2022-10

Effective Investigation and Prevention of Cyber Crime in Ethiopia: Assessment of the Legal and Practical Challenges

Seifu, Tinsae

“ከዓባይ ጓዳ ጥበብ ሲቀዳ”

Wisdom at the source of Blue Nile

EFFECTIVE INVESTIGATION AND PREVENTION OF CYBER CRIME IN ETHIOPIA: ASSESSMENT OF THE LEGAL AND PRACTICAL CHALLENGES

By

TINSAE SEIFU ALEMAYEHU (LLB)

School of Law

Bahir Dar University

October, 2022

EFFECTIVE INVESTIGATION AND PREVENTION OF CYBER CRIME IN ETHIOPIA: ASSESSMENT OF THE LEGAL AND PRACTICAL CHALLENGES

Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of Master of Laws (LLM) in Criminal Justice and Human Rights law at the School of Law, Bahir Dar University

By:

Tinsae Seifu Alemayehu (LLB)

Advisor:

Worku Yaze Wodaje (Asst. Prof, Ph.D. Candidate)

School of Law

Bahir Dar University

October, 2022

Thesis Approval Page

This thesis titled "*Effective Investigation and Prevention of Cyber Crime in Ethiopia: Assessment on the Legal and Practical challenges*" by Tinsae Seifu Alemayehu is approved for the degree of masters of laws (LL.M)

As a member of the board of examiners of LL.M thesis oral defense examination, we certify that we have read and evaluated the thesis prepared by Tinsae Seifu Alemayehu and examined the candidate. We recommended that the thesis be accepted as fulfilling the thesis requirement for the degree of masters of laws (LL.M).

Board of Examiners

Name Signature

Advisor ____________________ _______________

Chairperson ____________________ _______________

Internal examiner ____________________ _______________

External examiner ____________________ _______________

Date ____________

Declaration page

I, Tinsae Seifu Alemayehu, hereby declare that the work contained in this thesis is my own original work and that I have not previously in its entirety or in part submitted it at any University for a degree. I have duly acknowledged and referenced all the materials used in this paper. I understand that non-adherence to the principles of academic honesty and integrity, misrepresentation of any idea, facts, data, and other sources will constitute sufficient ground for disciplinary measure by the university and can also evoke criminal sanction from the state and civil action from the author of a source which has not been properly acknowledged or cited.

Signature

Name of the student

Tinsae Seifu Alemayehu

University ID. Number

BDU-1301647

Date

October 31, 2022

Acknowledgments

Before words of gratitude are extended to your creatures, The Father, The Son and The Holy Spirit (Lord God Almighty) the fountain of all powers, the owner of the visible and the invisible, thank you for showering me with the strength to cope this work.

First and for most, I would like to express my deepest and sincere gratitude to my advisor Worku Yaze (Asst. Prof, Ph.D. Candidate) for your unreserved and priceless advice, encouragement and prompt response to my questions. Had it not been for your contribution, this paper would have not been successfully accomplished. Honestly, it was such a privilege to be under your guidance, I just want to say, Thank you beyond thanks in advance.

I would also like to thank my research participants for their helpful cooperation and collaboration in handing over all necessary piece information at their disposal without any suspicion and hesitation upon data collection. I am indebted to your kindness.

Last but not least, my family members, Bahir Dar University School of Law staff members and my friends, I am very grateful for your direct or indirect support in academic reference materials and financial support. I am thankful for your contribution.

Contents

Declaration page iii

Acknowledgments iv

List of Abbreviations/ Acronyms viii

Abstract.. x

CHAPTER ONE 1

INTRODUCTION 1

1.1. Background of the Study 1

1.2. Statement of the Problem 5

1.3. Objectives of the Study 8

1.3.1. General Objective 8

1.3.2. Specific Objectives 8

1.4. Research Questions 9

1.4.1. General Research Question 9

1.4.2. Specific Research Questions 9

1.5. Significance of the Study 9

1.6. Research Methodology 10

1.6.1. Research Method 10

1.6.2. Type and Sources of Data 11

1.6.3. Data Collection Methods or Tools 11

1.6.4. Sampling Techniques 12

1.6.5. Data Analysis 13

1.7. Review of Related Literatures 13

1.8. Scope of the Study 17

1.9. Limitation of the Study 17

1.10. Ethical Considerations 18

1.11. Organization of the Study 18

CHAPTER TWO 20

THEORETICAL, LEGAL AND INSTITUTIONAL FRAMEWORKS FOR THE INVESTIGATION AND PREVENTION OF CYBER CRIME 20

2.1. Theoretical and Conceptual Framework of Cyber Crime 20

2.1.1. Conceptualizing Cyber Crime........ 20

2.1.2. Taxonomy of Cyber Crime 23

2.1.3. Extent and Impact of Cyber Crime 27

2.2. International and National Legal Framework of Cyber Crime 29

2.2.1. International Legal Framework........ 30

2.2.2. Regional Legal Framework........ 33

2.2.2.1. The Council of Europe Convention on Cybercrime (Budapest convention)........ 33

2.2.2.2. African Union Convention on Cyber Security and Personal Data Protection (Malabo convention)........ 35

2.2.3. The Legal and Policy Framework of Cyber Crime in Ethiopia........ 38

2.2.3.1. The Policy Framework........ 38

2.2.3.2. The Legal Framework........ 38

2.3. Institutional Setup........ 43

2.3.1. Information Network and Security Administration 43

2.3.2. National Intelligence and Security Service........ 44

2.3.3. Ministry of Justice: Attorney General........ 45

2.3.4. Federal Police Commission: Federal Crimes Investigation Office........ 47

2.3.5. Other Concerned Institutions 48

CHAPTER THREE: 50

LEGAL AND PRACTICAL CHALLENGES TO THE EFFECTIVE PREVENTION AND INVESTIGATION OF CYBER CRIME - FINDINGS AND DISCUSSIONS.................... 50

INTRODUCTION 50

3.1. Legal Challenges 50

3.1.1. Ambiguities on the Definition of "Computer Crime"... 50

3.1.2. Lack of Sufficient Coverage of Crimes 51

3.1.3. Inadequacy of Laws on Filtering and Blocking mechanisms 53

3.1.4. Failure to be Part of International Legal Initiatives 54

3.2. Practical Challenges 55

3.2.1. Limited Abilities of Law Enforcement Officials 55

3.2.2. Lack of Strong Institutional Cooperation 58

3.2.3. Confusion on the Investigative Power 60

3.2.4. Lack of Adequate Investigative Tools and Equipment.. 62

3.2.5. Shortage of Man Power and Brain Drain.. 63

CHAPTER FOUR:.. 67

CONCLUSION AND RECOMMENDATIONS 67

4.1. CONCLUSION 67

4.2. RECOMMENDATIONS 70

4.2.1. Concerning Computer Crime Proclamation.. 70

4.2.2. Concerning Cooperation and Collaborations.. 70

4.2.3. Concerning Cyber Crime Investigating Organs.. 71

4.2.4. Regarding Law Enforcement Authorities and other Technical Issues........................... 71

Bibliography 73

Annex…... 84

List of Abbreviations/ Acronyms

AG	Attorney General
ATM	Automated Teller Machine
AU	African Union
CCP	Computer Crime Proclamation
CCID	Cyber Crime Investigation Division
CoE	Council of Europe
DCPEC	Draft Criminal Procedure and Evidence Code
EAC	East African Countries
Ethio-CERRT-	Ethiopian Cyber Emergency Readiness and Response Team
EU	European Union
ICT	Information and Communication Technology
INSA	Information Network Security Administration
IPR	Intellectual Property Rights
FAG	Federal Attorney General
FCIO	Federal Crime Investigation Office
FDRE	Federal Democratic Republic of Ethiopia
FIC	Financial Intelligence Center
FHC	Federal High Court
FHC	Federal High Court
FPC	Federal Police Commission

MFA	Ministry of Foreign Affairs
MIT	Ministry of Innovation Technology
MLA	Mutual Legal Assistance
NISS	National Intelligence and Security Service
NGO	Non Governmental Organization
PM	Prime Minister
SIT	Special Investigation Techniques
USA	United States of America
UN	United Nations
UNGA	United Nations General Assembly
UNODC	United Nations Office for Drugs and Crime

Abstract

Cyber crime is one of the most serious challenges confronting the global community, affecting socio-political and economic as well as security aspects worldwide. Its evolving, trans-national and complex nature has made it difficult to comprehend its meaning, nature, characteristics, and type. Because of these factors, prevention and investigation of cyber crime is not an easy task for law enforcement authorities worldwide. In Ethiopia, there is also a high level of computer crimes from in and out-side of the country and law enforcement authorities face hindrances in effectively investigating and preventing its commission, as well as achieve legislative goals.

In this context, the study first aims to identify and examine the legal and practical challenges impeding the effectiveness of investigation and prevention of cyber crime in Ethiopia. The study also tries to assess the legal framework and the practice of cyber crime investigation and prevention in Ethiopia. To that end, the study used qualitative empirical and doctrinal research methodology. Most importantly, data was gathered through in-person interviews and questionnaires.

The thesis discovered that cyber crime investigation and prevention is hampered by a number of legal and practical as well as institutional difficulties. These gaps or difficulties includes: Inadequate coverage of crimes, and laws on filtering and blocking mechanisms; Failure to be part of international legal initiatives; Limited capacity of law enforcements authorities; and, Absence of well-built inter-institutional collaboration; as well as insufficiency of up-to-date investigative tools and equipment. After all, the researcher concludes that the existing substantial loopholes in laws and technical and institutional encumbrances highly hampered the efficacy of cyber crime investigation and prevention in Ethiopia.

Keywords: *Cyber crime, Investigation and Prevention, Computer Crime Proclamation, Law Enforcement Authorities, Ethiopia.*

CHAPTER ONE

INTRODUCTION

1.1. Background of the Study

Our world is very dynamic. One of the areas still evolving in this dynamics is the technological advancements throughout the world. The land mark invention that changed human history is the invention of electronic digital computer in 1940's.[1] Since then computer and computing system has been developed in various ways by which its impact shown up in countless ways. Despite their unspeakable positive accomplishments, computer or digital technology creates new and sophisticated problems.[2] In its infant stages, the problems were not of a great concern and mostly perpetrated by misbehaving workers or individuals. Technological advancements creates an opportunities for criminals to easily commit more severe and complex crimes.

The innovation of computer and digital system in the early 1940's is not a separate history with the development of ICT. Thanks to ICT, we became more connected than ever. Internet, the engine in ICT, has become an essential element of modern life for billions of people globally. According to a recent study, the number of internet users stood at 4.9 billion internationally.[3] Among these users, persons within the age of 25-34 are the highest in number of internet users with 62.5% global penetration rate.[4] The number of fixed broadband has reached 1.3 billion within which the mobile subscription is 83.2 per 100 inhabitants.[5] This shows the dramatic advancement and expansion of cyber-related technology and the omnipresent nature of cyber space all round the globe.

The high rate of development in the cyber space is also witnessed in the African continent. Africa shares 11.5% of world's internet users following Asia and Europe respectively.[6] Internet

[1] Johannes Xingan Li, 'Cyber Crime and Legal Countermeasures: A Historical Analysis', *International Journal of Criminal Justice Sciences,* 2017, Vol. 12, PP. 196-207, P. 196 [Hereinafter: Johannes, Cyber Crime and Legal Countermeasures]

[2] Ibid

[3] Internet usage worldwide – statistics and facts, at https://www.statista.com/topics/1145/internet-usage-worldwide/ [last accessed at 24/3/2022]

[4] Ibid

[5] Ibid

[6] Internet world stats: usage and population statistics; at https://www.intrnetworldstats.com/stats1.htm [last accessed at 24/3/2022]

penetration is rapidly growing in Africa more than any other regions and it grew 6.5% in 2000 to 43% in 2021.[7] Ethiopia has, also, registered around 24 million internet users with 20.6% penetration rate.[8] All of these facts reflect the fact that we are in the middle of information technology revolution that is advancing and changing our ways of organizing, living, working and even dying.

