Ethiopia

Studies have shown that[165] Ethiopia has massively undergone the process of expanding ICTs and Telecommunication services especially since the Growth and Transformation Plan (hereinafter GTP) I was announced. As a result of such development there is an increment in the internet penetration rate and the Internet users bases. Both Halefom and Iyasu argued that notwithstanding the advantage of technological transformation, the country has become abundant target for cyber-attack account the technological illiteracy of the majority of users,[166] having one of the poorest cybersecurity systems. Beside this fact, to reduce the threat of exploitation of technology by cybercriminals and henceforth to reap economic and technological benefit out of it, the country has taken numerous efforts. In net shell, legal and strategic/technical measures have been taken to fight cybercrime – by adopting policy measures (National Information Communication Technology Policy & Strategies, 2009 (NICTPS), National Information Security Policy, 2011 (NISP), and Criminal Justice Administration Policy, 2011(CJAP)). Legislative Measures are also adopted along with institutional and technical measures in order to implement these policies. Saying this much in general, now it is time to delimit the discussion to focus only on legislative

[164] Muktar Bello, 'Investigating Cyber Criminals in Nigeria: A Comparative Study' (n 148)
[165] Iyasu T., Cybercrime in Ethiopia: 'Lessons to be learned from International and Regional Experiences' (n 121) 46-47; see also Halefom H. 'The State Of Cybercrime Governance In Ethiopia', (n 111) 4-5
[166] Ibid

and institutional frameworks employed in the country to prevent cybercrimes and cyber criminality.

i. Legislative Measure in Ethiopia

To examine legislative measures in Ethiopia, before the enactment of Computer Crime Proclamation No 958/2016, there exist some legislations which had limited provisions regarding cybercrime and crime on information security including Money Laundering and Financing Terrorism Proclamation No. 780/2013[167], Vital Events Registration and National Identity Card Proclamation No. 760/2012[168], Telecom Fraud Proclamation No. 761/2012[169] and FDRE Criminal Code 414/2004[170].

Money Laundering Proclamation No. 780/2013 has a provision under its Art. 8 which requires financial institutions whose activities include wire transfer shall take appropriate customer verification measures and follow up transactions. This is to prevent the financial institutions from being an avenue for cybercriminals to launder ill-gotten money through electronic money transfer systems. Financial Intelligence Center (hereinafter FIC) which was established pursuant to Council of Minister Regulation No. 171/2009 has empowered to carry out powers and duties stated by the proclamation. Among these, the center, upon reasonable suspicion, shall forward the information to appropriate crime investigatory bodies for further action to be taken.

Vital Events Registration and National Identity Card Proclamation No. 760/2012 is the other law that deals with cyber-security related issues.[171] Art. 65 states that the protection of information from electronically designed attack, theft or from other similar criminal abuses. Such offenses have culminated with punishment stipulated under subsequent Art. 66. Again, Telecom Fraud Proclamation No. 761/2012, also another law that criminalizes misuse or interference into telecommunication resources and services. The proclamation can be considered the first "Internet

[167] FDRE Money Laundering and Terrorism Financing Proclamation No. 780/2013 (hereinafter Money Laundering Proclamation), entered into force Feb 4, 2013

[168] FDRE Vital Events Registration and National Identity Card Proclamation (amendment) Proclamation No. 1049/2017 (Vital Event Registration Proclamation), entered into force August 7, 2017

[169] FDRE Telecom Fraud Proclamation, Proclamation No. 761/2012 (hereinafter Telecom Fraud Proclamation), entered into force Sep 4, 2012

[170] FDRE Criminal Code (n 18)

[171] Halefom H. 'The State Of Cybercrime Governance In Ethiopia' (n 151) 16

law" in Ethiopia and contained measures aimed at combating cyber-attacks, including "unlawful interference," "unlawful interception" and "illegal access to a telecom network."[172] As quite clearly stated under art. 5 violation into the prohibition prescribed to commit illegal interception, unlawful interception and illegal access to a telecom network may be punishable with rigorous imprisonment from 10 – 15 years and fine from 100,000 – 150,000 ETB.[173] Lately, upon the enactment of the Computer Crime Proclamation this specific article was repealed.

There were also rules under criminal code to regulate the use of computers, which criminalized violations against information systems and misuse of computers, however, a very few acts of computer abuses were only criminalized – see art. 706-711, these are hacking, dissemination of malware and DoS attacks. On the fact of insufficiency of rules under the criminal code, Molalign A. argued that the gravity of the computer crimes is incomparably higher than the available legal remedies under the Criminal Code.[174] There are no sufficient lists of offenses to address ever-evolving cybercrime as the rules remain obsolete. This inadequacy of rules under Criminal Code in terms of criminalizing various offenses and disproportionality of punishment while compared to how devastative computer misuse is, enacting new cybercrime law at this point is unquestionably needed.

Accordingly, Computer Crime Proclamation No. 958/2016 was enacted. It is the most recent addition to the legal regime that criminalizes a range of cybercrimes and introduces a number of novel evidentiary and procedural rules that will assist in the investigation and prosecution of cybercrimes.[175] Numerous offences are criminalized under the proclamation; act of illegal access/hacking, illegal interception, system interference, DoS attack, dissemination of malicious computer programs, computer related forgery & fraud, identity theft, cyber stalking/harassment, child pornography and cyber terrorism[176] are among the prohibitions.

Furthermore, to regulate the distribution of illegal content data, the proclamation has imposed a duty upon ISPs that requires them not to take part in dissemination/edition and take appropriate

[172] Iginio Gagliardone and Nanjira Sambuli, 'Cyber Security and Cyber Resilience in East Africa', Global Commission on Internet Governance, Paper Series: no. 15 — May 2015, 4
[173] Telecom Fraud Proclamation, Art. 5.
[174] Molalign Asmara 'Compturer Crimes in Ethiopia: An Appraisal of the Legal Framework' (n 57) 99
[175] Kinfe Micheal, 'Some Remarks on Ethiopia's New Cybercrime Legislation' (n 31)
[176] Computer Crime Proclamation, Art. 3 – 14.

measures to remove or disable accessibility of this content.[177] To put it in effect, ISPs are required to retain computer traffic data that disseminates through its computer systems or traffic data related to data processing or communication service for one year.[178] Moreover, ISPs have also the duty to notify illegal content disseminated through its computer systems or networks to INSA and report the commission of crimes to the police.[179] When coming to the investigative power, the Public Prosecutor and Police are given joint power to conduct cybercrime investigation. In the meantime, INSA is empowered to provide technical support, conduct analysis on collected information and provide evidence if necessary.

In 2020 hate speech and disinformation proclamation[180] was enacted four years later to the Computer Crime law, to prevent and suppress dissemination of hate speech and disinformation, among other things, through electronic media including social media platforms. Dissemination of hate speech using broadcasting and social media platforms is prohibited and punishable with simple imprisonment not less than 2 years to 3 years or fine not less than 100,000 ETB.[181] In case when hate speech that has been aired inflicts damage on a person or groups the punishment would be simple imprisonment from 1-5 years.[182] Dissemination of any disinformation also made punishable under the proclamation for imprisonment of not exceeding 1 year or fine not exceeding 50,000 ETB, if the violence or disturbance followed, then the punishment would be rigorous imprisonment from 2-5 years.[183] Where an offense of hate speech and disinformation committed by social media accounts more than 5,000 and broadcasting services then the punishment would be simple imprisonment not less than 3 years or fine not less than 100,000 ETB.[184] It has imposed duties on social media service providers that they should suppress and prevent dissemination of disinformation and hate speech through their platform or should act within 24 hours to take appropriate measures to take down the circulation of such content.[185] Generally, the proclamation

[177] Ibid Art. 16
[178] Ibid Art. 24 (1)
[179] Ibid Art. 28(1).
[180] Hate Speech and Disinformation Prevention and Suppression Proclamation No. 1185/2020 (hereinafter Hate Speech Proclamation), entered into force March 23, 2020.
[181] Ibid Art. 7 (1)
[182] Ibid Art. 7 (2)
[183] Ibid Art. 7 (3)
[184] Ibid Art. 7 (4)
[185] Ibid Art 8 (1-3)

has its share to suppress and control hate speech and disinformation through computer technologies and information systems. However, in respect of having legal frame the government has made a huge call but remains behind in stepping to international cooperation mechanisms to work in joint hand with giant online service providers such as Facebook, Yahoo and Google whose online platform would be used to abuse the law. Mostly, as hate speech and disinformation have been committed using offshore social media platforms and browsing websites. However, through this proclamation government have an opportunity to consider cooperation with different countries and private online industries to limit the effect of hate speech and disinformation that nowadays influx in Ethiopia with rapid pace.

ii. Regulatory Mechanism Devices to Enforce Cybercrime Laws

Regarding institutional arrangements, since mere existence of laws that prohibit and prevent information security threats and attacks on computer systems does not produce effective results in terms of tackling the problem, thus it becomes imperative to have well-organized institutions for effective implementation of cybercrime law and measures. Considering this fact Ethiopia has established various institutions composed of experts and equipment required to detect, investigate and respond to cybersecurity threats and cybercrimes. Accordingly, in this section we are going to discuss hereafter institutions mandated to protect information security and investigate cyber-attacks in Ethiopia.

INSA is one of the information intelligence agencies; it was established as a primary organ to deal with the issue of cybersecurity and entrusted with the task of protecting the country from cyber-attacks of both domestic and international sources.[186] In 2006, it was established by the council of ministers regulation no. 130/2006 and re-established in 2011 by regulation no. 250/2011 & proclamation no. 808/2013.[187] Among other powers and duties stated under art 6 of the establishment proclamation, the agency is required to take countermeasures against cyber-attacks, organize and administer National Computer Emergency Response Team (hereinafter CERT-Et) and provide assistance and support regarding cybercrime investigation. As well, the Computer Crime Proclamation imposed a duty upon INSA to establish an online computer crimes

[186] Iyasu T. 'Cybercrime in Ethiopia: 'Lessons to be learned from International &Regional Experiences' (n 151) 49
[187] Iginio Gagliardone and Nanjira Sambuli, 'Cyber Security and Cyber Resilience in East Africa', (n 158) 4

investigation system and provide other necessary investigation technologies. The other institution is the FPC, which is empowered to conduct investigations against crimes over information networks and computer systems by virtue of article 6(5, b) of the Federal Police Establishment Proclamation. Computer Crime Proclamation maintains the same and empowers federal police to monitor and investigate computer crime in collaboration with the MoJ. Cyber Unit was organized under FPC in 2004 with the help of the FBI to carry out forensic and cybercrime investigation. Also, the FIC was established by the Council of Minister Regulation No. 171/2009 to coordinate the fight against money laundering and financing terrorism, organized and analyzes information and performs other related task to implement the proclamation. By doing so, the center has a role in suppressing money laundering through electronic transfer systems. INSS is another intelligence organ with the responsibility to keep the country safe from both inside and outside threats, collect intelligence and evidence on national or economic security in collaboration with foreign country's counterparts. Alongside other relevant cybercrime relevant organs, it is the other institution with the mandate of information and cyber security protection.

Part III. Lesson Ethiopia Could Learn from India and Nigeria

In the effort to combat cybercrime and its consequences, as has been discussed in the preceding part, the government of Ethiopia, since the day it recognized the vulnerability of the national cyber environment to online malicious activities, has taken legal and technical measures. Among these measures, legal and regulatory measures employed to prevent cybercrimes are the basis to this comparison. In this context, the international legal approaches and best practice of the selected jurisdictions employed to prevent cybercrime in their respective jurisdiction have been discussed.

As mentioned in the preceding part of international frameworks, the Malabo and Budapest Convention are complimentary in supporting the effectiveness of Ethiopia's cybercrime legislative and enforcement efforts, this is why the researcher calls Ethiopia to join and magnify the benefit that would be gained by becoming part of such a cooperative framework. At global level, international legal framework could bring comprehensive international cooperation means in fight of transnational cybercrime cases, as it attempts to respond to 'lack of criminal laws, lack of procedural powers and lack of enforceable MLA provisions'[188]. To benefit from the opportunities

[188] UNODC, 'Comprehensive Study on Cybercrime' (n 180) 195

that such regional frameworks provided in terms of facilitating LEAs accessing electronic evidence in investigation of cross-border cybercrime cases and cooperation in law enforcement, it has indispensable advantage for Ethiopia. Ethiopia has included many provisions from Budapest Convention while it enacted computer crime proclamation.[189] But beyond this modeling, if Ethiopia were to be part of this regional instrument with the rising recognition at international level, the country would benefit from the international cooperation method that it strives to realize.

Then, to look for best lessons from legislative and regulatory activities taken by the selected countries, here below the experience of both India and Nigeria have been discussed in fair detail. Firstly, Ethiopia is supposed to get a lesson on the administration of the spamming problem which has grown as one of the prevalent offenses committed over electronic communication. The legislative measure taken to repel the effect of spamming, Nigeria has included in its Cybercrime Act and tries to address this most prevalent and dominant online criminal activities in the country. Typically, in Nigeria spamming is rampant and makes headline news.[190] Considering this fact, the government in mitigating the problem posed related to spams, it addressed the issue under s 32 of cybercrime Act. Initially, the Act has defined spam as '*an abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages to individuals and corporate organizations.'* Within this definitional context, it criminalized such acts to prevent unauthorized messages through email or any electronic communication that has been sent to fake the recipient. Unlike this trend in Nigeria, the Ethiopia computer crime law does not provide rules directly deals with such act of spams, save for the provisions that criminalized computer related fraud[191] and advertisement messages (unsolicited commercial email) sent without recipients consent that lacks deepness.[192] In comparison with the evolving trend of sending bulk unauthorized messages through the internet and other electronic communication which is available for criminals to exploit and send spam messages, Ethiopia fails to address this worldwide problem within its cybercrime law. Fraudulent may use it to disseminate, *inter alia,* product or service advertisement, online auction and sales, that is, fake or non-existed. Furthermore, those spam emails which have not commercial purpose

[189] Iginio Gagliardone and Nanjira Sambuli, 'Cyber Security and Cyber Resilience In East Africa' (n 173), 4
[190] See BBC News, Available at <https://www.bbc.com/news/world-africa-49759392>; Wired, Available at <https://www.wired.com/story/migerian-email-scammers-more-effective-than-ever/> Accessed on Nov 25, 2021
[191] Computer Crime proclamation, Art. 10
[192] Ibid, Art. 15

but which are used to disseminate malware, fraudulent schemes and the like must be address to limit the magnitude, among other, electronic messages containing sexually oriented material.[193] Therefore, Ethiopia should learn from the legislative experience of Nigeria to deal with spamming and related crimes in its broadest sense to mitigate fraudulent activity affecting trust and confidence of electronic users to engage in electronic transactions including e-commerce, electronic financial and banking transactions. So, in this respect Ethiopia needs to either incorporate specific provisions to deal with spam by amending the existing computer crime law or enacting specific law on the area to address the legal and practical problem in detail.

Secondly, Ethiopia must consider mechanisms to mitigate online intermediaries as a source of cybercrime. Ethiopia has expressly prohibited and criminalized content-related crimes under the computer crime proclamation and hate speech proclamation. But these laws did not comprehensively regulate information technology intermediaries or ISPs to enforce the prohibition by making distribution of illegal content data not pass through their computer systems or networks. Except for criminal liability provided under the above-mentioned laws that oblige taking measures to remove or disable accessing illegally contented data and duty to report the commission of crime through service provider's computer systems and networks. Though, it was not as proactive as it is in the case of India and Nigeria. The system that needs ISPs and internet intermediaries to provide rules, regulation, and term and policy noticing that their computers and networks shouldn't be used to disseminate and browse illegal content data and retain relevant data records of users. Instead in Ethiopia the law primarily focuses on being reactive to the crime rather than being proactive with the issue, if any, to make notice of any suspicion to the relevant investigative organ.

On this specific issue, Nigeria has dealt with the case by mentioning under s 7 of Cybercrime Act which stipulates the requirement that internet cafes to register in Computer Professionals' Registration Council and keep record of their users. They should make this record available to law enforcement personnel whenever required. Also, AFF Act of 2006 regulates ISPs and cybercafé operators and it imposes a duty to keep record of users and to get registered as business entities.[194] The same Act has imposed the duty of care on service providers to ensure that their services and

[193] Jonathan Clough, 'Principles of Cybercrime' (n 106) 242
[194] Advance Fee Fraud and Other Related Offences Act, 2006, Section 12(1), 13(1)

facilities are not exploited for unlawful activities.[195] India also enact guidelines to regulate the functions and responsibilities of intermediaries and cybercafé operators,[196] in addition to due diligence requirements stated under s 79 of ITAA. In Ethiopia, like the case in the rest of the world, along other targets wireless internet access points are vulnerable to cybercrime activities. To state a few offenses committed through the use of public and private internet access, such as disseminating illegal contents, commit hacking on bank accounts, make illegal electronic transfers and scams when cybercriminals easily get weaker access points. Undeniably, this could make the duty of LEAs and intelligence agencies to detect and investigate cybercrime more cumbersome and difficult unless certain rules are deployed to set duty over ISPs such as hotels, education and other public and private institutions and over internet café operators in Ethiopia. However, to reduce the mismanagement and inappropriate use of the internet from internet café putting regulation in place will rescue not only individual victims but also the country's national security. To secure cyberspace from attacks originated from networks and computer systems of internet service providers the government should take the lesson from the aforementioned trends of India and Nigeria that create specific and robust legislative measures and regulatory institutions akin to EFCC in Nigeria, intermediary and ISPs guideline rules in India. Accordingly, Ethiopia is supposed to take a move to enact rules to guide internet service provision within the country and mandate institutions to bear regulatory roles to enforce the legal framework.

Thirdly, regarding regulatory mechanisms to enforce and oversee effective implementation of legislative measures, Ethiopia may impart some basic practice in this respect. While electronic crime has been committed, the criminal justice system is effective, so in this way enforcing cybercrime law would begin, that is, culminated by electronic data collection, investigation and prosecution of perpetrators. Accordingly on investigation as the course in the criminal proceed, the regulatory capacity for example in this specific aspect as highlighted by Iyasu Takele the Cyber Unit is shortly limited. Since it has been confined to investigate some criminal acts among a vast array of computer offenses that have been committed and committed in the country.[197] Let us look

[195] Ibid, s 13(3); see also ABUBAKAR, R. *et al*, 'Appraising Institutional Capacity for Implementation of the Nigerian Cybercrime Act 2015' (2017), Vol. 2, Proceedings on Big Data Analytics & Innovation (Peer-Reviewed) (n 140) 65
[196] See Eze Kenneth Uzor, 'A Review of The Problems in Regulating the Internet Use: Enforcement Mechanisms Against Cybercrimes Under International Law' (n 129)
[197] Iyasu T., Cybercrime in Ethiopia: 'Lessons to be learned from International and Regional Experiences' (n 172)

at the experiences. In India, police developed cybercrime investigation cells all over India and 39 forensic labs at both state and central level to investigate plenty of criminal activities over the Internet and computer.[198] These Cyber Crime Cells investigates cases pertaining to hacking, spread of the virus, pornography, manipulation of accounts, alteration of data, software piracy, create false websites, printing of counterfeit currency, forged visas, theft of intellectual property, email spamming, denial of access, password theft, crimes with cell phones and palmtops, cyber terrorism etc.[199] No doubt, this has offered India the chance to address a broad array of cybercrime offenses in terms of detecting, responding and investigating. Unlike India, in Ethiopia there is only one forensic investigation unit that is organized under the FPC and burdened with heavy responsibility to give forensic investigation function nationwide as there is no such organ existing under any of the regions. In terms of equipping with latest and advanced forensic investigation tools which help detection and investigation of cybercrimes, Nigeria also has built a DNA Forensic Laboratory Centre in addition to the EFCC's own Digital Forensic Lab equipped by the UK government. Hence in this respect Ethiopia has to share this best practice to establish a number of cybercrime units enough to meet the current need and reorganize the existing with all relevant investigation tools, methods and human resources.

Fourthly, Ethiopia needs to share the practice of working jointly with private sectors. In terms of establishing and promoting partnership with private sectors to get technical capacity, expertise and resources of private industries, the Indian government has undertaken cooperative and collaborative relations with private sectors. As part of this effort, in 2004 with the support of the Department of Electronics and Information Technology India's Cyber Labs program initiated by the NASSCOM (private sector institution).[200] This institution has the resources and capacity to educate a number of police officers, prosecutors and others on cybercrime related matters and undertake cyber-security awareness creation activities.[201] Previously, these all were upon the government and its organs, though this has impacted the efficiency of combating cybercrime and implementing regulatory responses otherwise partnership arrangement has resolved the problem.

[198] Dr. Karnika Seth, 'Combating Cybercrime in India' (2019) (n 133) 42
[199] Vineet Kandpal and R. K. Singh, 'Latest Face of Cybercrime and Its Prevention in India' (2013), Vol. 2. No. 4, International Journal of Basic and Applied Sciences, 154
[200] Nir Kshetri, 'India's Cybersecurity Landscape: The Roles of the Private Sector and Public-Private Partnership' (2015), IEEE Security and Privacy Magazine, 5
[201] Ibid

In Nigeria, for example, the memorandum of understanding signed with Microsoft that gives an advantage to tackle cybercrime through implementing awareness creation and capacity building activities invites the involvement of institutions and stakeholders in the fights.[202] To accrue these and other benefits in the fight against cybercrimes, specifically, regarding hate speech and fake news that become endemic in the country, Ethiopia must stick to such experiences and join effective and operable bilateral and multilateral cooperation frameworks.