With this high level of ICT revolution across the globe, the international community connected as it lives in a village. However, cyber space brings both great promises and safe environment for criminals. Nowadays, cyber crime reached high level of security concern in every country. According to one study, the cost of cyber crime annually estimated to be 10.5 billion dollar by 2025. Most of these attack are financially motivated, espionage, and property and identity theft.[9] Surprisingly, cyber crime has become 5 times more profitable than global transnational crimes combined.[10] In addition, these criminals attack or hit the target in a very sophisticated ways through circumventing computer defence mechanisms.[11] Due to this fact, it takes 207 days on average to identify a given cyber security breach.[12]

Africa, as a continent that has the fastest growing telephone and internet networks in the world, is also highly exposed to major cyber risks. As per Interpol's' report, the top five cyber threats in Africa are online scams, digital extortion, business email compromise, ransom ware and botnets.[13] Ethiopia is not an exception to this fact. And, there are several cyber attacks against both governmental and non-governmental institutions.[14]

In early times, computer-related crimes were investigated on the basis of traditional investigatory framework by which law enforcement organs did not provide adequate preventive

[7] Ibid

[8] Digital 2021: Ethiopia; available at: https://datareportal.com/reports/digital-2021-ethiopia [last accessed at 24/3/2022]

[9] 40+ Cyber security Statistics and Facts For 2022, at https://www.websiterating.com/research/cybersecurity-statistics-facts/ [last accessed at 23/3/2022]

[10] Ibid

[11] Ibid

[12] Ibid

[13] INTERPOL report identifies top cyber threats, at https://www.interpol.int/en/News-and-Events/News/2021/INTERPOL-report-identifies-top-cyberthreats-in-Africa [last accessed at 24/3/2022]

[14] Iyasu Teketel, *Cybercrime in Ethiopia: Lessons to be Learned from International and Regional Experiences*, LLM Thesis, Addis Ababa University, School of Graduate Studies, 2018, [Unpublished, available at Law library], P. 2 [hereinafter Iyasu, Cybercrime in Ethiopia]

and investigative mechanisms.[15] Nowadays, given the modernization and sophistication of cyber crimes or attacks, states have begun to employ more organized, specialized and latest criminal investigation techniques. As the internet played a major role in the commission of cyber crime through new locations and techniques in the manner that is more devastating and complicated, law enforcement organs are expected to track down using advanced and clandestine techniques. One of the criminal investigation techniques that has been widely accepted for the new form of crimes is special investigation techniques [Hereinafter SIT] which is characterized as covert and proactive ways of investigation. [16] Despite the absence of agreed definition to SIT, it is generally known and accepted that it involves some kind of secrecy and deception. This is for the reason not to alarm the subject about the ongoing investigation. [17]

As a result, law enforcement authorities may use complex, clandestine and sophisticated measures or any other proactive and covert strategies so as to tackle any attempt of cyber crime or other serious offences.[18] This is to have effective cyber crime prevention and investigation process and to secure both the national order and individual rights. Besides, as cyber crimes are perpetrated through computer networks, the exact location of criminals is, mostly, undefined. Or, the effects of cyber crime are beyond territorial boundaries of a given state. Accordingly, the problems of cyber crime investigations have worsened by transnational character of computer crime.[19] Given cybercrime investigations' potential danger to the enjoyment of human rights, it is agreed that its application is on the basis of effective legislative framework coupled with rigid procedural follow ups.[20] In Ethiopia, though cyber crimes were governed by very few provisions

[15] Johannes, Cyber Crime and Legal Countermeasures, (n 1), P. 197

[16] Peter Nyeste, 'The principles of the use of the special investigative techniques', *Національний університет,* 2018, vol. 17, No. ,1, PP. 1-11, P. 1

[17] Toon Moonen, 'Special Investigation Techniques, Data Processing and Privacy Protection in the Jurisprudence of the European Court of Human Rights', *Pace International Law Review Online Companion,* 2010, vol. 1, No. 9 PP. 97-136, PP. 99-100

[18] Worku Yaze, 'The Use of 'Special Investigation Techniques and Tools' in the Fight against Serious Crimes: Legal Basis and Human Rights Concerns in Ethiopia', *Journal of Ethiopian law,* 2015, VOL. XXX, PP. 81-111, P. 106 [hereinafter Worku, The Use of 'Special Investigation Techniques and Tools]

[19] Steven Malby et al, Comprehensive Study on Cybercrime, (draft report)UN New York, 2013, P.119 [hereinafter Steven, et al, Comprehensive Study on Cybercrime]

[20] Stefan Budjakoski, 'Use Vs abuse of special investigative measures in detecting severe form of crime in republic of Macedonia', *European Scientific Journal,* 2014, Vol. 1, PP. 345-352, Pp. 345-346

of the 2004 criminal code, the enactment of computer crime proclamation in 2016 marks a separate and organized cyber crime administration, detection, and investigation.[21]

Though, the proclamation introduces advanced investigation and prevention process, there is gaps of investigating cyber related incidents in a very effective manner. These investigations are composed of traditional and very new and advanced techniques and, require all inclusive and comprehensive legal frameworks that govern the implementation of the techniques adequately. In relation to this, writers like Misganu Y. and Kinfe M., noted that the existing legislations and policy initiatives are inadequate in cyber crime governance and investigations in this specific area failed to attain the objectives as expected yet.[22] In the same vein, the report on the status of Ethiopia regarding Budapest convention clearly reveals the gap by noting that there is no known procedural law governing how to detect, prevent and investigate acts enumerated as cyber crime. Besides, Bejatovic S. suggests in his article that the timing of; the level of probability; the jurisdiction of; duration and; criminal offences and persons against whom, the measures used are issues that can be considered as standards that an effective cyber crime prevention and investigations required to be met.[23] Besides, the effectiveness of cyber crime investigations depends on the existence of possibilities for information sharing and cooperation's with other sovereign states and employing newly advanced technologies for the proper implementation of investigations.[24] Unfortunately, Ethiopia is not a member to initiatives of cooperation both internationally and regionally and only has the 2016 proclamation which is subject to various criticisms and challenges.

The gap also relates to the absence of adequate literatures that has been conducted on the same issue that this research intends to conduct. As it will be discussed in the literature review part of this study, the existence of absence of scientific works in Ethiopia that contributes to the

[21] Computer crime proclamation, 2016, Federal Negarit Gazette, proclamation no 958, 22nd year No. 83 [hereinafter Computer crime proc. No. 958/2016]

[22] Misgana Yifiru, 'Assessment of Cybercrime Governance in Ethiopia Since 2004', *New Media and Mass Communication*, 2021, vol. 96, Pp. 1-8; see also Kinfe M., infra (n 29)

[23] Bejatovic Stanko, 'Special methods of revealing and investigating criminal offences committed by organized crime', *Journal of Criminology and Criminal Law*, 2006, vol. 44, Pp. 43-72

[24] Worku, The Use of 'Special Investigation Techniques and Tools (n 18), P. 86; see also Council of Europe Convention on Cybercrime, 2001(infra note 123) and African Union Convention Cyber Security and Personal Data Protection (infra note 133)

efficacy of cyber crime investigation and prevention triggers this researcher to conduct study on this area.

Therefore, this study is committed to identify and examine the legal and practical hindrances for the effective prevention and investigation of cyber crime in Ethiopia.

1.2. Statement of the Problem

Cyber crime is one of the crimes that reached the status of most serious crime universally. Given its complex and serious nature, it, heavily, impacts the socio-economic, political and security aspects of the global community. What makes the fight against cyber crime more complex and difficult is that it still lacks world-wide agreeable definition and absence of defined categories of acts considered as cyber crime.[25] As a number of existing literatures suggests, the criminal justice system that intend to effectively investigate and prevent such a serious crime needs to design investigative techniques that involve both traditional and *covert* or *deceptive*[26] actions and develop clear cut definition with precise classification of acts of crimes. Though the term cyber crime has been a subject of a number of legislative and academic discussions, up until now, there is a problem concerning the definition and typology of cyber crime activities. And, scholars in this field tend to view the term through the spectacles of their specialty. Besides, the existing understandings of the concept are either too general for practical application or highly restrictive to the concept. Therefore, lack of definitional and content wise clarity of both concepts is the first problem that is addressed in this study.

It has become almost more than half of a decade since Ethiopian government came up with a new legislation concerning computer crime [Hereinafter: Computer crime proclamation].[27] And the enactment of this proclamation introduced the formal and advanced administration, prevention and investigation of cyber crimes. However, apart from this advancement,[28] a number of writers in this field argued that, despite the existence of an increasing level of cyber attacks in various forms such as cyber hacking, dissemination of pornographic content, disruption, internet fraud and the like, the depth and breadth of

[25] Steven et al, Comprehensive Study on Cybercrime (n 19), PP. 6-7

[26] Id, PP. 122-123; see also Worku, The Use of 'Special Investigation Techniques and Tools (n 18), P. 86

[27] Computer Crime Proclamation (n 21)

[28] Id, article 25; see also Worku, The Use of 'Special Investigation Techniques and Tools (n 18)

proclamation 958/ 2016 is not adequate and prevention and investigation of cyber crimes is not as such effective.[29] Accordingly, they argue that lack of sufficient procedural stipulation about investigatory and preventive measures has become one the main problems in the fight against cyber crimes.[30] Thus, identifying and examining existing legal gaps that limits the effectiveness of cyber crime investigation and prevention is the other focal point of the study.

In addition to that, the proper application of cyber crime investigations require the presence of multiple sources of data that can indicate or alarm law enforcement organs to take all inclusive measures and to track down the commission of cyber crime as well as collect evidences. Cyber crime is one of the crimes that have transnational character and, given the sovereignty principle that every state entitled, gathering important data for cyber crime investigation beyond once own territorial boundary will be challenged.[31] Thus, the effective prevention and investigation of cyber crime depends on the existence of active collaboration with other states about sharing relevant information or evidences and working together in the fight against cyber crime. To this effect, CCP empowers the attorney general to work on the cooperation on cyber crime matters with other states. This is also one of the area that the legislators of DCPEC working on. However, Ethiopia's international cooperation and collaboration on cyber crime investigation and prevention is still at infant stage and the activities of assigned institutions are very weak and it looks surrounded by problems. Literatures also argue that, though the government has take part in some international cooperation and collaborations, institutions working on the prevention and investigation of cyber crime is challenged to effectively share necessary information and evidence or collaborate in cyber crime matters.[32] Hence, once the law stated the manner how and the body should engage in cooperation or legal assistance activities, it needs to identify the legal and practical gaps in relation with international cooperation status that causes ineffectiveness in the prevention and investigation cyber crimes.

[29] Kinfe Micheal, 'Ethiopia's new cybercrime legislation: Some reflection', *computer law and security review*, 2017, Vol. 33, PP. 250-255

[30] Ibid

[31] Farsam Salimi, 'Cybercrime Threats, Offences and Special Investigation Measures from a European Perspective', *New Zealand Yearbook of International Law,* 2017, vol. 15, Pp.47-60, P.54

[32] አገር አቀፍ የተቀናጀ የወንጀል መከላከል ስትራቴጂ, በሚኒሰተሮች ምክር ቤት የፀደቀ, 2012, ገጽ 10-11 ና 14

Moreover, the advancement introduced in the 2016 proclamation is a great move towards a comprehensive and modernized prevention of cyber crime investigation.[33] And once the law concerning cyber crime investigation is adopted, the practical application of investigation and prevention measures is expected to be very accurate and effective against such a complex and clandestine type of crime. Even if institutions such as Federal Police Commission, INSA and Ministry of Justice (Public prosecutors) are appointed for the proper detection and investigation of cyber-related crimes, the reports of a number of institutions such as Global Cyber security Index reveals the existence of institutional and professional problems in cyber crime investigations. Pursuant to the report of Ethiopia's intelligence office, there were 167 cyber crimes incidents that has left undetected in 2020.[34] The report also underlines the fact that this number would increase if those incidents that are left unreported or unknown were considered. One of these crimes was the crime that was perpetrated by Egypt-based group called the Cyber-Horus Group. Even though INSA claimed to have thwarted the attack, the group did manage to hack government web pages, post messages threatening war if the country began filling the renaissance dam.[35] Other sources, for instance, KasPersky recently revealed that there is 1058 ransomware, 1251 on-line malware, 5829 malware detection during web anti-virus scan, and 2484 network intrusion cyber crimes in Ethiopia at this time.[36] In addition to that, there is also high range of: electronic identity theft; computer related forgery and fraud; offences related to child pornography specifically and pornography in general such as indecent and erotic images and videos and revenge porn; racist and hate speeches; fake news; hacking; cracking; illegal data and system interference; illegal interception; website defacement; spam and virus dissemination, crimes commission both in governmental and non-governmental institutions and individual private matters including email and other social media accounts as well as electronic financial cards (ATM) or bank accounts. However, most of these crimes are left undetected and law enforcement officials are not effectively and adequately investigating reported crimes. Surprisingly, there are around 6 cases that are effectively investigated and prosecuted as well as

[33] Kibreab Adane, 'The Current Status of Cyber Security in Ethiopia', *The IUP Journal of Information Technology*, 2020, Vol. XVI, No 3, Pp. 1-13, P. 3

[34] Ethiopia's intelligence office foils 787 cyber attacks-official, at http://www.apanews.net/mobile/unelnterieure_EN.php?id=4943340 [last accessed at 1/4/2022]

[35] Africa's evolving cyber threats: Africa center for strategic studies; at https://africacenter.org/spotlight/africa-evolving-cyber-threats/ [last accessed at 28/3/2022] [hereinafter: Africa's evolving cyber threats]

criminals are convicted.[37] Thus, there is a problem in the investigation and prevention of cyber crime and it needs to assess and identify legal and practical difficulties in investigating and preventing cyber crime issues in Ethiopia.

Therefore, this study explores and assesses the existing legal and practical challenges that affect the effective prevention and investigation of cyber crime and recommend possible solutions.