[202] Muktar Bello, 'Investigating Cyber Criminals in Nigeria: A Comparative Study' (n 150) 60

Chapter Four

Challenges Facing Prevention and Control of Cyber Criminality, Enforcement of Cybercrime Law and Curtailing Mechanism in Ethiopia

Introduction

Relentlessly, cybercriminals are finding innovative ways to overpass the existing control and protective measures, thus obviously countries should review their status to determine whether they are capable to respond properly to this continuously evolving problem. However, their assessment should not only be confined to technical and legislative measures, rather it should extend to review and improve the regulatory enforcement mechanisms to address the situation well. Right away, while the outcome shows a gap in cybersecurity and cybercrime prevention and control readiness, the government should strive to improve measures that have to be taken to mitigate cybercrimes.

Accordingly, under this chapter, the study has been examining the challenges hinder LEAs and investigatory organs from properly carrying out their duties as expected in the law. We are also undertaking comparisons with the situation in India and Nigeria to draw lessons for Ethiopia if they develop best practices that help combat cybercrime and survive its destructive effect.

4.1 Challenges Facing Prevention and Control of Cyber Criminality: Specific Reference to Ethiopia's Case

Nowadays, it has been an undeniable fact that countries, especially developed countries, have been equipped with advanced technologies and built robust cyber-security systems. Though, at the same times, there are professional cybercriminals possessed excellent technological knowledge and tools[203] to circumvent electronic technologies to use it for their criminal purpose. Worst, cybercriminals often have more advanced skill and tools than law-abiding technology professionals acquired.[204] Accordingly, under this section of the study we are going to examine some of the technology enabling challenges that hinder law enforcers and investigatory bodies from implementing criminal law and criminal justice systems pertinent to cybercrimes cases. To

[203] See Kabiru H. Mohammed, *et al*, Cybercrime and Digital Forensics: 'Bridging the gap in Legislation, Investigation and Prosecution of Cybercrime in Nigeria' (2019), Vol. 2 Issue 1, International Journal of Cybersecurity Intelligence & Cybercrime, 58
[204] Ibid

state some instances; the cross-border nature of cybercrimes, complicated methods used by perpetrators to curve-out investigation techniques in a way that help them - the technique that was initially developed to counter cybercrimes, perhaps this may further exacerbate the hurdle on LEAs. Also, there is a challenge to create a law enforcement mechanism that is designated specifically to preserve and collect electronic evidence for investigation as the existing investigation method didn't suit the new development on crime commission through virtual or electronic technologies. In turn, if this challenge has been handled properly it will be used to fill gaps of traditional crime investigation methods. Fundamentally, the above illustrated challenges could be a limitation to the country's strive against cyber criminality, considering the fact that cybercriminals are often ready, skilled, and acquire scientific knowledge and tools to cause cyber-attack. On the other hand, countries especially developing like Ethiopia, those that had not yet developed strongest cyber-security systems and even struggling to finance cyber-security governance, *inter alia*, to incentivize experts to get their allegiance and to ensure that they would not turn to weaponized their expertise. Instead, to use them to hunt down cybercriminals who exploit technological savvy. Undeniably, these and other challenges may have hindered cybercrimes prevention and strives to enforce criminal justice in relation to cybercrime cases unless timely resolved.

To look specifically at Ethiopia's case, there are already numerous challenges posed against the effort to curb cybercrime. As the former INSA Director-General, Ifrah Ali alleged it 'lack of awareness creation', 'inadequate legal framework' and 'poor cybersecurity governance' are among the major challenges in relation to cybercrime prevention, as reported by the Ezega News.[205] Likewise, the information gathered from data informants selected purposely from INSA, MoJ and FPC have proven that these limitations still existed in the Ethiopia cybercrime legal regime. Also, this has accompanied by lack of developing comprehensive prevention and investigation systems which culminate by hampering police and legal experts from conducting pre-assessment to reverse prematurely or to gather evidence, conduct investigation and apprehend the criminals upon the commission of cybercrime respectively. Fundamentally, Ethiopian computer crime and related laws face implementation problems associated with technical, legal, and enforcement challenges

[205] Ezega News, Dec 6, 2019, Available at <https://www.ezega.com/News/NewsDetails/7518/INSA-Aborts-Cyber-attacks-on-Finanacial-Institutions > Access on Dec 16, 2020

to fight cybercrime as relevant data shows. Typical challenges that face prevention and control of cybercrime have been discussed below.

4.1.1 Inadequacy of the Legal Framework

In many countries, cybercrime related laws remain obsolete in comparison to the emerging technologies across the globe and cybercriminals' restlessness in finding ways to exploit technologies.[206] Thus, in the fight of cybercrimes, deceleration in legislating new law to regulate online criminal activities and abuse of computer systems or lack reviewing the existing laws to readjust with the emerging computer offenses will be at the expense of the process. In addition, this may enable cybercriminals to operate with impunity in a particular jurisdiction because the criminal law has not been upgraded or non-exist at all to take care of the emerging cybercrimes and cyber criminality.

Mindful of the importance of having tailored law in prevention of cybercrimes, Ethiopia has already enacted laws to address the problem. Here to start with, the computer crime proclamation no. 958/2016 is a comprehensive and cyber specific law that criminalizes offenses against computer systems, data and networks. Among others, there is also hate speech proclamation that has a direct cybercrime implication. Besides having such laws on this specific issue, there are offenses that have been committed through or against computer systems but yet remain unaddressed. For example, using internet to produce, disseminate and possess obscene articles such as pornographic materials that is against public morality and should be criminalized to daunt the tendency to it. Likewise, the act of blackmailing someone through the use of the internet to disseminate his/her privacy that ought to be criminalized has left to be addressed in Ethiopia in a clearly and technology affiliated sense. So, Ethiopia needs to address by promulgating laws against such and other content related cybercrime to limit their psych-social effect.

Almost all respondents from INSA, FPC and MoJ succinctly state the situation in Ethiopia as it is characterized by the lack of compatible legal regime when it comes to cybercrime related offenses. Mr. Getiye Belihu from the MoJ briefed that the cybercrime legal regime of Ethiopia as ‘the country is quickly and widely diving to the electronic technologies that in reality ensue technology

[206] World Bank and United Nations, ‘Combatting Cybercrime: Tools and Capacity Building for Emerging Economies’ (Washington, DC: World Bank, 2017), 19-22; see also ITU, ‘Understanding cybercrime’, (n 110) 82-83

related crimes, beside this fact looking at our law on the other side doesn't match the effort that has been done to digitalized the country'. He firmly says that the country must have worked parallel to have best cyber-security governance by enacting laws that regulate e-transaction and which envisage criminal activities that would introduce as of the new development. Likewise, anonymous respondents from the same institution share the same view and add that 'there has been technological advancement in the country that requires sufficient laws that are comparable to such development but it is lagging behind by far'. Furthermore, other anonymous respondents from FPC state that numerous cybercrime related offences are committed but considering lack of provision addressing such specific acts that the criminal responsibility would not be entailed. The same respondent from FPC indicates that the development of cybercrime legal regime has not only fallen behind technological development but also the cyber criminals' cautiousness to evade responsibility has overarched legal regime in Ethiopia.

At this juncture, we can understand that in the absence of trends to review law in a continuous interval for containment of evolving cybercrime offenses and standardizing procedural and evidentiary rules that enhance detection and investigation it could be found difficult to combat cybercrime. Hence, using this legal loophole cybercriminals could expand their criminal activities to undermine information security and in turn it may be to the detriment of individuals, business and government interest. Inevitably, this would also create safe haven for criminals and facilitate for the same criminal mentality to swiftly develop in Ethiopia unless the measure to detract legal lacuna has been taken instantly. At initials, regarding computer related offenses Ethiopia should take to criminalize those offenses have not yet criminalized. As it has been clear as crystal, in the absence of as much effort to harmonize laws, the country may trend/encounter challenges to accept law enforcement cooperation requested by other countries concerning the cyber offense which has not yet been criminalized in Ethiopia cybercrime regime. Therefore, as the country has not welcomed the legal assistance request, in turn since international legal cooperation is highly motivated with reciprocity, Ethiopia would not get the same and thus the process of cooperation would fail to operate properly. Therefore, Ethiopia must promptly act for legal harmonization in every potential development related to cybercrimes. This way the country would get foreign legal cooperation on law enforcement, expedite preservation and collection of evidence and joint cybercrime investigation.

4.1.2 Lack of Collaboration and Cooperation

Regarding cybercrime investigation, considering the development in sophisticated crime commission method, collaboration among states, between states' LEAs and with private sectors has firmly needed to pool together expertise and technical capability. Definitely, this cooperation also needed to exist at regional or international level to widen the extent of cooperation. Conformingly, there must also be effective cooperation between states to enforce cybercrime law that is dependent on the consent of the requested state – where the perpetrator lives, the attack has been from or the evidence has been found. At the same time, dual criminality is also contingent to put cybercrime law in effect, to get MLA cooperation (preserve and deliver data stored in foreign servers, conduct joint investigation and collect electronic data) or to have extradition. This is what makes the country must stick to the cooperation framework which is so important to deal effectively with such transnational cybercrime cases. Yet, there are hurdles surfacing the effort in combating cybercrime like absence of uniformity on cybercrime law, states' less responsiveness to join international cooperation platforms and slow feedback to the MLA requests.