1.3. Objectives of the Study

1.3.1. General Objective

The cardinal objective of the study is to identify and examine the legal and practical challenges hindering the effectiveness of the prevention and investigation of cyber crimes.

1.3.2. Specific Objectives

Towards the achievements of the general objective, this study specifically aims to:

- ❖ Expose the meaning, extent and taxonomy of cyber crime;
- ❖ Discuss the institutional framework of cyber crime investigation and prevention in Ethiopia;
- ❖ Examine the legal framework of cyber crime and identify the legal gaps hindering the effectiveness investigation and prevention;
- ❖ Explore the practical and institutional challenges to the effectiveness Cyber crime investigation; and
- ❖ Recommend what measures should be taken by the concerned organs of the government for the effective investigation and prevention of computer crime.

[36] CYBERTHREAT real-time map, at http://cybermap.kaspersky.com/ [last accessed at 9/5/2022]

[37] Federal Ethics and Anti-Corruption commission v. Michael Worku (no. 85025); Federal Public Prosecutor v. Abraham Benti and Wendwesen Girma (0075/05); Federal Public Prosecutor v. Mesele Yohannes (no. 113949); and Riyan Miftah v. Elsewdi Kebels PLC (no. 91710). Interview with W/rt Mignot K., Public prosecutor at Organized and Trans-national as well as National Affairs Criminal Matters Directorate (Ministry of justice), on the practice of cyber crimeinvestigation and prevention, August 21, 2022

1.4. Research Questions

1.4.1. General Research Question

The study principally intends to answer the question:

What are the legal and practical challenges that hamper the effective prevention and investigation of cyber crimes in Ethiopia?

1.4.2. Specific Research Questions

The general research question is divided in to the following specific research questions:

- ❖ What looks the practice of cyber crime prevention and investigation in Ethiopia like?
- ❖ Is the current stand of Ethiopian computer crime legal framework adequate or sufficient to effectively prevent and investigate cyber crime incidents?
- ❖ What gaps of existing Ethiopia legislation dealing with cyber crime hinder the effectiveness of cyber crime investigation and prevention?
- ❖ What practical and institutional challenges hinder the effectiveness of cyber crime investigation and prevention in Ethiopia?
- ❖ What other measures should be taken by the concerned organ for the effectiveness of cyber crime investigations?

1.5. Significance of the Study

Since this study explores the legal and practical challenges hindering the effectiveness of cyber crime prevention and investigation in the study area, it is strongly anticipated that the study have both theoretical and practical significances.

As a practical significance, the study:

- Reveals the weakness of the contemporary practice of cyber crime prevention and investigation and alert the concerned government organ to revisit the current practices;
- Persuades the legislator to amend the existing computer crime proclamation to a comprehensive, harmonized and more advanced law that create suitable conditions to the effective prevention and investigation of cyber crime investigation in every perspectives;

- Gives new and groundbreaking insights as to how the government and other concerned organs should work to address the existing problems and to develop strong, modern and effective prevention and investigation of computer crimes.

As a theoretical significance,

- Since there is a drought of literatures written on Investigation and prevention of cyber crime, the study will add something to the existing stock of knowledge because as it is revealed in the literature review part, the theme of this thesis is genuine and fill the existing gaps in Ethiopian criminal investigation studies.
- The study is expected to encourage and inspire future researchers who want to further explore the issue.
- The study could be the key information source for policymakers, the public, security professionals, and other academics through revealing the existing difficulties in the prevention and investigation of cyber crime in Ethiopia.

1.6. Research Methodology

1.6.1. Research Method

In this study, the researcher has employed qualitative research methodology. Because the qualitative type of research method is helpful to get the feeling, opinion and richer and in-depth understanding of research participants and to deeply explore the problem and to get deep information.[38] According to Mike MCconvil and Wing Horey Chuvi, the best research approach that enables the researcher to understand a particular setting and practice is the qualitative research method.[39] The qualitative research method is also helpful in exploring the social world and realities in an in-depth manner and to draw courtesy to processes, structural features, and meaning patterns.[40] It also helps to describe the world from the participants' point of view.[4142]

[38] Nega Ewnete(Associate professor), *Advanced legal research*, Lecture delivered at School of Law, Bahir Dar university, October 2020. [here in after Nega, Advanced legal research]
[39] Mike Mcconvil and Wing Horey, *Research methodology for law*, Edinburgh university press, 2007, P. 32
[40] John Creswell, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*, 4th ed., Sage Publication Inc., Thousand Oaks, 2014, P. 32
[41] Jenner B., *A Companion to Qualitative Research*, 2nd ed., Sage Publications Ltd, 2004, P. 21

The study has blended both doctrinal and non-doctrinal qualitative research methods. Regarding the justification to use doctrinal research method, it is helpful to identify, thoroughly scrutinize, analyze and interpret the legal challenges for effective investigations cyber crime incidents. The doctrinal aspect of the study is helpful, predominantly, to identify and examine those gaps on the basis of selected national and international legal and non-legal documentary sources.

Since, the nature of the problem or the research questions demands identification and examination of the practical challenges hindering the proper investigation of cyber crime, the study has also employed non-doctrinal qualitative research approach. The rationale behind employing the non-doctrinal research approach is that it is highly important to study the gaps between legislative goals and social (practical) reality and to strengthen data collected doctrinally.

1.6.2. Type and Sources of Data

This research has employed both primary and secondary sources of data. For the non-doctrinal research method, the primary sources of data are an in-depth interview and open-ended questionnaires to/ with key informants. To supplement the data gathered through interview and questionnaires, the study has consulted published and unpublished materials. For the doctrinal research method, the primary sources are national laws dealing with cyber crime prevention and investigation in tandem with international and regional legal instruments dealing with the subject of this study. As the secondary sources of data, published and unpublished literatures, legal periodicals (journals) and other internet sources are employed.

1.6.3. Data Collection Methods or Tools

The study has employed semi-structured interviews and open-ended questionnaires. Regarding justification for using semi-structured interviews, on the one hand, it is helpful to have in-depth and rich information about the issue to be scrutinized.[43] On the other hand, it is helpful to get additional information from the respondent in case of ambiguity and vagueness and more importantly, it makes the researcher to be more flexible in changing or modifying interview

[42] Charles K. and Ahmed B., 'Understanding and Applying Research Paradigms in Educational Contexts', *International Journal of Higher Education*, Vol. 6, No. 5, PP. 26-28

[43] Nega, Advanced legal research (n 38)

questions that he will develop in advance.[4445] The researcher also used open-ended questionnaires because it is a proper tool to obtain the needed information on the subject matter when there is shortage of time to conduct in-depth interview and/ or if key responds is not available at every time. Interviews were conducted face to face and via telephone.

Moreover, policies, documents and pertinent laws are also collected and reviewed to get more understanding of the issues under study using catalogs; computer and mobile phone from the internet and different online data-bases.[46]

1.6.4. Sampling Techniques

Sampling technique basically classified in to two: random and non-random. In the case of random sampling, each member of the sampling frame has an equal chance of being selected as a participant of the research. In the latter case, each member of the sampling frame does not have an equal chance of being selected as a participant in the study.[47] Thus, this study has employed non-random purposive sampling technique. Because, to effectively answer research questions and attain the stated objectives, participants of the research were the key informants within INSA, Federal Police and Ministry of Justice (Public prosecutors) situated in Addis Abeba, Ethiopia. Informants were purposely selected and interviewed on the basis of their official position, experience and familiarity with the subject matter of the research.

In addition to the stated sampling techniques, the researcher has determined the sample size on the basis of data saturation and redundancy test.[48] This is mainly because; the data gathered in qualitative research is expected to be more in-depth, rich and accurate for the effective analysis. And findings may not be generalized to the larger population. So, if the information's become redundant and the researcher believes the recruitment of additional respondent doesn't add new information, it is concluded that the data is saturated.

[44] Ibid

[45] Catherine D., *Practical Research Method*, Magdalene Road, United Kingdom, 2002, p. 28

[46] Wondemagegn Tadesse, 'Legal Research Tools and Methods in Ethiopia', *Journal of Ethiopian Law*, 2012, Vol. 25, No.2, P. 79

[47] Nega, Advanced legal research (n 38)

[48] Saturation in qualitative research: exploring its conceptualization and operationalization; at https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5993836/ [last accessed at 30/3/22]

1.6.5. Data Analysis

To properly answer the stated research questions and scrutinize the collected data, the researcher has used qualitative data analysis method. In doing so, the study has used qualitative data analysis technique. For the doctrinal part of the research, the study has employed document analysis technique to interpret and conclude data collected from legal and non-legal documents. Concerning the empirically collected data, raw data that has obtained through interview and questionnaires was structured systematically, organized and analyzed by narrative analysis method. The rationale for using this method is that it is very helpful to assess the content of responses of key respondent with data collected from legal and non-legal documents in a way that answers the research questions.[49] Before analyzing the data, since the data gathered through interview and questionnaires were scattered and in Amharic language, the researcher prepared the collected data and translate the data verbatim to English language in understandable manner. After making these, the researcher has made deeper reading to internalize the collected raw data and eventually the researcher summarized, interpreted and expounded the result in order to reach at a conclusion.

1.7. Review of Related Literatures

Plenty of studies has been conducted on the issue of cyber crime and it has become the common topic in academic and non-academic researches across the globe, yet very little studies was made on the issue of special investigation techniques in relation with cyber crime or any other serious crimes. The following discussion is devoted to explore some of the previous works related with the focal point of this paper.

The first scholarly work in relation with cybercrime is the research conduct by Tewodros Getaneh and titled as "Cyber Security Practices and Challenges at Selected Critical Infrastructures in Ethiopia".[50] In his study the researcher found Tailoring Cyber Security Framework by examining the practices and challenges of cyber security at three selected critical

[49] Humans of Data, available at https://humansofdata.atlan.com/2018, [last accessed 26/3/2022]

[50] Tewodros Getaneh, *Cyber Security Practices and Challenges at Selected Critical Infrastructures in Ethiopia*, Master thesis, Addis Ababa University, Department of Science in Information Science, [Unpublished, available at Law library], pp. 1-93

infrastructure in Ethiopia, viz., Ethiopian Electric Power, Ethiopian Electric Utility and Ethio-Telecom. The study revealed that the top four challenges at selected critical infrastructure are lack of in-house expertise, inadequate enabling technology, and difficulty in locating the right security alert and evasion of preventive security controls by conducting survey. In addition, the selected critical infrastructure is inadequately prepared to detect, prevent, and respond to cyber threats and breaches. The study developed a tailored cyber security framework based on INSA's Critical Mass Cyber Security Requirement Standard and failed to depend on other international standards and frameworks.

In the same vein, Iyasu Teketel also conducted a research titled as "Cybercrime in Ethiopia: Lessons to be Learned from International and Regional Experiences"[51] and argued that though there is high level of access to internet and expansion of digitalized system in a number of infrastructure, but such development has not been matched with equal investment in the fields of security and adequate legislation to govern the area. Ethiopia as a country vulnerable to an increasing rate of cybercrime needs to develop a more comprehensive law and consider the regional and international efforts.[52] Regardless of the enactment of new Computer Crime Proclamation and the establishment of INSA to principally deal with the matter of cyber security, there is still a lot to be done so as to offer better protection to the public from cybercrime and ensure a safe and smooth business transaction that depends on and make use of the appropriate technology.[53]

The other literature is the research titled "Computer Related Crime under Ethiopia: Comparative Study, by Meserert Lakew.[54] Apart from an attempt to define the term cyber crime, the researcher tries to comparatively discuss the governance of computer crime; and tries to highlight the types of cyber crime. After all, the researcher concludes that computer crime is a branch of vast categories of crime. The elements of legal, material and mental elements should be fulfilled for criminate computer crime conviction. And, in order to control computer criminals, like almost all countries in the world, Ethiopia has recently promulgated computer

[51] Iyasu, cybercrime in Ethiopia (n 14)
[52] Ibid
[53] Ibid
[54] Meserert Lakew, 'Computer Related Crime under Ethiopia: Comparative Study',…, PP. 1-42; at http:// www.abyssinialaw.com [last accessed 4/4/2022]

crime legislation, but when it compared with other countries the legislation is rather vague, limited in its scope, leaves no room for definition and not clear.

The other related literature is the research titled "The Quandary of Cyber Governance in Ethiopia" by Temesgen Aschenek;[55] The researcher found out the dilemma of cyber governance in Ethiopia and the findings revealed that there are a number of legal, policy and institutional initiatives designed to guide cyber governance in Ethiopia. However, the overall aspects of cyber governance have posed a peril to digital landscape; there is excessive control and restriction of access to information in Ethiopian digital landscape; institutional structures lack transparency and coordination of tasks for responsive service delivery. The researcher suggested that the government must focus on expanding the infrastructure to assure accessibility and revising the policies and legal instruments to ensure digital freedom so as to get the maximum blessings that the digital world has brought to us.

In addition to the above literatures, "Some Remarks on Ethiopia's New Cybercrime Legislation"[56] by Kinfe Micheal is also the other literature (comment) in relation to computer crime. In his paper, the writer has highlights the developments of Ethiopian legal framework on computer crime and discusses the silent features of the 2016 computer crime proclamation. The paper through elaborating the new issues and the content within the law identified major problematic issues of the proclamation with regard to human right and freedoms of the citizens. The paper was conducted by the doctrinal methodology and doesn't assess the challenges on ground. Though the writer has revealed some difficulty for the governance and prevention of cyber crimes, it is not comprehensive and doesn't examine with the existing developments in computer crime investigation and prevention.

The last but not the list related study is the research titled "Developing national cyber security strategy for Ethiopia" conducted by Abenezer Birhanu.[57] The researcher chiefly argued

[55] Temesgen Aschenek, 'The Quandary of Cyber Governance in Ethiopia', *Journal of Public Policy and Administration*, 2019, Vol. 3, No. 1, pp. 1-7

[56] Kinfe Micheal, 'Some Remarks on Ethiopia's New Cybercrime Legislation' *Mizan law review*, 2016, Vol. 10, No.2, PP. 448-458

[57] Abenezer Berhanu, *Developing National Cyber-security Strategy for Ethiopia*, Master's Thesis, Tallinn University of Technology, School of Information Technologies, Department of Software Science, 2019 [unpublished]; available at: https://digikogu.taltech.ee/et/Download/06ef8980-4c08-94d1-7918a42e80a0 [last accessed at 5/4/2022]

that existence of National Information Security Policy in Ethiopia, there is an apparent lack of practical and comprehensive strategy that addresses contemporary cyber security challenges. Lack of effective measures to fight against cyber incidents have resulted in the growth of cyber crime in the country. The researcher had conducted comparative analysis about cyber security strategy of Ethiopia with other countries such as Rwanda, Canada, and Germany.

There are also ample of domestic and foreign studies conducted in relation with investigation or prevention of cyber crime. "Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice" by Australian writer Cameron S. D. Brown;[58] "Process of Legalizing Special Investigative Techniques in China" by Liao Ming;[59] "Cybercrime Threats, Offences and Special Investigation Measures from a European Perspective" by Salimi Farsam;[60] "Intelligence Acquisition Methods in Cyber Domain: Examining the Circumstantial Applicability of Cyber Intelligence Acquisition Methods Using a Hierarchical Model" by Karri Wihersaari;[61] and "Investigating cybercrime" by Jan-Jaap Oerlemans[62] are the literatures that this researcher can find with exhaustive internet based searches. But, this doesn't mean that there is no any other literatures related to this study, but given the knowledge, skill of, and technical difficulty faced by this researcher, the above reviewed materials are the existing and directly or indirectly related literatures to the study. Accordingly, since the stated research problem, objectives and questions are different in view of the above reviewed literatures either in its perspective or subject-matter, this researcher believes that the topic of this study remains a novel area of legal research and practice. Therefore, the gaps exists in the above reviewed literatures and the contribution that this research produces for the better investigation and detection of cyber crime fascinates this researcher to conduct this study. As pointed out above, this study explores and examines the legal and practical challenges of cyber crime investigation in Ethiopia.

[58] Cameron S. D. Brown, 'Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice', *International Journal of Cyber Criminology***,** 2015, Vol. 9, PP. 55–119

[59] Liao Ming, 'Process of Legalizing Special Investigative Techniques in China', *The Frontiers of Law in China*, 2015, Vol. 10, No. 3, PP. 510-536

[60] Salimi Farsam, 'Cybercrime Threats, Offences and Special Investigation Measures from a European Perspective' (n 30)

[61] Karri Wihersaari, *Intelligence Acquisition Methods in Cyber Domain: Examining the Circumstantial Applicability of Cyber Intelligence Acquisition Methods Using a Hierarchical Model*, Master's Thesis, National Defence University, Master of Military Sciences, 2015, [Repository: National Defense University Course Library], PP. 1-63

[62] Jan-Jaap Oerlemans, *Investigating cybercrime*, Doctoral dissertation, Leiden University, 2017,[repository: Leiden University] [Hereinafter: Jan-Jaap Oerlemans, *Investigating cybercrime*]

1.8. Scope of the Study

The subject matter of this study is confined to examine and identify challenges for effective prevention and investigation of computer crime incidents in Ethiopia. In doing this, the study explored and assessed the existing legal gaps, practical hindrances and institutional difficulties. The justification for intending cyber crime prevention and investigation as a focal area in this study is its emerging, complex, more advanced and damaging nature along with its impact across the globe as well as the contemporary high rate of cyber crime commission in Ethiopia. Almost all studies on cyber crime focus on the definition and classification of cyber crime, and on the human right perspectives and impacts of computer crime related laws. Thus, there is a need to study on the advancement and effectiveness of crime investigation and prevention, particularly computer crime investigation and prevention.

Area wise, the study has explores and examined the challenges in Ethiopia. And, no further move is taken to identify another country's challenges in relation with cyber crime investigation and prevention. With regard to laws to be examined, the researcher has exclusively focuses on the 2016 computer crime proclamation and other laws dealing with computer crime. The study also takes a look at draft criminal procedural and evidence law and FDRE criminal justice policy to grasp important issues and directions that the government working in relation with the subject matter of this study. International (regional) and sub-regional legal instruments in relation with cyber criminal prevention and investigation as well as official statistics were consulted to strengthen the discussion.

1.9. Limitation of the Study

In conducting this study, the researcher was challenged. First, as the issue of cyber crime is a very new and complex concept, the researcher has faced shortage of literatures which are written on its normative and institutional framework as well as statistics and government reports on the commission, investigation and prevention of cyber crime in Ethiopia. But, the researcher has tried to overcome through the interview with respondents and other literatures that can fill the gap. Second, the existence of lack of well organized and accessible data recording, handling (documents) and management problems in the governmental offices which the researcher has contacted with. In such a case the researcher faces the absence of relevant information and document as well as cases on cyber crime investigation. Third, the other limitation that this researcher faced is the absence willingness and cooperation from interviewees and other participants of the research in the course of collecting first hand information. Especially, Judges and one public prosecutor tacitly refused to give information and participate in the research. In our country, the government institutions are full of tide and complex bureaucratic approach. So, having access to documents exists in a governmental offices and a time to discussion with officials has, really, made things more difficult and challenging to the proper compilation and comprehensiveness of the study.

1.10. Ethical Considerations

In this research, the writer has given much emphasis to ethical consideration. Given that, to confirm the voluntary participation of participants, the researcher has selected respondents after their full and free consent and being informed of their right to withdraw at any time if it is appropriate. In doing so, the researcher has prepared the form to disclose the informed consent of the participants. The researcher has clearly disclosed the nature and purpose of the research to the participants to enable them to know about the theme of the research. Besides, the identity and confidentiality of the participants has kept secret and only the names of those respondents who are willing to reveal themselves are disclosed. The impartiality and genuineness of the data has not been prejudiced by the researcher. Finally, the study has employed the rule of citation of Bahir Dar University School of law for acknowledging each and every data or idea that has collected from others work or respondents. In general, the researcher has guided the study with all ethical standards related to conducting a research.

1.11. Organization of the Study

This research paper is structured in to four chapters. The first chapter is tasked to deal with the issues of how and why the researcher conducted this study and covers background of the study, statement of problem, research objectives and questions, methodology, scope of the study and the like. Chapter two is devoted to elaborate the definition and conceptual frameworks of cyber crime, its types and the existing national legal framework governing the issue. In addition to that, international laws and rules dealing with the notion of cyber crime and cyber crime prevention and investigation are discussed under this chapter. This chapter also made an attempt to highlight the institutional set ups for the prevention and investigation of computer crimes in Ethiopia.

Under chapter three, the study has made in-depth analysis of the data collected. And, the existing legal and practical challenges for the effective prevention and investigation of cyber crimes in Ethiopia are explored and assessed. At the end, on the final chapter the paper draws conclusion for the entire work and forwarded appropriate recommendations.

CHAPTER TWO

THEORETICAL, LEGAL AND INSTITUTIONAL FRAMEWORKS FOR THE INVESTIGATION AND PREVENTION OF CYBER CRIME

2.1. Theoretical and Conceptual Framework of Cyber Crime

2.1.1. Conceptualizing Cyber Crime

Despite the presence of ample of literatures talking about the notion of cyber crime, there is no agreed upon definition for the term cyber crime yet. Though elaborating the concept of cyber crime from definitional point view is an attempt to attach some meaning full words for its explanation, the nature of and the manner how cyber crime is committed in present days create hurdles for having clear picture of the crime. Different writers have pondered around the idea of defining the term, but they have given a definition either too general for practical application and controlling the crime or too narrow to understand what it means. Crutchfield once said that *"The act of defining crime is often, but not always, a step toward controlling it".*[63] Thus, without going into detail at this stage, it needs to undertake an overview of definitions given by a number of scholars, researchers and bodies having legislative power.

Jan-Jaap, the researcher in this area, defines cyber crime as "*criminal acts committed using electronic communication networks and information systems or against such networks and systems* ".[64] According to this definition, cyber crime can be understood as criminal activity that uses computer and networking system both as a tool and as a target. Ahmet Nuredini in his article also defines the term in a very descriptive manner as:

> …unauthorized interception of computer systems and computer data through computers with intent to intercept the network and computer systems, in order to obtain personal data or manipulate with these data, use of computer resources for terrorism, intercept and obtain data from computer systems for financial, political and blackmailing purposes, unlawful hindrance of computer systems, acts against confidentiality, integrity and availability of the computer system data etc.[65]

[63] Crutchfield R., Crime: Readings (Pine Forge Press, California, 2000), P. 7 [Hereinafter: Crutchfield R., Crime: Readings]

[64] Jan-Jaap Oerlemans, *Investigating cybercrime*, (n 62), P. 20

[65] Ahmet Nuredini, 'Challenges in combating the cyber crime', Mediterranean Journal of Social Sciences, 2014, vol. 5, no. 19, Pp. 592-599, P. 593

Besides, a number of literatures describe cybercrime as any activity in which computers or networks are a tool, a target or a place of criminal activity.[66] Even if this definition is used as a common way to describe the crime in those literatures, it is very broad definition by which it encompasses any of traditional crimes that involves the hardware of the computer such as body injury which is perpetrated by hitting the victim by either the monitor or key board. Kate Brush defines the term as "*any criminal activity that involves a computer, networked device or a network*".[67] And describes its nature as "*Cybercrimes generally do not occur in a vacuum; they are, in many ways, distributed in nature. That is, cybercriminals typically rely on other actors to complete the crime".*[68] Accordingly, likewise the definition stated above, this definition is also very general and she tries to address cyber crimes as a crime resulted from activities of a number of (groups) of individuals having connection for the perpetration of a single cyber crime. Thus, Kate's perspective urges us to think about cyber crime outside the box and to understand its real nature.

Further, during the 10th UN Congress on the Prevention of Crime and the Treatment of Offenders, two definitions were developed within a related workshop:[69] the first describe cybercrime as an act that covers any illegal activities directed by means of electronic operations that target the security of computer systems and the data processed by them. And the second definition reads as:

> [an act that] covers any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network.

From the reading of the above definitions, one can understand the fact that the first definition is more of a narrow definition by which it doesn't recognize the involvement of network in cyber

[66] Carter, Computer Crime Categories: How Techno-Criminals Operate, FBI Law Enforcement Bulletin, 1995, page 21, available at: www.fiu.edu/~cohne/Theory%20F08/Ch%2014%20-%20Types%20of%20computer%20crime [last accessed at 20/5/2022]; *Charney*, Computer Crime: Law Enforcement's Shift from a Corporeal Environment to the Intangible, Electronic World of Cyberspace, Federal Bar News, 1994, Vol. 41, Issue 7, page 489

[67] Cyber crime, available at https://www.techtarget.com/searchsecurity/definition/cybercrime [last accessed at 20/5/2022]

[68] Ibid

[69] Crimes related to computer networks, Background paper for the workshop on crimes related to the computer network, 10th UN Congress on the Prevention of Crime and the Treatment of Offenders, 2000, A/CONF.187/10, page 5; available at: www.uncjin.org/Documents/congr10/10e [last accessed at 20/5/2022]; see also *Kumar*, Cyber Law, A view to social security, 2009, page 29

crime activity. Conversely, the second definition looks wider and ties to encompass every criminal activity that involves computer or network.

Vijaykuma Shrikrushn, one of the prominent writers in this field, also defines the term generally as "the harmful acts committed in Cyber space *with, on or by means* of computer networking".[70] Hence, according to this definition only those acts that involve networks can be assumed as cyber crime and this limit the scope of the crime in a very narrow manner in comparison with other definitions.

Furthermore, the council of Europe under the convention on cyber crime defines the term cyber crime as "a wide range of malicious activities, including the illegal interception of data, system interferences that compromise network integrity and availability, and copyright infringements".[71] The council in this definition tries to define cyber crime by exploring the acts that constitute the crime and failed to define the crime at hand in a descriptive manner.