Since the objective of this research is to assess the Ethiopian responses to this evolving problem in context of legal and institutional measures, we need to ask the question like 'Is the country committed to international cooperation and creating means of collaboration among its LEAs and with private security agencies'? On this question Mr. Tefera Debela from INSA, states that the country has bilateral legal cooperation with the countries to work over cybercrime law enforcement, joint investigation, information sharing and capacity building collaboration.[207] He said that INSA has mainly been established to effect such activities from its very inception even though the institution yet hasn't established an effective system in this specific regard to regulate international cooperation and to lead the cooperation satisfactorily.[208] Lack of a well-organized and comprehensive international cooperative system and institutions certainly hampers both

[207] The key respondent from INSA

[208] Ibid, anonymous respondent from MoJ also argued that to his knowledge even if INSA has assigned to such tasks and has designed plan to work on the issue, but has not fully engage to protect national information security and prevent attacks against private and public computer systems.

prevention of cybercrime and even after the commission the process to detection, investigation and prosecution of cybercrime considering its cross border effect, *per se*.[209]

Seemingly, having in mind the importance of promoting collaboration between government and private sector to tackle cybercrime, the Nigerian Cybersecurity Policy which was adopted in 2014, mentions the significance of strategic partnership with the private sector as policy guide.[210] Following this guide, Nigeria has mandated CERT-ng, which has been established under ONSA, to organize and coordinate law enforcement agencies activities so as to enhance comprehensive fighting against cybercrime.[211] Likewise, the Indian government also takes concrete measures as it establishes the seven pronged Indian Cyber Crime Coordination Center (I4C) to deal with cybercrime in a comprehensive and coordinated manner. Under this I4C Scheme the National Cybercrime Threat Analytics Unit (TAU), National Cybercrime Reporting, Platform for Joint Cybercrime Investigation Team, National Cybercrime Forensic Laboratory (NCFL) Ecosystem, National Cybercrime Training Centre (NCTC), Cybercrime Ecosystem Management Unit, National Cyber Crime Research and Innovation Centre are organized to enhance comprehensive responses. It has organized under the MoHA, among other, to leverage the strength and expertise of all stakeholders (from research institutes, private sector or inter-governmental organizations) and to create strategic partnerships with all stakeholders.[212] Moreover, in all of its activities and efforts the center aims to overcome obstacles by assisting states'/provinces' law enforcement agencies through conducting research on cybercrimes, facilitating exchange of information and cooperation amongst themselves.[213]

---

[209] Ibid, anonymous respondent from MoJ and FPC firmly state the negative implication that has come from lack of international, regional and bilateral cooperation especially in case when the perpetrator has lived in another country it has been hard to caught even if he is red-handed.

[210] National Cybersecurity Policy, Part Four, Section 4.5, Online Available at: <https://www.Cert.Gov.Ng/Ngcert/Resources/National_Cybersecurity_Strategy.pdf>

[211] Online available at: <https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-March-2019/Comments/Nigeri>; Article by Josephine Uba, 30 November 2021, Nigeria: The Legislative Framework For Cybercrime In Nigeria: Current Status, Issues And Recommendations <https://www.mondaq.com/nigeria/terrorism-homeland-security-defence/1136732/the-legislative-framework-for-cybercrime-in-nigeria-current-status-issues-and-recommendations> Accessed on 18 January 2022

[212] Online available at: <https://www.mha.gov.in/division_of_mha/cyber-and-information-security-cis-division/Details-about-Indian-Cybercrime-Coordination-Centre-I4C-Scheme> accessed on 18 January 2022

[213] CyTrain website, Available at: <https://cytrain.ncrb.gov.in/local/staticpage/view.php?page=CyTrain> Accessed on 10 January 2022

Speaking of how important creating institutional mechanisms that could help the works of different government institutions to be comprehensive in the fight against cybercrime, the I4C and the Nigerian CERT-ng could be a typical example. Therefore, Ethiopia needs to create a comprehensive scheme that can lead the efforts that have been done at different government institutions in the fight against cybercrime. With this regard the information from anonymous respondents with the rank of sergeant shows that there is a task force organized in collaboration by the MoJ and FPC to investigate and prosecute cybercrime. However, he argued that this collaboration is not sufficient as it is too specific in its scope to work only on cybercrime investigation and prosecution matters whereas there should be a broad collaboration scheme with all relevant bodies to effectively deal against cybercrime in every important aspect. In this sense, specifically the practice in India that devises to create partnership among governmental, research institutes, private industries and non-governmental organizations to conduct research and facilitate investigation, knowledge and information sharing would be the best lesson for Ethiopia to integrate partners in combating cybercrime using the same pattern as has been in the case of India. This means the country must organize institutions to facilitate collaboration among concerned cybercrime prevention and control bodies to work together, accessing similar databases for relevant crime records and information. Also, to be a point of contact and facilitate collaboration between LEAs and private sectors to enable joint research, training and capacity building on the use of forensic investigation technology and techniques.

4.1.3 Law Enforcement Responses: Inadequacy of Resources and Training Facilities

There are difficulties facing law enforcement responses that are to curtail the effect of cybercrime that range from organizing effective and efficient institutions filled with resources and training facilities to being active. However, here under this section the discussion has confined to problems facing in fulfilling human and material resources, and training facilities. Law enforcement responses must be reinforced with human resource, procedural and technical tools to conduct forensic investigation, analyze evidence, and prosecute cybercriminals. Firmly, there is also a need to resolve the problem associated with insufficiency of funds to enforce cybercrime measures effectively. Moreover, cybercriminals in an attempt to layer themselves and to remain anonymous might use a range of techniques including encryption, proxies, cloud computing service, ‘innocent’ computer systems infected with malware, and multiple (or ‘onion’) routing of internet

connections.[214] In order to address this challenge and volatility of digital evidence states' intelligence agencies and LEAs must be equipped with adequate resources, forensic science technologies and get continuous training in cybercrime investigation. The complex cyber-attacks that have been experienced from time to time in Ethiopia have presented a challenge to LEAs in their attempt to detect, investigate and reverse cyber-security threats and cybercrime.[215] Public prosecutor Mrs. Tenaye Abebe and anonymous respondent from FPC share the same ideas as they stressed that lack of well-developed schemes that enable them to conduct pre-assessment and investigation of this evolving technology-oriented crime has significantly affected the effectiveness of LEAs in conduct of their activities.[216]

It has been claimed that Over 90 percent of cyber-attacks in Ethiopia have occurred due to lack of proper tech knowledge.[217] Thus far the lack of professionalism and tech savvy in the country's cybercrime regime has been manifested.[218] Mr. Desalegn Agumas has further characterized Ethiopia's cybercrime regime as in which technological knowledge and skill possessed by cybercriminals has surpassed that of law enforcers.[219] Furthermore, he has succinctly argued that 'cybercriminals have used anonymity technology and tools, and proxy servers as this may cause knowing identity and character of cybercriminal unlikely possible'.[220] And he added that if the act of cybercrime attack has been supported/ sponsored by states so it will worsen the case even more. On this specific issue, his professional view is that the government must train technological experts, police, prosecutors, judges and others involving partners and must build a proactive cybercrime control and prevention system for effective enforcement of cybercrime law. Otherwise,

---

[214] UNODC 'Comprehensive Study on Cybercrime' (n 174) 122

[215] Ethiopian Monitor News, Aug 24, 2020, Available at <https://ethiopianmonitor.com/2020/08/24/insa-thwarts-787-cyber-attacks-on-ethiopia-in-2019-20-fy/> accessed on Dec 17, 2021

[216] The information that has received from the respondents of Minister of Justice and Federal Police Commission reveals the fact that the country doesn't have well organized scheme prevention and control of cybercrime incident to the level the context requires to be proactive.

[217] INSA's Deputy Director Kefyalew Tefera indicate that over 90 % of cyber-attack has occurred due to lack of technological awareness as reported by Ethiopian Monitor, online available <https://ethiopianmonitor.com/2020/08/24/insa-thwarts-787-cyber-attacks-on-ethiopia-in-2019-20-fy/>.

[218] Based on the information obtained from the respondents of INSA, FPC and MoJ

[219] In addition, the respondents from FPC reveal that individuals those commit computer related crime have utilizes anonymity techniques and proxy server to spoof the investigative police. The other respondent from MoJ affirms the same saying that cybercriminals install electronic materials or software that help hid their identity in order to further complicate verification of perpetrator's identity and locate the device or system the act has been emanated from.

[220] One of the key respondent and public prosecutor who is currently working at the cybercrime department in Minister of Justice.

it would cost the country unless timely responded by facilitating education and training mechanisms, among others, that may enable the production of educated and skilled workforce and establish forensic investigation centers filled with necessary investigation tools and scientific technologies.

Let us examine regulatory readiness and capability to enforce cybercrime law in terms of human resource, investigation techniques and tools, and training capability. Respondents from the institution of public prosecutor refer that the MoJ has been organized with human resources but is not at the best as relevant technologies are not fulfilled and saving the sudden training ensures the staff of cybercrime department do not get training at continuous intervals. Furthermore, Mr. Getiye Belihu argued that it is hard to say that LEAs and information intelligence agencies in Ethiopia have been organized in terms of experts, investigation technique and technology, and capacity building and training facility as sufficient as to counter the challenge at the course of implementing laws.[221] Generally, most of the respondents from all, INSA, FPC and MoJ have elucidated that regulatory readiness and law enforcement response remain incomparable to the evolving (in terms of magnitude and type) technology enabling offences.

Moreover, in resolving the problem associated with having trained manpower capable of comprehending and adapting to technologies so as to stand by the cybercrime prevention efforts. In this regard, academic institutions including law school, police training colleges and technology institutes should dedicate themselves to producing skilled and knowledgeable manpower.[222] Obviously, higher education institutions in the country provide technology affiliated education, but on the legal aspect such as on tactics of cybercrime investigation, use of technical terms in laws to effect prosecution and adjudication there is no curriculum to train. Firmly, respondents urge that the country, firstly, to design cybercrime related curriculum to include law education and other relevant institutions. Second, recruiting professionals and experienced law enforcement personnel, prosecutors and judges, in turn this may help to create technologically and professionally advanced institutions capable of reinforcing regulatory tasks. Lastly, engage in an awareness creation campaign to present individuals and institutions to have continuously updated

[221] Most of the respondents have also share the same and furthermore indicate that the country must commit to do more in order to reach the level required these days as the cybercriminals are advancing themselves by far, in terms of human resource, investigation technique and technology and training asset.