In Ethiopia also the term cyber crime has been the subject of a number of literatures and most of them defines in a various ways and obviously lacks consensus in any one of them. Among these definitions the definition given by proclamation no. 958/ 2016 is the governing definition in Ethiopia. And the proclamation defines it as:

> A crime committed against a computer, computer system, computer data or computer network; A conventional crime committed by means of a computer, computer system, computer data or computer network; or Illegal computer content data disseminated through a computer, computer system, or computer network;[72]

The issue of defining the term cyber crime is one of a problematic and unsettled issue till today and as we have seen above scholars, writers and even governmental organs attempt to explain what it really means from different perspectives. Most of the definition given for cyber crimes can be categorized as descriptive, functional, elaborative, purposeful or expressive; and made up of the characteristics and nature that the crime has. As Vijaykuma and other writers noted the

[70] Vijaykuma Shrikrushn, 'The concept of cyber crime', *Global Journal of Enterprise Information System*, 2011, vol. 3, PP. 72-84, P. 79; [Hereinafter: Vijaykuma Shrikrushn, 'The concept of cyber crime']

[71] Cyber crime, available at https://www.techtarget.com/searchsecurity/definition/cybercrime [last accessed at 20/5/2022]

[72] Computer Crime Proclamation, (n 21), article 2(1)

existing definitional problem is related to the jurisprudential and jurisdictional problems along with the changing nature of the crime at hand.[73]

Moreover, the existing problem is not only about the definition of the crime rather it is also about terms used to refer the crime. The term cyber crime, computer crime, e-crime, high-tech crime, internet crime and digital crime have been used by a number of writers, scholars, reports and legislative documents interchangeably. However, writers like George Curtis and Jan-Jaap Oerlemans identify the existence of difference as between those terms and they mention the fact that they preferred computer crime and cyber crime to refer the crime at hand respectively.[74] As a result, it is obvious to see writers choosing one term over another to refer the crime. But, this researcher opted to use these terms interchangeably because without having an agreed definition for the crime, it would be better to use multiple terms to address the crime in all spectrum.

In conclusion, even if it is challenging to draw a conclusion and have a definition free from criticism, but for the purpose of this research and to put the readers in line, the following definition is preferred by this researcher. Cyber crime is "*any criminal conduct that relates to attacks on or/ and with computers, computer data, computer networks and other information and communications technology*" [emphasis added].[75] This researcher is of an opinion that every attempt that intends to define cyber crime should consider the place where it is committed, the person (identity) behind the crime, the victim, the general society at stake and the tools that used to commit the crime.

2.1.2. Taxonomy of Cyber Crime

As we have seen above, different writers and scholars attempt to define the term computer crime but none of these definitions have reached to acceptance globally yet. As a result, it has become a wise move to understand its nature and know what really means through classifying or categorizing each activity that are accepted as cyber crime in different groups. However, there is no universally agreed up on classification of the types of cyber crime. And different scholars and legislative documents have developed different kinds of categories. For instance, Kejal Chintan categorized cyber crimes in to two main categories: computer as a target and computer as a

[73] Vijaykuma Shrikrushn, 'The concept of cyber crime' (n 70)

[74] Jan-Jaap Oerlemans, *Investigating cybercrime',* (n 62), p.72

[75] Worku Yaze(Asst. professor, PhD candidate), *Contemporary issues in criminal law*, Lecture delivered at School of Law, Bahir Dar university, February 24, 2021.

weapon.[76] She further classifies cyber crime as unauthorized Access, online fraud and hacking and cracking.[77] From another perspective, Adam M. Bossler and Tamar Berenblum also classify computer crime in to four categories: cyber trespass, cyber deception/ theft, cyber obscenity/ porn and cyber violence.[78] They categorize a number of cyber crime activities on the basis of the nature and characteristics as well as their impact.

A number of writers including but not limited to Kelly J. Harris[79] classifies cyber crime in to three types. First, computer as the tools of the crime or incidental to the crime: this is when someone use your computer to gain access to or alter data stored on another computer, second, Computer as the subject of the crime: when anyone use your computer or any other computer to get the data stored in the computer and third, computer as the object of the crime: when computers and the system component of the computer be stolen or destroyed and also all sensitive information stored in a computer can be lost when the computer stolen.

Besides, Divy Shivpuri very differently classifies cyber crime in to four categories as: cyber Crime against individuals; cyber Crime against property; cyber Crime against organization; and cyber crime against society.[80] Divy uses different approach to classify cyber crimes and he try to develop his own taxonomy of cyber crime on the basis of victims of the crime.[81] Nevertheless, such classification looks weak and have overlapping nature one to the other.

Furthermore, one relevant approach can be found in the Budapest Convention on Cybercrime, which classifies cyber crime into four different types of offences[82]: Offences against the confidentiality, integrity and availability of computer data and systems is the first category of crimes and it consists offences such as illegal access to the computer through hacking, cracking

[76] Kejal Chintan, 'Cyber Crime and its Categories', *Indian journal of applied research*, 2013, Vol. 3, Pp. 130-133, P. 130; [Hereinafter: Kejal Chintan, 'Cyber Crime and its Categories]
[77] Ibid
[78] Adam M. Bossler and Tamar Berenblum, 'Introduction: new directions in cybercrime research', *Journal of Crime and Justice*, 2019, Vol. 42, No. 5, Pp. 495–499, P. 495
[79] Kelly J. Harris, 'Computer Crime: An Overview', *National Consortium for Justice Information* and *Statistics*, 1995, PP. 1-6, P. 2
[80] Divy Shivpuri, 'Cyber Crime: Are the Law Outdated for this Type of Crime', *International Journal of Research in Engineering, Science and Management*, 2021, Vol. 4, Pp. 44-49, P. 45
[81] Ibid
[82] Convention on Cybercrime, 2001, Council of Europe, European Treaty Series - No. 185, articles 2-5.; at https://rm.coe.int/1680081561 [Last accessed at 15/7/2014]see also :

and other methods; illegal interception; illegal acquisition of data; data interferences and system interference. As the name of the category indicates, all of the offences in this specific class are directed against (at least) one of the three legal principles of confidentiality, integrity and availability of computer and computer data. Computer-related offence is the other category of acts constituting cyber crimes. As a peculiar feature, offences under this category are traditional criminal acts but need computer and a computer system to be perpetrated. The category includes computer-related fraud, computer-related forgery, phishing, identity theft and misuse of devices.

Under the content-related offences category the convention includes offences such as illegal gambling's and online games; racism, hate speech and glorification of violence; libel and false information; spam and related threats; xenophobic material or insults related to religious symbols; child pornography, exchange of erotic or pornographic materials and any other illegal contents. Chiefly, this category is based on the content of the transaction or activity that the computer is needed. Copyright and trademark-related offence is the fourth category in the convention and consists every illegal activity that are committed in trade and business as well as entertainment activities motivated to misleading users and domain name related offences. But, this taxonomy is criticized because the categories are inconsistent and the drafter failed to use a single criterion to develop this classification.[83]

However, various numbers of writers, reports, researches and other literatures widely classify computer crime in to four different categories.[84][85] Depending on the relation of the crime to the computer, cyber crime is categorized as: computer as a target; computer as the instrumentality of the crime; computer is incidental to other crimes; and crime associated with the prevalence of computers.

Computer as a target: crimes under this category are relatively new form of crime and require the extensive knowledge of computer system. Mostly, such crimes are perpetrated by a selected

[83] Marco Gercke, 'Understanding cybercrime: phenomena, challenges and legal response', ITU, 2012, available at: www.itu.int/ITU-D/cyb/cybersecurity/legislation.html [last accessed at 20/5/2022]; [Hereinafter: Marco Gercke, 'Understanding cybercrime: phenomena, challenges and legal response]

[84] Hamid Jahankhani, et al, 'Cybercrime classification and characteristics', researchget, 2014, available at https://www.researchgate.net/publication/280488873 [last accessed at 22/5/2022]; [Hereinafter: Hamid Jahankhani, et al, 'Cybercrime classification and characteristics]

[85] Cybercrime, available at https://illicittrade.org/cybervrime [last accessed at 23/5/2022]

group of individuals who uses computers to get data stored in another's computer.[86] Here it is important to draw a clear picture as to what computer is mean. Though literatures provides both the broadest and narrow meaning to the term computer, it may be considered as any electronic device that can store, process, transfer data and perform logical operations.[87] Thus, any criminal act that targets the integrity, confidentiality and availability of computers will fall under this category.[88] Most of the times criminal acts including but not limited to hacking, cracking, illegal data acquisition (espionage), phishing, denial-of-service attack, data interference, illegal interception, system interference, virus dissemination falls in this category.[89] In general, cyber crime under the category of computer as a target may be taken as unlawful access to computer or computer network for the sake of malicious or deceptive data alteration, sabotage of computer software or hardware, program or data theft, and computer virus implantation.[90]

Computer as the instrumentality of the crime: this category is mostly referred as "computer as a tool" and consists numerous activities that uses computer for the purpose of the commission of crimes of real world.[91] For criminals in this category, computer and computer network play an essential role in the commission of traditional crimes. The crime committed existed since time immemorial and what makes such crime new is the use of computer and the internet. Mostly, criminals are unknown or commit anonymously and the result, most of the times, is psychological and intangible. Crimes such as fraudulent use of ATM, identity theft, child pornography, copyright infringement, mail or wire fraud, spam, religious offences, hate speech, racism, illegal gambling, cyber terrorism, cyber stalking, cyber defamation, online drug trafficking and others related crimes may be categorized under this type of cyber crime.[92]

Computer Is Incidental to Other Crimes: unlike the previous types of cyber crime, in this category, computer and computer network may be used as a means of facilitating the commission of different kind of crimes. Thus, when computer and computer network serves as a tool by which it contains necessary and valuable information or evidence in the planning and

[86] Joseph Aghatise, 'Cyber Crime Definition', Researchget, 2014, available at: https://www.researchgate.net/publication/265350281 [last accessed at 20/5/2022]

[87] Cornell law school; available at: https://www.law.cornell.edu/cfr/text/48/23.701 [last accessed at 28/5/2022]

[88] Marco Gercke, 'Understanding cybercrime: phenomena, challenges and legal response' (n 83)

[89] Ibid

[90] Ibid

[91] Kejal Chintan, 'Cyber Crime and its Categories', (n 76)

[92] Hamid Jahankhani, et al, 'Cybercrime classification and characteristics', (n 84)

execution of crime or about the identity of the criminal it becomes cyber crime.[93] In short, if computer is used but not used as the primary instrument of the crime, we can say that computer is involved as incidental to the commission of other crimes. Crimes such as money laundry, child pornography, unlawful banking transactions, organized crime records or books, and bookmaking will fall in this category.

Crime associated with the prevalence of computers: most of the times, crimes under this category are the result of the need to digitalize industrialization. Companies or any other body may use internet to distribute their product along with their logo.[94] Meanwhile, cyber criminals may counterfeit or copy other brand or image for the distribution of counterfeit products. Thus, such crimes involve technological growth that creates crime targets. Crimes such as piracy/ counterfeiting, copyright violation of computer programs, counterfeit equipment, black market computer equipment and programs, and theft of technological equipment will fall under this category.[95]

To sum up, given the absence of valid and sufficient statistics along with the dynamic (growing) nature of acts constituting cyber crime, it is almost impossible to know the exact number of acts of cyber crime and become hard to find a single and widely acceptable category. Thus, this researcher suggests the use of taxonomy of cyber crimes which is adopted in national legislations in tandem with classification employed under legislations having international character.

2.1.3. Extent and Impact of Cyber Crime

Nowadays it is not only the definitional matter of cyber crime that is very complex and unsettled but setting the exact extent and impact of cyber crime activity also unknown. This relates to lack of consensus as between scholars, governmental and non-governmental reports and researches. The aim of this paper is not to discuss these differences rather it is to make a quick overview of the extent and impact of cyber crime both internationally and domestically.

[93] What is computer crime? Available at https://www.geeksforgeeks.org/what-is-computer-crime [last accessed at 23/5/2022]

[94] The computer is a crime machine, available at https://www.hg.org/legal-articles/the-computer-is-a-crime-machine-21217 [last accessed at 23/5/2022]

[95] Hamid Jahankhani, et al, 'Cybercrime classification and characteristics', (n 84)

The rationale is enable law-enforcement agencies to advance anti-computer crime strategies, deter prospective attacks and enact apposite and effective legislation.