[222] The research participants from all (INSA, FPC and MoJ) institutions designated for this research wholeheartedly suggested that Ethiopia should have to incorporate cybercrime and related courses into the academic curriculum to produce experts in the field.

cybercrime prevention and control methods. Therefore, experts of legal knowledge and skill related to cybercrime will be available and as well continuous training should be accessible to personnel those already involved. Thus, this might strengthen regulatory capacity in dealing with cybercrime and related problems. The trend in India is helpful in this regard, there is Cybercrime Training Center created to provide standardization of curriculum and training focused on containment, detection, investigation and reporting of cybercrime through simulation and real training.[223] At present, the center has given virtual training for lawyers and police personnel on relevant issues that assist cybercrime prevention and control.[224] Ethiopia should have to learn from this and facilitate the incorporation of cybercrime and cyber-security related courses on law education curriculum and on other training institutions' programs and strive to create a body comprehensively lead with this task. The other best practice for Ethiopia, there has been a forensic laboratory facility under the NDFL to facilitate forensic investigation and provide LEAs with forensic technology, professional training, and investigation facilities and enhance cooperation in the combating cybercrime.[225] Also, this may support the creation of arrangements for strategic partnership with relevant stakeholders in the area of research and innovation focused on cybercrimes, cybercrime impact containment and investigations.[226]

4.1.4 Investigation and Preservation of Electronic Data

The data stored in computers has been susceptible for removal or alteration shortly by cybercriminals to remain unidentified and to impede the process of detection and investigation. In transnational cybercrime cases, international cooperation requests may easily take a longer time than the lifespan the data will exist or before the relevant search warrant or order for supply of stored data can be obtained.[227] This has been a problem in Nigeria, as its law enforcement officers lack the technical skills and appropriate technological tools to investigate electronic related

[223] CyTrain website, Available at: <https://cytrain.ncrb.gov.in/local/staticpage/view.php?page=CyTrain> Accessed on 22 January 2022

[224] The Economic Times, 21 Dec, 2021, Available at: <https://economictimes.indiatimes.com/news/india/modi-government-committed-to-deal-with-cyber-crime-says-home-minister-amit-shah/articleshow/88419150.cms> Accessed on 22 February 2022

[225] Available at: <https://www.csb.gov.bn/national-digital-forensics-laboratory> Accessed on 7 February 2022

[226] Ibid

[227] Williams P., 2008. Digital forensics and the legal system: A dilemma of our times. Available at: <http://ro.ecu.edu.au/adf/41/>

offenses that enable them to track down cybercriminals.[228] As a strategy to fill this gap, the Nigerian government made an understanding for cooperation with Microsoft that enables the country to get smart technology to take down malicious websites and cybercriminals and cooperation agreements with the FBI that help to have qualified and talented workforce to solve the problem associated with lack of expertise.[229] This problem has also faced Ethiopia too as the country does not have significant cooperation agreements to facilitate sharing of information, electronic evidence and moreover enforcement of cybercrime law.[230] LEAs in the country are unlikely to secure collaboration from foreign countries LEAs regarding expedite preservation and sharing digital evidence found in the server situated there and which is crucial to investigate and prosecute cybercriminals because of the limited number of cooperation agreements it has. No doubt this has encouraged cybercriminals to commit cyber-attacks against information and computer systems or hijacked innocent systems which are found in Ethiopia through botnets hence used to commit cyber-attacks against other countries. At the same time, the problem associated with expedite evidence preservation and investigation requires the help of foreign state's LEAs otherwise it substantially undermined Ethiopia's cybercrime prevention and controlling capability. Therefore, effective cooperation between or within countries to preserve electronic data and maintain its integrity becomes vital to overcome the challenge in this regard and to bring suspects to criminal justice and deter them.

As the development in technology grows continuously, India has organized the National Cyber Crime Training Center to boost detection, responding, investigation and prosecution capacity of LEAs.[231] Under the same Scheme of I4C, there is also Cyber Crime Research Center to carry out research on the issue related to cybercrime and enhance understanding on the emerging

[228] Online available at: <https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-March-2019/Comments/Nigeri> Accessed on 7 February 2022

[229] Nir Kshetri (2019) Cybercrime and Cybersecurity in Africa (n 196) 80; Premium Times, June 25, 2018, EFCC partners FBI to fight cybercrime, <https://www.premiumtimesng.com/news/more-news/273811-efcc-partners-fbi-to-fight-cyber-crime.html> Accessed on 23 January 2022

[230] Respondent from INSA reflect that even if Ethiopia do have cybercrime related cooperation agreement with few countries and with IGAD for having the capacity building support, but it needs significant work to be done since the country does not reach yet technological and legal cooperation and support agreement with regional and international organizations and international electronic and internet service providers.

[231] CyTrain website, Available at: <https://cytrain.ncrb.gov.in/local/staticpage/view.php?page=CyTrain> Accessed on 22 January 2022

technologies globally and to identify if they could be used negatively.[232] This would have considerable advantage for LEAs to use the emerging technologies that could be exploited by cybercriminals and develop investigative knowledge and skill. Hopefully, it would be a good trend for Ethiopia to adopt the best investigation mechanisms and establish a point of contact to keep communication with other country's LEAs to promptly obtain the required electronic evidence.

4.1.5 Lack of Awareness and Subtle Reporting Trend

Obviously, the police are considerably dependent on reports coming from victims of cybercrime in conducting investigations to detect and prosecute the criminals.[233] Hence reporting by victim users of computer related crimes or companies that trended system interference, breach of their clients' information etc. have great value in prevention of cybercrime. Low or lack of reporting has numerously affected detection, investigation and conviction of cybercrimes as there is lessen the probability of obtaining information on crime commission.[234] In turn, digital evidence will vanish as it doesn't collect in time before a perpetrator intervenes due to dearth of reporting.[235]

Providing awareness about cybercrime and cybercrime associated risks have an implication beyond making users responsive to reporting duty as it can determine effectiveness of cybercrime laws and its enforcement.[236] In Ethiopia, existing low awareness about cybercrime and negligence of some institutions to report attempts or commission of cybercrime have been counted among the reasons hampering the INSA's effort to tackle the problem.[237] Former Deputy General, Ifrah Ali, succinctly states that 'despite the growing trends of using technologies in the country, the awareness and capacity to prevent cyber-attacks is still poor; and this makes the situation even worse'.[238] To further this proposition the informant from FPC states that cybercrime reporting trend is not enough and stress that the very reason responsible for this is the lack of awareness

[232] Online Available at: <https://www.deccanchronicle.com/nation/current-affairs/250220/hyderabad-new-centre-to-fight-cyber-crimes.html> Accessed on 22 January 2022

[233] The respondents from FPC stated about the importance of reporting to put criminal justice system in effect.

[234] Ibid, on the implication that cybercrime reporting has on the process of detection, investigation and prosecution of cybercrime.

[235] Ibid

[236] See R. Abubakar, *et al,* 'Appraising Institutional Capacity for Implementation of the Nigerian Cybercrime Act 2015' (n 190)

[237] Ethiopian Monitor News, (n 199)

[238] Ezega News, Dec 6, 2019, Available at <https://www.ezega.com/News/NewsDetails/7518/INSA-Aborts-Cyber-Attacks-on-Financial-Institutions> Accessed on November 17, 2021

associated to unnoticed of whether the act has been criminalized or not. He added that the absence of crime communication is not due to ignorance of the attack rather it is due to unawareness of existing cybercrime law. Almost all respondents across INSA, FPC and MoJ agreed upon the fact that the fundamental reasons are fear of the consequence of publicity and lack of knowledge that individual users to understand whether they are under cyber-attack. These two facts are substantially preventing the reporting of cybercrime incident that expected from public/private organizations and individuals experiencing or have knowledge of the attack. Handful of respondents, on the other hand, convinced that organization are fail to report the cyber incidents they are experienced not because either they fear negative publicity or unawareness of the incident. Rather, it is because of nonexistence of mandatory reporting system in the country that expect such private and public organization to make reporting. Therefore, organizing comprehensive cybercrime incident reporting scheme has been highly recommended.

On this basis, the country needs to work to make the user aware of the crimes activities committed through online platforms or computer systems to take proactive measures and to report those incidents for further intervention by the police or information security intelligence. In this regard, we can cite the Nigerian trend in educating Nigerians about cybercrime that has been led by Paradigm Initiative Nigeria (PIN) to work in partnership with Microsoft on this issue.[239] The Nigerian Communications Commission (NCC) also mandated monthly national cyber security awareness which is carried out annually in order to create responsiveness towards providing the public with knowledge and safety of the use of the internet.[240] There is also a National Cyber Crime Reporting Portal (NCRP) that has been enable citizens to report cybercrime and other electronic crime like pornography, financial crimes and social media related crimes.[241] This portal would have been a point of contact for users of digital technology to get advice and help on how to report cyber incidents and how to get rid earlier/ being proactive, beside its importance of availing mechanism for reporting it may support reporting to be a trend. NCRB has also signed a MoU with National Centre for Missing and Exploited Children (NCMEC) USA, the organization which has

[239] Nir Kshetri (2019) Cybercrime and Cybersecurity in Africa (n 223), 80

[240] Online available at: <https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-March-2019/Comments/Nigeri>; <https://simplifiedupsc.in/i4c-indian-cyber-crime-coordination-centre/> Accessed on 7 February 2022

[241] Online available at: <https://www.drishtiias.com/daily-updates/daily-news-analysis/citizen-centric-services-of-ncrb> Accessed on 7 February 2022

centralized reporting system by which internet service providers across the world or intermediaries like Face book, YouTube, etc. can report about persons who circulate images of child pornography.[242] This could be a best example for Ethiopia to deal with the issue as we are nowadays experiencing epidemic of pornographic related materials, hate speech, false news and disinformation viral over the social media. Notwithstanding, requiring organizations to have security protection schemes in order to be cautious, able to defend integrity of its system and safety of clients using its service and observe obligation to report incidents is crucial. Beyond this reporting requirement, undertaking capacity building activities to equip institutions and its experts and employ necessary technological tools shall be taken indispensable to tackle the risk of cybercrime.

To conclude, the problem that has been observed from the perspective of LEAs and security intelligence coupled with low cybercrime reporting experience that might be associated with lack of knowledge about legal and regulatory regimes or lack of confidence in LEAs have been putting considerable hurdles in Ethiopian cybercrime prevention and control effort. In addition, cybercriminals have become more resourceful and powerful because, *inter alia*, their offenses often aren't reported and law enforcement agencies related obstacles let them prevail. Having in mind these difficulties, in the subsequent section the mechanisms deployed to repel cybercrime have been discussed.

4.2 Mechanism Used to Curtail Cybercrime in Ethiopia

In an effort to fight cybercrime and mitigate its effect, states have considered the need to adopt effective legal and regulatory frameworks. At present, cybercrimes have growingly been an international threat thus it has been believed that the best response is not unilateral domestic action, instead collective action taken under international legal framework may produce meaningful results in combating cybercrime of its transnational nature. The networked nature of modern communications in itself means that data will routinely be routed through a number of jurisdictions before reaching its destination, making tracing of communications extremely difficult and time sensitive.[243] Due to this legacy of internet technology, domestic effort could not effectively address the transnational character of such crimes. The same is true in legal enforcement mechanisms to

[242] Ibid

[243] ITU, 'Understanding cybercrime: phenomena, challenges and legal response' (n 69) 7

implement law, investigate or apprehend perpetrators in another state unless mutual understanding has been reached for the same effect. Therefore the attention of both government authorities and the international community has long been focused on finding efficient ways of legal harmonization and cooperation in combating criminal offenses committed through operation of information and communication systems.[244] Recent developments show there are measures such as adopting domestic cybercrime legislation, establishing law enforcement institutions, initiating awareness creation and capacity building programs and arranging public private partnership in combating cybercrime. Hereunder, discussion on the mechanisms used to tackle cybercrime in specific reference to Ethiopia would be conducted.

4.2.1 Cybercrime Legislation

Firstly, legal and regulatory measures should have to keep pace with digital evolution envisioned in Ethiopia to reverse the setbacks. Among the problems posed as a result of digital technology, cybercrime associated risks considering its socio-economic repercussions should be prioritized. In this respect, the strategy used to combat cybercrime – enacting law that directly dealt with the menace of cybercrime activity is necessary to survive from its devastating consequences (economic, social, political, psychological etc.). Most importantly, enacting a law to criminalize the abuses of ICTs and the internet and commit to harmonize at the international, regional and national levels is imperative to meet the transnational challenge it will pose. This is because legislation plays a crucial role in prevention and prohibition of cybercrime. Thus, legislation relevant to cybercrime may address a wide range of issues, including: criminalization of particular conduct; police investigative powers; issues of criminal jurisdiction; admissibility of electronic evidence; data protection responsibilities of electronic service providers; and mechanisms of international cooperation in criminal matters involving cybercrime.[245] In this context, looking at Ethiopia legislative structure reveals that it has computer crime proclamation embodied as many computer offenses criminalized and punished, procedural and evidence rules related to jurisdiction, investigation, collection of electronic evidence and establish the mandate to carry out international cooperation under MoJ. There is also hate speech and disinformation proclamation to avoid illegal traffic contents created and disseminated through computer systems or networks. These are

[244] Eurasian Group, 'Cybercrime and Money Laundering', (n 85) 6
[245] UNODC, 'Comprehensive Study on Cybercrime' (n 209) 53

cybercrime related laws under Ethiopian computer crime legal regime even it has to be review to regulate previously unaddressed criminal activities such as revenge pornography, blackmailing and email spam. In addition, hate speech proclamation should be reviewed to regulate the international internet and social media service providers and facilitate a means to work with such organizations to limit the effect unregulated social media activities may bring in the country's social, economic and political life.

4.2.2 Regulatory Measure

Undoubtedly, enacting cybercrime law is the most important step to tackle criminal activity but it has to be accompanied by effective law enforcement response. This is what makes law enforcement as important as enacting laws to prevent and control criminal activities, particularly in cybercrime cases. Broadly, law enforcement response constitutes an effective legal framework for investigative measures, access to investigative tools and techniques including means of obtaining electronic evidence from third parties, such as ISPs; and sufficient training and technical capabilities both for specialized and non-specialized officers.[246] Computers as it is used to commit criminal activity might also serve as venues of electronic evidence that implicate the commission of cybercrime. So that investigative authority (police and other relevant organs) should organize a cyber-specific unit as it would not be enough to consist of a few trained officers to effectively discharge its regulatory duty of securing and protecting the law.

Moreover, countries should commit to having adequate personnel and resources to strengthen their law enforcement capacity. Progressively, states to cope against the danger of cybercrime must improve the abilities of their LEAs to locate and identify criminals, collect and share evidence internationally as this may have a direct implication in a work to prevent and control repercussions of cybercrime. In this perspective, Ethiopia has law implementing institutions organized to undertake law enforcement activities such as detection, investigating, prosecuting and carrying out international cooperation. Accordingly, INSA is one of institutions devoted to ensure national information security, particularly to defend cyber-attacks, organize and administer a national computer emergency responding center and conduct forensic investigation (including online investigation system and provide necessary investigation techniques).[247] As well, INSA upon

[246] Ibid, 148

[247] Information Network Security Agency Re-establishment (INSA's proclamation) Proclamation No. 808/2013, enter into force 2 Jan 2014, see its preamble and art. 6 (4,6 & 8); Computer Crime Proclamation, Art 39.

reasonable suspicion that computer crime will be committed shall take appropriate measures to prevent and control the crime. These are, providing early warning to citizens, in collaboration with the investigatory organ and upon court warrant conduct sudden searches, digital forensic investigation, provide appropriate security equipment or take other similar measures to minimize the risks or for effectiveness of the investigation.[248] In addition, whenever necessary and requested, INSA provides technical support, conducts analysis on collected information, and provides evidence if necessary to support the cybercrime investigation process.[249]The Federal Police Commission has a Cyber unit that is organized to conduct computer crime investigation, collect and analyze digital forensic evidence in joint cooperation with public prosecutors.[250] Beyond joint cooperation to conduct computer crime investigation by public prosecutor and police, the law has imposed a duty to follow up enforcement of the provisions of the proclamation.[251] The Minister of Justice is another institution with the task to carry out international cooperation on matters related to computer crimes.[252] Regarding investigation and evidence collection process, MoJ will approve and decide in the absence of other means to evidence collection for the request of warranty for surveillance and interception to be submitted to the court.[253] Notwithstanding the above, the MoJ will decide and permit the investigator organ to carry out surveillance without court warranty if there is reason to believe the computer crime is or will be committed imminently, but must present its reason within 48 hours to the president of high court.[254] To accompany the activity of cybercrime prevention and control at the higher level the establishment of the National Executive Task Force that comprises the Minister of Justice, Federal Police Commission, and other relevant bodies.[255] Based on the information obtained from one of the respondents, so far we have a joint investigation task force that has been established by INSA and FPC to conduct investigation of computer crime in collaboration.

As mentioned above, the institutional structure established in Ethiopia to deal with cybercrime could be taken as an important aspect of the fight against the destructive nature of cybercrime.

[248] Computer Crime Proclamation, Art. 26 (1)
[249] INSA's proclamation, Art. 6(7); Computer Crime Proclamation, Art. 23(2)
[250] Ibid Art. 23(1)
[251] Ibid Art 38(1)
[252] Ibid Art. 42
[253] Ibid Art. 25 (2)
[254] Ibid Art. 25(3 & 4)
[255] Ibid Art. 41

Even though there are some lessons imparted from the best practice of other states to get effectiveness out of the legal enforcement mechanisms already operated in Ethiopia. In this regard, Indians have practices that enhance the states/Union Territory to have their LEAs with cyber intelligence, investigation and forensic units fully equipped and the knowledge required.[256] This has given India added opportunity in the ongoing effort of fighting cybercrime and its destructive effect. Thus, Ethiopia needs to readjust its law enforcement mechanism and let regional security apparatus have cybercrime specific units with all required equipment and knowledge to enforce cybercrime legislation. As this could offload the activities concentrated on the law enforcement institutions organized at the federal level to bring effectiveness and efficiency in the fight against cybercrime nationwide.

4.2.3 Education and Awareness Creation Measure

Education plays an important role in developing a culture of secure behaviors amongst users in the cyber domain.[257] To make the public aware of the danger of cybercrime might serve a double advantage; firstly, to make users aware of the risk of victimization and secondly, as a result of awareness tipped, they would be cautious in taking protective measures. Through this effort, users will be able to get tips about how to protect their computer and data from cyber-attack. And it will solve the underreporting problem of cybercrime, which in turn helps countries to know the level of its prevalence in order to take measures that fit the situation. Moreover, this program allows users to device protection techniques such as using the latest and up-to-date anti-virus, encryption technology, and anti-spy software etc., to complement the national effort in combat cybercrime. Inadequacy of awareness not only among the users but also in the government will deepen the challenges of cybercrime. Understanding this very fact, INSA has launch Cyber Security Month long awareness creation program for the year 2021 under the motto "Cyber Security Shared Responsibility, Let's Know & Be Cautious".[258] In addition, INSA has launch '*cyberigna/ሳይበርኛ*' TV program and create Facebook account (named as Information Network Security Agency -

[256] Online available at: <https://cytrain.ncrb.gov.in/local/staticpage/view.php?page=CyTrain> Accessed on 12 February 2022

[257] Muktar Bello, 'Investigating Cybercriminals in Nigeria: A Comparative Study' (n 194) 76

[258] Walta News, Oct 20, 2021, Available at <https://waltainfo.com/insa-urges-media-institutions-to-enhance-capacity-to-prevent-cyber-attack> Accessed on December 20, 2021

ኢመደኤ) to facilitate information sharing and awareness creation.[259] Basically, this is aimed to create awareness for individuals, governmental and private institutions as part of the effort to mitigate and control cyber-attacks. Even if it is not enough compared to the real challenge coming due to lack of awareness, it could be taken as initial fuel for a long journey that awaits the country in this regard. With regards to other organs authorized to ensure information security and when cybercrime has already committed; to detect, investigate and prosecute including NFIU, FPC and MoJ - they don't have awareness creation platforms or even TV programs at all.[260]

4.2.4 Initiate Public Private Partnership Scheme in Combating Cybercrime

Global electronic communication technology presents accessible and affordable high speed internet broadband that has resulted in the breakdown of national and transnational boundaries. Such advancement in international communication could challenge the government's effort to cripple cyberspace threats as all technologies have their own backside. As a result, the government needs a joint force that will boost its capability to curtail the consequences of cybercrime, thus, collaboration with private sectors becomes imperative in this respect. Therefore, public private partnership framework should be among the forefronts to pool the potentials. This is, for one thing private organizations themselves are vulnerable and in search of strong security partners, the government on the other hand needs technical capacity to counter cyber incidents, therefore, joining hands to counter cyber threat certainly serves both. To speak of the experience in India, the I4C Schemes has among its mission to organize partnership with research institutes, private sectors and inter-governmental organizations within India and abroad to undertake research on needs of LEAs and adoption of new technologies and forensic tools.[261] Basically, this will serve as a forum for public and private sector collaboration in the work of fighting against cybercrime.

---

[259] Informant from INSA has indicate that this TV program has been providing digital technologies related information and knowledge, specifically illegal activities committed through ICT infrastructure and internet against information security and computer systems. SMS text has also been sent in collaboration with Ethio Telecom but its aim has short effect and seasonalthat is only to inform electronic device users to take necessary precaution while the information system falls under attack. However, he concluded such move yet has to be improved and upgraded to reach significant users of electronic transaction and uncover the complicated nature of cybercrime. At the same time, INSA must facilitate training and education program to train and continuously update law enforcement personnel.

[260] Those informants participate from FPC and MoJ state that their institutions have not yet built awareness creation program to provide end users and law enforcement personnel with basic knowledge of cybercrime and related electronic crime.