Currently Cyber crimes become a subject that poses a very real and tangible threat to the socio-economic and political matters of the global community. Scholars in this field recently estimated that about half of all property crime is now cyber crime.[96] The scale and complexity is wide ranging and reached the level of a global threat than any other crime. According to one study, financially motivated acts, such as computer-related fraud or forgery, make up around 1/3 of acts across almost all regions of the world. In England and Wales, criminal activity of fraud and computer abuse has reached more than 5 million in a single year.[97] Criminal acts against the confidentiality, integrity and accessibility of computer systems and content related acts make up 1/3 or more than 1/3 of the whole cyber crimes depending on the capacity of identifying the crime, reporting of the occurrence and level of prosecution across the globe. In terms of cost, as noted by Calif, if cyber crime measured as a country, the cost of cyber crime damages is estimated $6 trillion USD internationally in 2021.[98] Such costs consists damage and destruction of data, theft of intellectual property, fraud, stolen money, reputational harm, post-attack disruption to the business, hacking so and so on.[99]

Having clear and reliable information on the extent of the problem of cyber crime is a very tough and problematic task. Given the high number of under-reporting of cyber incidents either by individuals or companies and the application of different and complex parameters to evaluate the extent by government organs around the world, it is hard to accept every statistics and surveys on the extent of cyber crime. Due to such facts we are witnessing the fact that cyber crime incidents costs in trillions annually but the rate of successful cyber crime investigation are very few.

With regard to the impact of computer crime, a number of cyber attacks ranging from hacking and denial-of-services (DoS), to ransomware and spyware infections, and can affect everyone from the public to the critical national infrastructure of a country. This digital crime has

[96] https://legaljobs.ic/blog/cyber-crime-statistics [last accessed at 11/6/2022]

[97] https://www.pinsentmasons.com/out-law/news/extent-of-fraud-and-cyber-crime-laid-out-in-new-statistics [last accessed at 11/6/2022]

[98] https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016 [last accessed at 12/6/2022]

[99] Ibid

a number of social and psychological (emotional and behavioral) as well as economical impacts across the globe.[100] When we see the impact of cyber crime in relation to the global economy, it costs about $600 B every year within which the $160 of this loss to individual intellectual property theft and business damages.[101] Even though most of such incidents relates to lack of knowledge to the threat and lack of adequate preventive mechanisms, the development of advanced technologies and the low-level detection rate in most of countries due to low reporting and weak investigatory scheme also play a significant role in the prevalence of cyber crimes.

From the sociological perspective, the impact of computer crime has become extremely high. From a very recent time onward, humans across the globe has become highly dependent on computer and networking system in the way that every detail about family, himself/ herself, business and other secret issues are stored in computer.[102] This gives a fertile ground for criminal actors to engage with full capacity and get whatever they want with secured and untraceable manner. From individual theft of personal information or loss of secret data to the high level of societal interests such as power plant, financial services and other damages are caused by cyber crime.[103] The number of online terrorist and extremist activities causing wide range of mental and physical damages on the society in general is also another serious issue in cyber crime discussions. Given the unprecedented online malicious movements and unknown nature of the crime, the life's of billions of people around the world gets endangered.

2.2. International and National Legal Framework of Cyber Crime

The aim of this section is to make birds'-eye view of existing international, regional and national legal frameworks that set guideline on the prevention and investigation of cyber crime. Variety of international instruments contains provisions that address investigation and prevention of cyber crime and constitute a commitment on the part of the States parties to combat computer related acts (crimes). These provisions constitute an integral part of the international legal framework to combat cyber crime and calling on states to undertake for combating the

[100] Maria Bada, 'The Social and Psychological Impact of Cyber-Attacks', Cybercrime Centre, 2019; available at https://arxiv.org/ftp/arxiv/papers/1909/1909.13256.pdf [last accessed at 12/6/2022]

[101] https://www.sbir.gov/tutorials/cyber-security/tutorial-1 see also https://www.csis.org/analysis/economic-impact-cybercrime?amp= [last accessed at 12/6/2022]

[102] Cybercrime and its impact on society, available at https://studycorgi.com/cybercrime-and-its-impact-on-society/ [last accessed at 12/6/2022]

[103] Ibid

phenomenon. Besides, this section will also review the existing legal framework in Ethiopia dealing with administration, investigation and prevention of cyber crime.

2.2.1. International Legal Framework

Even though cyber crime is relatively new area of crime and governed by laws having national character for a long period of time, the last decade has seen significant developments in the promulgation of binding and nonbinding instruments aimed at countering cybercrime.

At international level, unfortunately, there is no convention or declaration that governs the prevention of cyber crime yet. Despite lack of agreement as between the member states, UN has announced its decision to work on developing convention on cyber crime. UN on Dec, 2019 has adopted Resolution 74/247 establishing an Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. One can understand how much this convention would become important in shaping and guiding cyber crime understanding, investigation and prevention as well as administration all around the world. Even if it is yet at negotiating stage, it is unknown the scope of the convention regarding what crimes should be specifically encoded in the treaty; and what this treaty might ultimately include: whether it focuses on cyber security, national security, or cyber warfare or cybercrime in the sense of either pure cyber crime or cyber-enabled acts. Though the nature and likely scope of the convention are unclear, the convention is expected to further enable international cooperation in the continuing and increasingly complex fight against cybercrime and expected to put definition for the term cyber-crime. The ad hoc committee has started its formal process in 2022.

However, there are plenty of resolutions that discuss the issue of cyber crime under the UN legal framework including but not limited to resolution on effective crime prevention and criminal justice responses to combat sexual exploitation of children adopted by the United Nations Office for Drugs and Crime (UNODC)[104] and the Commission on Crime Prevention and

[104] Commission on Crime Prevention and Criminal Justice Twenty-eighth session; available at https://www.unodc.org/documents/commissions/CCPCJ/CCPCJ_Sessions/CCPCJ_28/ECN152019_L3REv1_e_V1903716.pdf [last accessed at 13/6/2022]

Criminal Justice;[105] United Nations Economic and Social Council's resolutions on international cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes[106] and on the sale of licit drugs via the Internet that explicitly took account of a phenomenon related to a computer crime;[107] UN General Assembly's resolution wherein international community's endeavors to the enhancement of existing cooperation to prevent cyber crime were encouraged, fascinating advanced exploration of the feasibility of providing assistance to State parties in tackling cyber crime under the guidance of the UN, along with other organizations partnership.[108] UNGA also adopted resolutions 55/63[109] and 56/121[110] recalled by resolution 57/239 and 58/199[111] and both resolutions focuses on the need for international cooperation in fighting cybercrime for the better and effective fight against the criminal misuse of information technology.[112] With the adoption of resolution 55/63 UNGA identified variety of measures to prevent the misuse of information technology such as:

> States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies;[113]

[105] Resolution 16/2, available at: https://www.unodc.org/documents/commissions/CCPCJ/Crime_Resolutions/2000-2009/2007/CCPCJ/Resolution_16-2.pdf [last accessed at 13/6/2022]. The Commission on Crime Prevention and Criminal Justice (CCPCJ) was set up in 1991. It is a subsidiary body of the Economic and Social Council.

[106] ECOSOC Resolution 2004/26, on International cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes; available at https://www.unodc.org/documents/commissions/CCPCJ/Crime_Resolutions/2000-2009/2005/ECOSOC/Resolution_2004-26.pdf [last accessed at 13/6/2022]

[107] ECOSOC Resolution 2004/42, on Sale of internationally controlled licit drugs to individuals via the Internet; available at https://www.unodc.org/documents/commissions/CND/Drug_Resolutions/2000-2009/2004/ECOSOC_Res-2004-42.pdf [last accessed at 16/3/2022]

[108] UN General Assembly Resolution 60/177; available at https://www.unodc.org/documents/commissions/CCPCJ/Crime_Resolutions/20002009/2005/General_Assembly/A-RES-60-177.pdf

[109] UN General Assembly Resolution 55/63 on Combating the criminal misuse of information technologies; available at https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf [last accessed at 13/6/2022] [Hereinafter: UN General Assembly Resolution 55/63]

[110] UN General Assembly Resolution 56/121 on Combating the criminal misuse of information technologies; available at https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_56_121.pdf [last accessed at 13/6/2022]

[111] UNGA resolution 58/199 on Creation of a global culture of cyber security and the protection of critical information infrastructures; available at https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf and UNGA 57/239 Creation of a global culture of cyber security; available at https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf [last accessed at 13/6/2022]

[112] Ibid

[113] UN General Assembly Resolution 55/63 (n 109), art 1(a)

> Law enforcement cooperation in the investigation and prosecution of international cases of criminal misuse of information technologies should be coordinated among all concerned States;[114]

Domestic legislative development and capacity building along with cooperation across borders are the target areas of the GA in the adoption of this resolution.

Apart from regulation cyber crime incidents, the 2000 UN Convention on combating transnational Organized crime encourages state parties to use enhanced investigation techniques and tools with the view to facilitate and support the effectiveness of cyber crime investigation.[115] In conclusion, the international community is still yet to develop binding and agreeable legal instrument targeting cyber crime or the misuse of information technology.

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

Although the 1989 convention on the right of the child is concerned so much on the protection of the child from variety of abusive activities, it failed to elaborate one of the dangerous activity that affect the Childs' life in unspeakable manner the so called "child pornography". Nor it does contain provisions committing member states to criminalize the dissemination and distribution of online child pornography.

In order to fill such gaps, the convention is supported by the optional protocol to the convention adopted by A/RES/54/263 of 25 May 2000.[116] The protocol addresses issues concerning child pornography in general and the online distribution and dissemination of pornographic material.[117] Thus, even if the protocol is not genuinely an instrument forming cyber crime legal framework, it is useful in the criminalization of acts of child pornography involving cyber space and harmonization of the criminalization of the distribution of online child pornography. As we seen above, child pornography is one type of cyber crime accepted in a

[114] Id, art 1(b)

[115] Convention on combating transnational Organized crime, 2000, UNGA treaty series, res. 55/25; available at: https://www.unodc.org/documents/middleeastandnorthafrica/organized-crime/UNITED_NATIONS_CONVENTION_AGAINST_TRANSNATIONAL_ORGANIZED_CRIME_AND_THE_PROTOCOLS_THERETO.pdf [last accessed at 21/6/2022]

[116] Optional Protocol to the United Nations Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, UN, treaty series, vol. 2171, 2000, available at https://www.ohchr.org/Documents/ProfessionalInterest/crc-sale.pdf [last accessed at 11/6/2022] [Hereinafter: OPSC, 2000]

[117] OPSC, 2000

global scale. Therefore, such facts suggest how strong the optional protocol is in creating cyber crime legal framework at international level.

Article 2 of the protocol defines Child pornography as:

> Any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes[118]

As per the protocol, child pornography consists among others the recording and broadcasting of digital images. And this shows that the distribution and accessibility of pornographic materials through the internet is one of the target areas of the protocol.[119] Apart from that, the close reading of article 3(1(c)) suggests that state parties to the protocol are obliged to punish the possession of child pornography when it is verified that the possession is to produce, distribute, disseminate and the like.[120]

Moreover, the protocol also underscores the necessity of and the need of cooperation and mutual legal assistance in the prevention and investigation of the above mentioned criminal acts.[121] As per article 6 and 7 of the Optional protocol, state parties are required to be active in a great measure of mutual collaboration and assistance in connection with investigation and execution of any request of seizure and confiscation from another state party. Thus, such detailed stipulations of the protocol lay a basis for creating effective cyber crime investigation and prevention framework for member states in relation with child pornography.

2.2.2. Regional Legal Framework

Paradoxically to the international legal framework, regionally there are plenty of conventions and other binding and non-binding instruments dealing issues related to cybercrime.

2.2.2.1. The Council of Europe Convention on Cybercrime (Budapest convention)

After five years of discussions and deliberations on the proposal, the convention was adopted by the council of Europe so as to control, investigate and prevent crimes committed via

[118] Id, art 2(c)

[119] Handbook on the optional the Sale of Children, Child Prostitution and Child Pornography, UNICEF, 2009, available at https://www.unicef-irc.org/publications/pdf/optional_protocol_eng.pdf [last accessed at 11/6/2022]

[120] OPSC, 2000, (n 116), art 3(1(c))

[121] Id, article 5-7

the internet and other computer networks, dealing particularly with violation of network security, computer related fraud and infringements of copyright and entered in to force in 2004.[122] The convention has 66 member states as of May, 2022.[123] Even though a large number of members are from the council of Europe, given stipulation provided under article 37(1) of the convention which says "*...any State which is not a member of the Council and which has not participated in its elaboration to accede to* [the] *Convention"* non-member states to the council have become party to the convention. And this let the convention to be considered as an international model legal instrument on cyber crime even if it is not actually.

With the objectives of harmonizing domestic Laws on cyber crime and supporting investigations along with increasing international cooperation in combating cyber crime, the convention set an impressive framework consisting legislative measures important in the fight against computer crime.[124] Though the convention failed to define what cyber crimes mean, it provides a meaning to the term Computer System, Computer Data, Service Provider and Traffic data.[125] As it is described above, the convention classify cyber crime in to four categories taking, the nature of activities constituting cyber crime, in to consideration.