[261] Available online at: <https://www.mha.gov.in/division_of_mha/cyber-and-information-security-cis division/Details-about-Indian-Cybercrime-Coordination-Centre-I4C-Scheme> Accessed on February 2, 2022

Chapter Five

Conclusion and Recommendation

5.1 Conclusion

Introduction and development of ICTs have facilitated the communication to be made easily and instantly from anywhere across the world. Accessing information and knowledge from the internet and websites at an affordable cost within a fraction of minutes has been possible due to this technological advancement. Specifically, individuals, organizations and governments are truly benefited from the advancement of ICTs and the internet as it provides an online venue to store large size data in small and portable storage and retrieve valuable information, automate transactions for the sake of accelerated services and online marketplace for buyers or sellers. Besides these and other numerous advantages computer and information technologies have brought, there have been risks that such development comes with and one of them has been named *'cybercrime*'. In this sense, benefits are not the only things that come from the proliferation of information technologies and computer systems, there would also be losses (be economic, psycho-social or technological in nature) associated with its backside. Such devastating consequences shall need legal and technical interventions.

As stated, countries have yet lost economically, psycho-socially and technologically, even if they have taken legislative and technical measures to prevent cybercrime. In fact, Ethiopia is not an exception to this fact; the country has been hit repeatedly; especially, in recent years, hacking has become rampant. Epidemic fake news, hate speech and disinformation produced and disseminated through social media platforms are causing political instability, economic unrest against the country's interest and ensuing loss of life, bodily injuries and discrediting individual reputation and interest. Moreover, youths can access without limit illegitimate websites those to produce and disseminate indecent articles and pornography contented data and they exposed for early sexuality and deviant to social norms as ramification of internet in the country is high. Considering these realities, one can admit the fact that Ethiopia has its share from the problems posed by cybercrimes. Thus, a strong criminal justice response to this specific case has therefore been required to effectively reverse its effect. This includes measures on investigation, prosecution, and

adjudicating offenses committed against and via computer systems, as well as to safeguard electronic evidence used to be a proof in connection to any crime generally.

Ethiopia has taken fundamental moves in terms of legislative and regulatory measures as it enacted cyber specific legislation, set up institutions to enforce cybercrime laws and monitor information security of the country. Computer crime proclamation has been one of the comprehensive laws in this respect that criminalizes a range of cyber or computer offenses, and sets forth procedural and evidence rules. Even if this proclamation has indispensably to the fight against cybercrimes and criminalizes ample of offenses, there are illegal activities committed through internet and computer systems those left uncovered including email spam, revenge pornography, and online blackmailing. At this junction, there should be review of the existing laws to embody such offenses and criminalize its occurrence. In addition, cyber criminality has been mounting over the years as reports released against Ethiopia from outside sources. Given this global nature of cybercrime and, in particular, volatility of electronic evidence, protecting a country's cyberspace also necessitates effective international collaboration. Therefore, the country is supposed to join international and regional instruments and cooperation frameworks to prevent and control transnational cybercrime cases.

5.2 Recommendation

Looking at the alarmingly increasing cybercrime risks in Ethiopia, there has been a need to make timely review of existing (legislative and regulatory) approaches and establish an institution that can comprehensively and collaboratively lead the fight against cybercrime. Thereby, the followings are recommended;

- Global internet system has provided plenty of instances of electronic technology users being deceived by email scamming. Again, proliferation of Internet technologies has used to produce and disseminate pornographic related websites, magazines, photos, pictures and advertise sexual recruitment against public morality and well-being. Therefore, the Government of Ethiopia should regulate (at least by criminalizing the acts) the issue of email scam or phishing and adult pornography, dissemination of sexual articles and revenge pornographic activities that has not addressed properly by the existing computer crime proclamation (958/2016) by enacting specific law.

- Cybercriminals have used the borderless nature of cybercrime to commit cyber-attack from elsewhere against the national information system. The mechanism to deal with such transnational crime is strengthening international cooperation and collaboration with countries, regional and international organizations. Likewise, Ethiopia should make technological assistance understanding with private industry like software corporations, international ISPs, and to be part of international and regional cooperation frameworks for joint work.

- ISPs such as hotels, educational institutions, other private and public institutions and internet cafes must operate under legal guidelines that stipulate some sort of obligation that impel them to take responsibility in keeping their systems and networks. Specifically, the guideline rules that need information technology intermediaries to guarantee monitoring and control users joining their systems or networks from being involved in illegal activities. Mostly, such networks become hotspots of cybercrime as they find weaker access points to navigate illegal traffic data, to disseminate hate speech, fake news, computer viruses, and to hack passwords and financial information. Therefore, to curb this problem Ethiopia should enact rules that regulate the information technology intermediaries and ISPs to make them proactive and go beyond just reporting the crimes, but human rights issues should be taken seriously.

- Ethiopia needs to establish a cybercrime center. That can facilitate relevant information and technology sharing, organize forensic laboratory centers and conduct research and development, and become links for inter-sectoral collaboration and international cooperation. Which can also design and incorporate cybercrime and related programs to produce skilled and knowledgeable legal and technology experts.

- Lastly, along this centralized institution recommended above, establishing forensic lab centers at least in every region to improve the effectiveness and quality of fight against cybercrime is required since a single forensic investigation at the Federal Police Commission (FPC) is not sufficient.

BIBLIOGRAPHY

- **Primary sources**

- African Union Convention on Cyber Security and Personal Data Protection, Adopted by the 23rd Ordinary Session of the Assembly of the Union, Malabo, 27th June 2014.
- Council of European Convention on Cybercrime, ETS No. 185, Enter Into Force 1 July 2001.
- Council of Europe, Additional Protocol to the Convention on Cybercrime, Concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems, 28 January 2003
- Federal Democratic Republic of Ethiopia, Vital Events Registration and National Identity Card Proclamation (amendment) Proclamation No.1049/2017, entered into force August 7, 2017
- Federal Democratic Republic of Ethiopia, Computer Crime Proclamation No.958/2016, entered into force in July 2016.
- Federal Democratic Republic of Ethiopia, 'National Information Security Policy', Information Network Security Agency (2011)
- FDRE Money Laundering and Terrorism Financing Proclamation No. 780/2013, entered into force February 4, 2013
- FDRE Criminal Code Proclamation No. 414/2004, entered into force May 9, 2005.
- Hate Speech and Disinformation Prevention and Suppression Proclamation No. 1185/2020, entered into force 23 March, 2020.
- India Information Technology (Intermediaries Guidelines and Digital Media Ethics Code) Rules, 2021, Amending Rules, 2011.
- India Information Technology (Guidelines for Cyber Cafe) Rules, 2011

- Nigerian Advance Fee Fraud and Other Fraud Related Offence Act 2006 as amended, enter into force 5th June, 2006
- Nigerian Cybercrimes (Prohibition and Prevention) Act, 2015, enacted into law on May 15, 2015
- Nigerian Economic and Financial Crimes Commission (Establishment) Act 2004
- The Information Technology Act 2008 (as amended) of India

- **Secondary Sources**

A. Books

- Clough, Jonathan 'Principles Of Cybercrime' (Cambridge University Press 2010)
- ITU Global Cybersecurity Agenda (GCA), 'Framework for International Cooperation in Cybersecurity', Available at <www.itu/cybersecurity/gca/>
- Richards, James R., Transnational Criminal Organizations, Cybercrime and Money Laundering, A Handbook for Law Enforcement Officers (published in 1999)
- The ITU, 'Understanding cybercrime: phenomena, challenges and legal response' (published, 2012) available at: <www.itu.int/ITU-D/cyb/cybersecurity/legislation.html>
- UNODC 'Comprehensive Study on Cybercrime' (February 2013)
- World Bank and United Nations, Combating Cybercrime: Tools and Capacity Building for Emerging Economies, Washington, DC 2017

B. Journal Articles

- Abraha, Halefom, THE STATE OF CYBERCRIME GOVERNANCE IN ETHIOPIA (2015) <https://www.researchgate.net/publication/322234805>

- Abubakar, R. et al, ‘Appraising Institutional Capacity for Implementation of the Nigerian Cybercrime Act 2015’ (2017), Vol. 2, Proceedings on Big Data Analytics & Innovation (Peer-Reviewed)

- Asmare, Molalign, ‘Computer Crimes in Ethiopia: An Appraisal of the Legal Framework’ 2015 Vol. 3, Issue 1, International Journal of Social Science and Humanities Research;

- Awhefeada, Ufuoma V. & Ogechi, Ohwomeregwa ‘Appraising the Laws Governing the Control of Cybercrime in Nigeria’ (2020), Vol. 8 No. 1, Journal of Law and Criminal Justice;

- Basu, Subhajit and Jones, Richard, 'Indian Information and Technology Act 2000: review of the Regulatory Powers under the Act', (2005), Vol.9 No.2, International Review of Law, Computers & Technology;

- Eurasian Group on Combating Money Laundering and Financing of Terrorism ‘Cybercrime and Money Laundering’ (2014);

- Gagliardone, I and Golooba-Mutebi, F (2016), the Evolution of the Internet in Ethiopia and Rwanda: Towards a “Developmental” Model? Stability: Vol 5. Issue 1, International Journal of Security & Development;

- Gandhi, V. Karamchand ‘An Overview Study on Cybercrimes in Internet’ (2012), Vol 2, No.1, Journal of Information Engineering and Applications;

- Kandpal, Vineet and Singh, R. K. ‘Latest Face of Cybercrime and Its Prevention in India’ (2013), Vol. 2. No. 4, International Journal of Basic and Applied Sciences;

- Karali, Y. et al, ‘Cyber Crime: An Analytical Study of Cyber Crime Cases at the Most Vulnerable States and Cities in India.’ (2015), Vol. 5 Issue. 2, International Journal of Engineering and Management Research;

- Kshetri, Nir. ‘India's Cybersecurity Landscape: The Roles of the Private Sector and Public-Private Partnership’ (2015), IEEE Security and Privacy Magazine;

- Longe O. B, 'Internet Service Providers and Cybercrime in Nigeria –Balancing Services and ICT Development'

- Mohammed, Kabiru H. et al, Cybercrime and Digital Forensics: 'Bridging the gap in Legislation, Investigation and Prosecution of Cybercrime in Nigeria' (2019), Vol. 2 Issue 1, International Journal of Cybersecurity Intelligence & Cybercrime;

- Prasad, Arun B. 'Cyber Crime in India: Time Series Study of State Level data' (2017), Manakin Press;

- S. Adesina, Olubukola 'Cybercrime and Poverty in Nigeria' (2017) Vol. 13, No. 4, Canadian Social Science;

- Vineet Kandpal and R. K. Singh, 'Latest Face of Cybercrime and Its Prevention in India' (2013), Vol. 2. No. 4, International Journal of Basic and Applied Sciences;

- Woldehanna, Frehiwot et al, Legal Framework for Implementation of m-Government in Ethiopia: Best Practices and Lessons Learnt (2014), Vol. 32 Journal of EEA;

- Yilma, Kinfe Micheal, 'Some Remarks on Ethiopia's: New Cybercrime Legislation' 2016, Vol. 10, No.2 Mizan Law Review, available at <http://dx.doi.org/10.4314/mlr.v10i2.7>

- Yilma, Kinfe Micheal and Abraha, Halefom Hailu on their article titled 'The Internet and Regulatory Responses in Ethiopia: Telecoms, Cybercrimes, Privacy, E-commerce, and the New Media', available at <http://dx.doi.org/10.4314/mlr.v9i1.4>

C. Unpublished Thesis

- Berhanu, Abenezer 'Developing National Cybersecurity Strategy For Ethiopia' (Master thesis, Tallinn University, 2019). Mebrate, Yohannes 'E-Commerce And The Future Of Competition Regulation Under Ethiopian Law' (LLM thesis, Debre Berhan University, 2020);

- Getaneh, Tewodros 'Cyber Security Practice and Challenges at Selected Infrastructures in Ethiopia: Towards Tailoring Cyber Security Framework', (Master thesis, AAU, 2018).

- Teketel, Iyasu, Cybercrime in Ethiopia: 'Lessons to be learned from International and Regional Experiences' (LLM Thesis, AAU 2018);

- Usman, Mahboob 'Cyber Crimes: A Case Study Of Legislation In Pakistan In The Light Of Other Jurisdictions' (LLM Thesis, International Islamic University Islamabad, 2015);

- Uzor, Eze Kenneth 'A Review of The Problems In Regulating The Internet Use: Enforcement Mechanisms Against Cybercrimes Under International Law', (Phd Thesis, Nnamdi Azikiwe University, 2016)

D. Websites Report and Blogs

- African Center for Strategic Studies, Available at <https://africacenter.org/spotlight/africa-evolving-cyber-threats> Accessed Nov 21, 2021;

- Available at <https://chilot.me/2021/07/06/electronic-procurement-to-be-operational-from-july-7/amp/> Accessed on July 20, 2021;

- Available at <https://www.ericsson.com/en/press-releases/1/2021ethi-telecom-and-ericsson-launch-4g-network-for-south-west-ethiopia-at-major-event-in-jimma> accessed July 20, 2021

- Available at <https://www.hindustantimes.com/india-news/cyber-crimes-registred-11-8-increase-last-year-ncrb-101631731021285.html> Accessed on November 3, 2021;

- Available at <https://www.moneycontrol.com/news/india/heres-the-reason-behind-60-of-the-cyber-crimes-committed-in-2020-7489071.html> Accessed on November 3, 2021;

- BBC News, Available at <https://www.bbc.com/news/world-africa-49759392>, Accessed on Nov 25, 2021;

- Enact Observer Report, Available at <https://enactafrica.org/enact-observer/nigerias-financial-institutions-vulnerability-to-cybercrime> Accessed on October 26, 2021

- Ethiopian Monitor, Available at <https://ethiopianmonitor.com/2020/04/ethio-telecom-launches-lte-advanced-mobile-service/> Accessed on July 20, 2021;

- Ezega News, Available at <https://www.ezega.com/News/NewsDetail/6913/Ethiopia-to-Increase-Internet-Gateway-Capacity> Accessed on July 20, 2021;
- Fight The New Drug, 'Porn Tube Sites Are Free, So How Does The Porn Industry Make Money Today? Available at <https://fightthenewdrug.org/how-does-the-porn-industry-actually-make-money-today/> Accessed on October 12, 2021;
- IMB Report, Available at <https://www.dbta.com/Editorial.News-Fleshes/IBM-2020-Cost-of-DataBreach-Study-True-Cost-of-Todays-Security-Glitches-142198.aspx>, Accessed on July 18, 2021;
- SciDevNet, 'Cybercrime in Africa: Facts and Figures' Available at <https://www.scidev.net/sub-saharan-african/features/cybercrime-africa-facts-features/> Accessed on October 26, 2021;
- Statista Report, <https://www.statista.com/statistics/617136/digital-population-worldwide/> accessed on July 17, 2021;
- The Cable, Available at <https://www.thecable.ng/nigeria-ranked-16th-in-fbi-global-cyberime-victims-report/amp> Accessed on October 26, 2021;
- The Guardian Report, Available at <https://guardia.ng/news/is-nigeria-really-the-headquarters-of-cybercrime-in-the-world/> Accessed on October 26, 2021;
- U.S News, available at <https://www.usnews.com/news/best-countries/articles/2016-07-28/meet-the-yahoo-boys-nigerias-undergraduate-conmen> Accessed July 24, 2021;
- Walta News, available at <https://waltainfo.com/ethiopia-encounters-2,800-cyber-attack-attempts/> Accessed on December 2021

APPENDIX

Jimma University
College of Law and Governance

School of Law

I am Zelalem Tadesse Student of Jimma University College of Law and Governance, as I am doing my LL.M Thesis for the partial fulfillment of the program titled *"**Examining the legislative and regulatory responses to the evolving cyber criminality in Ethiopia: Enforcement Challenges and Lesson for Ethiopia".*** I hereby prepare the following semi-structured questionnaires to have your expert opinion and relevant information on the role that your institution plays in the effort to tackle cybercrime and challenges that are facing in the process.

Questionnaires Guides

Respondents Private Information

- **Name (if interested) - _____**
- **Position - _____**

Type of Study – A Master's Thesis in Law (LL.M Thesis)

Title - ***'Examining the Legislative and Regulatory Responses to the Evolving Cyber Criminality in Ethiopian: Enforcement Challenges and Lesson for Ethiopia'***

Objective of Questionnaires – based on the relevant information obtained for the participants from the selected institutions to conduct an assessment on the legislative frameworks, regulatory capacity and practical challenges that face the effort to prevent the evolving cybercrimes. Your expertise, opinion and relevant information have an irreplaceable role to identify the practical challenges, to recommend way outs and contribute for the study to be accomplished in best quality and integrity. Therefore, I kindly ask you to respond to the questions put in your attention to the utmost since it is an invaluable asset to the output of the study. I duly acknowledge that the anonymity and confidentiality of personal view has been kept in this study otherwise the respondent consented to it.

For your indispensable cooperation the researcher is immensely grateful!

Notice: for the question put in a choice you kindly asked to use 'X' sign

1. In your personal and expertise view which challenges are encountered in the effort to prevent cybercrime and cyber criminality in Ethiopia?
    - Incompatibility of legal framework with the ever-evolving cybercrime (in terms of its type and magnitude of harm) in Ethiopia? Yes _____ No_____
    - Structural/organizational failure to be well equipped in human capital, technology and investigation techniques and tools? Yes _____ No_____
    - Absence or inadequacy of legal cooperation agreement with countries and international electronic service providers? Yes_____ No_____
    - If there are other challenges other than these, please mention it?
    - From your expertise viewpoint and the information that you get from your position in your institution what the solution would be?
2. From your expertise, knowledge and assessment does the Ethiopia cybercrime legal framework compatible with the increasingly grown cybercrime and cyber criminality? If your answer is yes, how?
    - If no, what kept it behind, please let us know your reason because it is helpful for the study?
3. As you are closely working on one of the areas related to cybercrime, what is your knowledge on Ethiopia having the cybercrime cooperation framework with the countries? If there are such legal cooperation frameworks that Ethiopia is a part of, please mention it?
    - Does the existing cybercrime cooperation legal framework help to subvert the cross-border cybercrime attack that has occurred within Ethiopia territory or to conduct joint investigation with other country's law enforcement agencies? Does this agreement have an effect to prevent or cooperate, please if you have information help us to know with the specific case?
    - Effective cybercrime or computer crime prevention processes will help prompt collection of electronic evidence and information before the cybercriminal gets to remove or delete from the platform. In this context, does Ethiopia have a legal framework that supports collection of electronic evidence and preserve its integrity or enable it to conduct joint investigation? What is your assessment on the question; does Ethiopia have an institution duly and suitably execute such a task?
    - If you believe that Ethiopia is not a party to a single bilateral or multilateral cybercrime cooperation framework/instrument that has been introduced to harmonized national

cybercrime legislations, to create and promote international cooperation on the area, would this have negative implication on the country's effort to combat cybercrime?

4. Ethiopia's national effort to expand internet, computer technology and telecom services to digitize the country have immense importance to integrate the country into the international economy, technological advancement, social development, etc. However, at the same time the introduction and development of computerization has its own setbacks and, in this regard, cybercrime is typical.

- Can we say that the institutions established to prevent, detect and investigate increasingly growing cybercrime (including your institution) are well organized and equipped in accordance with the requirements listed here below?
    A. In terms of human capital (experts with technological knowledge & technique skill)?
    B. In terms of scientific technology and investigation techniques?
    C. With continued and timely capacity building training scheme?
- If you think it has been organized adequately, please share your opinion in the most important detail?
- If you are not pleased with your institution organization in terms of the aforementioned standard, what do you think as an expert has to be done for improvement?

5. In your institution would you believe that information technology experts, technology and training facilities have organized adequately to produce competent, experienced and as much required experts to be proactive in the fight or detect and investigate cybercrimes if it happened?

- If the above conditions are not properly fulfilled, would this bring negative implications in the effort to prevent cybercrime? Please share your opinion specifically in your institution.

6. Among the computer offenses or cybercrime often trended such as dissemination of computer virus, computer fraud, DoS, illegal interference, illegal interception, hacking, child pornography etc. Which of these are often and widespread in Ethiopia? If the data in your institution shows otherwise, please tell us which.

7. How do you describe the cyber reporting trend in Ethiopia? Do public or private institutions and individual users have the trend of reporting the cyber-attack they are experiencing or have knowledge of the commission to the law enforcement institutions? If its rate is low based on the inference in your institution what would be the cause?

Would it be?

- Fear of the consequence of publicity? Yes _____ No _____
- Lack of knowledge whether they are under cyber-attack or not? Yes___ No_____
- Please mention it if there are other reasons that keep victims from reporting?

8. Institutions that have been established to protect information security and to prevent computer crime or cybercrime, do they have an awareness creation scheme to educate and inform end users of electronic technology about the cybercrimes that have been committed through internet and computer technology? If your answer is yes, which institution is it? Just mention it.

- How would you assess your institution in this specific respect?
- What mechanism has been used to create awareness on the issue?
- Do you think that various technologies used by cybercriminals to go anonymous and make detection and investigation processes more complicated and difficult have a nexus with the low cyber incident reporting trend in Ethiopia? How?

9. Does Ethiopia have a system of public private partnership on the matter related to cybercrime and cyber security that would enable the joint work with private sectors to acquire specialized knowledge on information security and protective technology? Yes_____ No_____

- If your answer is in affirmation, please tell us the detailed information you have on this issue?

10. Anything you thought relevant and would be an additional input for this study please share with us your view and information.

The researcher is grateful for your time and kindly cooperation!