Most importantly, the convention consist provisions under chapter three which create a framework for international cooperation in the area of investigation of cyber crime incidents and extradition of criminals between parties to tackle cybercrime.[126] This instrument itself may be relied upon as the basis for requests for assistance from one state party to another.[127] As such, the instrument may also, without prejudice to conditions provided for by national law or other applicable mutual assistance treaties, set out the reasons for which a state party may refuse assistance.[128] It also provides procedural law tools to make the investigation of cybercrime and

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

[123] Convention on Cybercrime, 2001, Council of Europe, European Treaty Series - No. 185; at https://rm.coe.int/1680081561 [Last accessed at 15/7/2014]: see also The Budapest convention and its protocols: available at https://www.coe.int/en/web/cybercrime/the-budapest-convention [last accessed at 26/5/2022]

[124] Id, Preamble of the Convention

[125] Id, art 1 (a-d)

[126] Id, Chapter three of the convention article 23-35

[127] Id, article 27

[128] Budapest Convention (n 123), article 27

the securing of electronic evidence in relation to any crime more effective.[129] Thus, the convention plays a significant role in fostering the effectiveness of cyber crime investigation and prevention though providing 24/7 network enabling multilateral cooperation and sharing of important data relevant to tackle cyber crime incidents.

This convention is not the only instrument in the council of Europe but it is followed by protocol that support and upgrade the convention in the areas of criminalizing acts of a racist and xenophobic nature committed through computer systems.[130] The protocol mandates participating states to criminalize the racist and xenophobic-motivated threats and insults along with spreading of racist and xenophobic material through computer systems.[131]

The council of Europe also preparing another protocol named as "Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence" through cybercrime convention committee and the draft is approved by the committee on Nov 17, 2021 with the aim of extending the rule of law further into cyberspace, protect internet users, and help provide justice for those who become victims of crime.[132]

2.2.2.2. African Union Convention on Cyber Security and Personal Data Protection (Malabo convention)

The other most important regional legal instrument dealing issues related to combating cyber crime is the Malabo convention.[133] This convention was adopted in 2014 in Malabo, Equatorial Guinea in the presence of heads of 55 member states to the AU and as of March 2022, it is signed by 14 and ratified by 13 states.[134] In terms of scope, this convention is broader than the Budapest convention by which it concentrates on Electronic transactions, Personal data

[129] The Budapest Convention on Cybercrime: a framework for capacity building, available at https://thegfce.org/the-budapest-convention-on-cybercrime-a-framework-for-capacity-building [last accessed at 27/5/2022]

[130] Additional Protocol to the Convention on cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, council of Europe, European treaty series no. 189, 2003, available at https://rm.coe.int/168008160f

[131] Ibid

[132] Draft Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, approved by Committee of Ministers on 17 November 2021

[133] African Union Convention Cyber Security and Personal Data Protection, 2000, guided by the constitutive act of African union; at https://au.int/sites/default/files/treaties/29560-treaty0048__african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf [Last accessed at 15/7/2014]; [Hereinafter: Malabo convention]

[134] African Union, available at https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection [last accessed at 10/6/2022]

protection, Cyber security and cybercrime. In doing so, the convention envisions the continent (Africa) as a single entity concerning data protection and it urges more harmonized and independent legal framework having capacity to defend illegal activities related to data possession and control.

As explicitly stipulated under its preamble, the core objectives of the convention includes addressing the need for harmonized legislation in the area of cyber security and cyber crime in member states,[135] and acknowledging that cybercrime poses 'a real threat to the security of computer networks and the development of the information society in Africa.[136]

Despite the absence of definition for the term cyber crime, the convention attempt to criminalize acts having cyber crime nature and urges member states to adopt legislations and/or regulatory measures against criminal offences that affect the integrity, confidentiality, availability and survival of ICTs.[137] Such stipulations of the convention is supported by the argument presented by the AU which says that *"national legislation cannot be drafted in isolation and national governments must seek to harmonize national legislation, regulations, standards and guidelines on cybercrime issues"* [emphasis added].[138] Besides, the convention under article 31 (3) provide for a sub-set of procedural powers that are useful for investigating and prosecuting cybercrime and securing electronic evidence in domestic investigations which should be applied by member states.

In comparison with Budapest convention, this convention (Malabo) criminalizes most of the conduct which is considered as cybercrime and electronic evidence foreseen under the CoE convention.[139] Hence, most of the provisions that are included in the Malabo Convention are largely not inconsistence with that of Budapest Convention. Especially the criminalization of an illegal use of computer data is going beyond the standards defined by most other regional instruments including but not limited to Budapest convention.

[135] Malabo convention (n 133), Preamble Para 13

[136] Id, Preamble Para 15

[137] Id, art 25

[138] African Union, 'A global approach on cyber security and cybercrime in Africa', available at https://au.int/sites/defualt/files/newsevents/workingdocuments/31357-wd-a_common_african_approach_on_cybersecurity_and_cybercrime_en_final_web_site [last accessed at10/6/2022]

[139] Malabo convention (n 133), art 29

In conclusion, though the 2014 Malabo convention is not a convention that focuses chiefly on cybercrime, it incorporate various legal provisions relevant for the administration, prevention and investigation of cyber crime and it also it provides that states should make sure their efforts in fight against cybercrime could be harmonized regionally[140] and are encouraged to sign mutual assistance treaty if they don't already have one.[141]

In addition to Malabo convention, there are a number of sub regional binding and non-binding legal instruments that focuses on cyber crime. To mention but few: Economic Community of West African States (ECOWAS) Directive on Fighting Cybercrime.[142] ECOWAS is a sub regional organization consisting 15 West African countries established to promote economic integration in the region.[143] As one of the most active regional organization in the area of combating cyber crime, it adopted a legally binding act referred as Directive on Fighting Cybercrime in August 2011.[144] In addition to Directive on Fighting Cybercrime, the organization also adopted a legally binding and highly influenced by the EU data protection directive (95/46/EC) which is referred as Supplementary Act on Personal Data Protection.[145] Chiefly, both instruments work for the harmonization regional and national legislation on the fight against cyber crime and facilitate the cooperation between member states so as to improve capacity for fighting well against cyber crime.[146]

East African Community Draft Legal Framework for Cyber laws is the other instrument prepared by EAC with the aim of urging member states to the community reforming their national laws to facilitate electronic commerce, facilitate the use of data security mechanisms, to protect individual consumers' privacy in an online environment and to deter conduct against the confidentiality, integrity and availability of information and communication technology.[147]

[140] Id, art 28(1)
[141] Id, art 28(2)
[142] Economic Community of West African States directive C/DIR. 1/08/11 on fighting cyber crime with ECOWAS, 66th ordinary session of the council of ministers, 2011; available at https://issafrica.org/ctafrica/uploads/Directive%201:08:01%0on%20fighting%20Cyber%20Crime%20within%20ECOWAS.pdf [last accessed at 16/6/2022] [Hereinafter: Economic Community of West African States directive]
[143] Ibid
[144] Economic Community of West African States directive, (n 142)
[145] Economic Community of West African States; available at https://ccdcoe.org/organizations/ecowas/ [last accessed at 16/6/2022]
[146] Ibid
[147] United nations conference on trade and development, Draft legal framework for cyber laws, 2008; available at http://repository.eac.int/handle/11671/1815 [last accessed at 16/6/2022]

Though it is non-binding instrument, it is very useful for member states through harmonizing law reform mechanisms and shaping activities to be in line with international best practices.

There are also other instruments such as the 2011 Cyber Security Draft Model enacted by Common Market for Eastern and Southern Africa (COMESA)[148] and the 2012 Southern African Development Community Model Law on Computer Crime and Cybercrime.[149]

All of these instruments have been important to legislate and bring about worldwide harmony and collaboration on the issue of cybercrime at sub regional level and given their active and more flexible trait, they are very relevant in increasing the possibility member states of the community joining international and other regional cyber crime initiatives.

2.2.3. The Legal and Policy Framework of Cyber Crime in Ethiopia

2.2.3.1. The Policy Framework

With regards to policy measures to cyber crime, the fight against cyber crime in Ethiopia is supported and authorized by a number of policies that are enacted since 2009. These policies are: the 2011 criminal justice policy, 2011 national information security policy and 2009 national ICT policy and strategy. As per these policies, Ethiopia is vulnerable to cybercrime and the government is duty bound to enhance confidence and trust within the public, as well as to protect both data and network integrity.[150] Thus, so as to answer the urgency in reducing the threats and vulnerabilities, it has become important to formulate comprehensive national strategy, adoption of appropriate legislations, and promotion and strengthening of international cooperation to prevent, detect, investigate, and prosecute cybercrimes. Moreover, this shows the readiness and commitment of the government to combat computer crime at all level.[151]

2.2.3.2. The Legal Framework

Despite the existence of a number of legislations in relation to combating cyber crime in Ethiopia, the incorporation of cyber crime in legal documents dates back to 2004 when the current criminal code was enacted. As the first instrument having set of provisions about cyber

[148] Steven, Malby et al, Comprehensive Study on Cybercrime, (n 19), P. 64

[149] Ibid

[150] Federal Democratic Republic of Ethiopia national ICT policy and strategy, 2009, preamble

[151] Federal Democratic Republic of Ethiopia, Criminal Justice Policy Ministry of Justice, Addis Ababa, 2011; available at: https://www.abyssinialaw.com/online-resources/policies-and-strategies/criminal-justice-policy-amharic/viewdocument/1553 [last accessed at 17/6/2022]

crime, it criminalizes only three types of computer crimes namely ‘hacking’, ‘dissemination of malware’ and ‘denial of service attacks (DoS)’.[152] From the reading of the section where these provisions are incorporated one can understand that the code treat such crimes as ‘Crimes against Rights in Property’.[153] All these crimes are punishable when they are committed without authorization to do so. And any adding and abetting commission of computer crime will also entail criminal liability in the name of cyber crime. Besides, the code also criminalizes acts perpetrated with the view to ‘facilitate the commission of computer crime.[154] Thus, given the inadequate nature of the criminal code in terms of quantity of acts punishable as cyber crime, manner of incorporation of the existing criminal acts and absence of procedural and evidentiary provisions for the effective investigation and prosecution of these crimes, the legislator has started the enactment of new law specifically focuses on computer crimes and the HPR enacted this law in 2016 as Computer crime proclamation no. 958/ 2016.

The coming in to force of proclamation no. 958/ 2016 reveals a major reform that has been taken place in computer crime area of criminal code. To mention but few of these reforms, it defines the basic terms in relation to computer crimes such as ‘computer crime’, ‘communication service’, ‘network’, ‘computer system’, ‘traffic data’, ‘computer data’ and ‘computer program’.[155]

In addition to that, it broadens the scope of acts considered as computer crimes and puts these crimes in a very elaborate manner. In part two section one under the category of crimes against computer system and computer data it criminalizes illegal access, illegal interception, interference with computer system, causing damage to computer data, criminal acts related to usage of computer data and services, along with aggravation circumstances.[156] Under section two, acts such as computer related forgery, computer related fraud, and electronic identity theft are criminalized as ‘computer-related forgery, fraud and theft’;[157] obscene or indecent crimes committed against minors, crimes against reputation and liberty of persons, crimes against public security, dissemination of advertisement through computer system, illegal computer content

[152] The Criminal Code of the Federal Democratic Republic of Ethiopia, 2004, Federal Negarit Gazzeta, Proc. No. 414, arts 706, 707 and 708 respectively.

[153] Ibid

[154] Id, art 709

[155] Computer Crime Proclamation, (n 21), art 2

[156] Id, part 2 section 1 (3-8)

[157] Id, section 2 (9-11)

dissemination by service provider through computer system are criminalized as 'illegal content data' crimes under section three part two of the proclamation.[158] At last, the proclamation stated miscellanies provision under the category of 'other offences'.[159] Only those four crimes under the fist category are existed in criminal code and all other crimes are new. In doing so, the proclamation also tries to solve the problem in relation with adequate procedural and evidentiary matters and incorporate provisions of detailed procedural and evidentiary rules relevant for investigating and prosecuting Cyber crimes. This researcher believes that, given the volatile and fragile as well as the digital oriented nature of cyber crime related evidences, the separate and cooperative way of governance of digital evidences which consists identifying, collecting, acquiring and preserving evidences is an important and a great step taken by the government. Such separate governance of the procedural and evidentiary issues of computer crime should be continued despite the enactment of the current draft criminal procedure and evidence law.

Despite the absence of clear cut stipulation about the need to harmonize the provisions of the proclamation in line with international and regional human right and cyber crime instrument, the preamble of the proclamation stated that the enactment of cyber crime law is the result of the need to incorporate new legal mechanisms and procedures in order to prevent, control, investigate and prosecute cybercrimes. The preamble of the proclamation stated that:

> [T]he existing laws are not adequately tuned with the technological changes and are not sufficient to prevent, control, investigate and prosecute the suspects of computer crimes;

The other important area of development in cyber crime legislation is the power that is given for Federal attorney to engage in international cooperation with other countries in the investigation and prevention of computer crime.[160] This move of the proclamation fills the gap that exists in the criminal code and facilitates the effective implementation of the provisions of the proclamation.

Regarding investigation of cyber crime incidents, the proclamation gives the joint investigative power for police officers of federal police commission and public prosecutors. Despite the joint power entitled to both institutions, the public prosecutor is empowered to lead the cyber crime

[158] Id, section 3 (12-16)
[159] Id, section 4 (art 17-20)
[160] Computer Crime Proclamation, (n 21), art 42

investigation process.[161] Besides, the proclamation empowers INSA to provide technical assistances whenever requested by investigatory organs.[162] INSA also authorized to conduct sudden searches, conduct digital forensic investigation, provide appropriate security equipment or take other similar measures on computers, computer systems or infrastructures.[163]

Besides, as the preamble indicates, one of the issues that trigger the enactment of this law is the need to modernize laws dealing with investigation and prevention of cyber crimes. To this effect, in addition to traditional criminal investigation measures practiced on the basis of the 1961 criminal procedure code, it incorporates a number of Special Investigation Techniques that enables law enforcement organs to effectively investigate computer crimes. The proclamation under article 25(1) stated that:

> to prevent computer crimes and collect evidence related information, the investigatory organ may, request court warrant to intercept in real-time or conduct surveillance, on computer data, data processing service, or internet and other related communications of suspects, and the court shall decide and determine a relevant organ that could execute interception or surveillance as necessary

Accordingly, the investigative organs – the public prosecutor and the police[164] - are permitted to use various form of SITs so as to prevent the commission of computer crimes. Techniques such as interception and different form of surveillances are recognized and those investigative organs can apply them when the court authorized to do so.[165] The proclamation also stated that the Attorney General's approval of the use of SITs must be supported by the inability or insufficiency of conventional investigation method and it must be sure about the fact that *"no other means readily available for collecting such data"*.[166] Thus, one can understand that as it is required in a number of instruments this proclamation also underscores that the use of SITs is not a principle but is an exception by which it could be employed only in a limited circumstances with the oversight of both court of law and attorney general. Within these exceptional scenarios, the Attorney General is empowered to determine the use of SITs without court authorization *"where there are reasonable grounds and urgent cases"*.[167] However, this doesn't mean that it is

[161] Id, article 23(1)
[162] Id, article 23(2)
[163] Id, article 26(1)
[164] Computer crime proclamation, 2016, (n 21), art 23 (1)
[165] Id, art 25 (1)
[166] Id, sub art (2)
[167] Id, sub art (3)

the discretionary power of AG rather it is required to provide its reasons within 48 hours to the president of FHC.[168]

In addition, the proclamation also provides provisions dealing the search, seizure of computer data or systems[169] as well as admissibility[170] and authentication[171] of electronic evidences collected by investigatory organs.

Therefore, this proclamation has been used as an instrument governing every activity in relation with administration, prevention, investigation and apprehension of cyber crime and cyber criminals in Ethiopia. It is also used as both the substantive and procedural legal document concerning cyber crime.

In addition to the 2016 computer crime proclamation, there are other pieces of legislations incorporating cyber crime provisions and lay some foundations in the fight against cyber crime. These are: Telecom Fraud Proclamation No. 761/2012,[172] which criminalized the interception of, access of and interference with telecommunication networks, services, or systems without authorization. The other instrument is Proclamation No. 760/2012[173] which criminalizes cyber-related malicious activities such as the forgery, falsification, or unlawful accessing of identity cards or certificates of registration of vital events. The proclamation also stated that information shall be protected from electronically designed attacks, theft, or from other similar criminal abuse.[174] Besides, The National Payment System Proclamation No.718/2011[175] also criminalizes forgery and fraud related activities, specifically forgery of and fraud with payment instruments. But, it looks more of conventional financial-related forgery and fraud crimes.[176]

[168] Id, sub art (4)
[169] Id, art 32
[170] Id, art 33
[171] Id, art 34-35
[172] Telecom Fraud Proclamation, 2012, Federal Negarit Gazzeta, Proc. No. 761,18th year, No. 61
[173] Registration of vital events and national identity card proclamation, 2012, Federal Negarit Gazzeta, Proc. No. 760, 18th year, No. 58
[174] Id, art 65
[175] National Payment System Proclamation, 2011, Federal Negarit Gazzeta, Proc. No. 718, 17th year, No. 84
[176] Id, art 35

2.3. Institutional Setup

2.3.1. Information Network and Security Administration

INSA is an autonomous federal institution that was established in 2006 as a primary organ that works on cyber-security issues of the country. Pursuant to its establishing CoM regulation no. 130/ 2006, the chief objective of the agency is to defend the country's information infrastructure from potential cyber attacks.[177] Even though it was accountable to the PM, as per the new 1097/ 2018 proclamation art 33(4(b)), the NISS is made accountable to the Ministry of Peace.

The re-establishing proclamation no. 808/ 2013 also stated that the administration was established to work on securing and protecting the country's interests, infrastructures, the cyber-space, individual's interest, and information from any domestic and foreign cyber-related attacks. The proclamation in a brief manner stipulates the power and functions of the administration. The power entrusted to the administration is:[178] to provide assistance and support, in respect of preventing and investigating cyber crimes, to police and other organs empowered by law; take all necessary counter measures to defend any cyber or electromagnetic attacks on information and computer based infrastructures or systems or on citizens' psychology; draft national policies, laws, standards and strategies that enable to ensure information and computer based key infrastructures security, and oversight their enforcement upon approval; collect, analyze and disseminate to the concerned authorities, information on selected trans-boundary national security threat activities; and provide support to security organs; develop and implement research and study based information and computer based critical infrastructure's security products and services; regulate cryptographic products and their transaction, set necessary criteria and develop operating procedures, develop and implement cryptography infrastructure; build information technology testing and evaluation laboratory center; and the like. The proclamation also stated a number of duties and powers to the director general of the agency.[179]

[177] Information Network and Security Agency Establishment Council of Ministers Regulations, 2006, Federal Negarit Gazette, Reg. no 130, 13th year, no 5, art 5

[178] Proclamation to re-establish Information Network and Security Agency, 2013, Federal Negarit Gazette, proc. no 808, 20th year, no 6, art 8

[179] Ibid

Besides, the 2016 computer crime proclamation also provided that the administration will undertake functions including providing technical support, conduct analysis on collected information, and providing evidences if necessary up on the demand of the investigatory organs.[180] And, mandated to establish online computer crimes investigation system and provide other necessary investigation technologies.[181] Moreover, pursuant to article 26 of the proclamation, INSA is also authorized to conduct sudden searches, conduct digital forensic investigation, provide appropriate security equipment or take other similar measures on computers, computer systems or infrastructures.

Ethiopian Cyber Emergency Readiness and Response Team

Ethio-CERRT is the other most important organ in the fight against cyber crime. The team is under INSA and established with the mission to create a secure, reliable and enabling Ethiopian cyber space by coordinating and building national capacity of proactive readiness and effective incident response centered on analysis.[182][183] The main functions of the team includes:[184] monitor national cyber security 24/7; accept cyber attack complaint; conduct malware and intrusion analysis to identify attack causes and extract signatures; conduct investigation on cyber attacks; prepare and provide cyber security statistics at national level for policy makers; conduct regular risk assessment and identify vulnerability; assure performance of cyber security products based on standards; assure capacity of cyber security professionals based on standards; watch the technology and update professionals; provide education on cyber-attack to concerned bodies; train cyber security professionals regularly and certify; deploy the necessary infrastructure; create global relationship.

2.3.2. National Intelligence and Security Service

The other institution sharing some similar tasks with INSA is the NISS. NISS is an intelligence aimed institution tasked with gathering information of national interests. Pursuant to the new 1097/ 2018 proclamation art 33(4(a)), the NISS is made accountable to the Ministry of

[180] Computer Crime Proclamation, (n 21), art 23(2)

[181] Id, art 39

[182] https://www.africacert.org/ethiopia/ [last accessed at 29/6/2022]

[183] https://www.coe.int/en/web/octopus/country-wiki-ap/-/asset_publisher/CmDb7M4RGb4Z/content/ethiopia?_101_INSTANCE_CmDb7M4RGb4Z_viewMode=view/ [last accessed at 29/6/2022]

[184] https://ethiocert.insa.gov.et/web/guest/about-us [last accessed at 29/6/2022]

Peace. Though this institution is established to protect and defend the sovereignty of the country and the constitutional order by strengthening national intelligence and security service, it is also vested with powers that have some cybercrime implication.[185] Pursuant to article 7 sub 1 of the re-establishing proclamation, NISS have the power and mandate to lead the work of intelligence and security service that have both domestic and international character.[186] So, cybercrime also fall in this category of tasks of the NISS. Among the powers enumerated under article 8 of the proclamation, the power stipulated under sub 1 and 4 have a clear cyber crime implication.[187] And most importantly, the power to: follow up and investigate espionage activity against the interest of the country and its people, collect information and undertake counter-espionage activity; and follow up and collect intelligence and evidence on other serious crimes which are threats to the national interest and security, and work in collaboration with other relevant organ is directly related with cyber crime investigation and prevention.[188] In addition to that, the NISS is also has a power to employ one of the SITs – surveillance – with the court authorization so as to perform its tasks.[189]

2.3.3. Ministry of Justice: Attorney General

The other most important organ in the fight against cyber crime is department of attorney general. Pursuant to proc no 943/2016, the FAG is empowered to lead, coordinate and follow up criminal investigation function of federal police.[190] These are not the only power and duties stated under the proclamation but there are other crucial powers and duties enumerated under article 6 of the proclamation.

Besides, the FAG is tasked to the prosecution of alleged crimes with a view to protect the public's peace and security in a uniform, effective and efficient manner.[191] Both its establishment proclamation and computer crime proclamation stipulates a number of power and function. As

[185] National Intelligence and Security Service Reestablishment Proclamation, 2013, Federal Negarit Gazette, Proc. 804, 19th year, no. 55 [Hereinafter: National Intelligence and Security Service Reestablishment Proclamation]

[186]Id, Art. 7(1)

[187] Id, sub art 1-4

[188] National Intelligence and Security Service Reestablishment Proclamation, (n 199], sub art 1-4

[189] Id, sub art 5

[190] Federal Attorney General Establishment Proclamation, 2016, Federal Negarit Gazette, Proc. 943, 22nd year, no. 62, art 6

[191] Id, par 1

per proc no. 958/ 2016, the public prosecutor is one of the organs that are mandated to conduct the investigation and prosecution tasks. Within this function, the public prosecutor is a leading organ of every cyber crime investigation.[192] Besides, it is also empowered to: follows up computer crime cases and enforces and causes to enforce the provisions of this proclamation;[193] organize separate specialized task units when necessary to follow up computer crimes;[194] cooperate or enter in to an agreement with the competent authority of another country in matters concerning computer crime, including the exchange of information, joint investigations, and extradition and other assistances; and exchange information with institutions of another country having similar mission, perform joint cooperation in other forms or sign agreement with institutions of another country, when necessary.[195]

The FAG has a directorate office referred as "International Cooperation on Legal Affairs Directorate". The directorate is established for the purpose, among others, of coordinating activities involving international cooperation with respect to criminal matters. In doing this, the main mission, to mention but one, is to conclude agreements in criminal matters with selected foreign countries work for the creation of effective and efficient international judicial legal cooperation with others.[196]

In addition, the FAG has a directorate named as "Organized and Trans-national as well as National Affairs Criminal Matters Directorate" the directorate has the power to investigate and prosecute cases related to computer crimes. The prosecution of every computer crime and related offences and the joint investigation power bestowed under the computer crime proclamation is implemented by public prosecutors within this directorate. Moreover, the FAG also empowered to approve and decide whether investigatory organs can use special investigation techniques for cyber crime investigation or not with the duty to present the reasons for his/ her decision to do so.[197] This power of the FAG is also covers the power to decide the immediate destruction of any

[192] Computer Crime Proclamation, (n 21), art 23(1)
[193] Id, art 38(1)
[194] Id, sub art 2
[195] Computer Crime Proclamation, (n 21), art 42
[196] A Proclamation to provide Definition of Powers and Duties of the Executive Organs of the Federal Democratic Republic of Ethiopia, 2015, Federal Negarit Gazette, Proc. no 916, 22nd year, no 12, article 16(14); see also Computer Crime Proclamation, (n 21), art 42(1)
[197] Computer Crime Proclamation, (n 21), art 25(2) and (3)

irrelevant information collected through SITs.[198] The FAG is also, in collaboration with the police, empowered to organize specialized task unite for the necessary follow up of cyber crime incidents.[199] Not only that, the AG is appointed to lead the national executing task force which comprises the FAG, FPC and other relevant bodies with the aim of prevention and control of cyber crimes.[200]

2.3.4. Federal Police Commission: Federal Crimes Investigation Office

FPC is an autonomous federal institution vested with the power of investigation of crimes, and the backbone in the detection and prevention of crimes and apprehensions of alleged criminals in Ethiopia. As one of law enforcement organs, FPC always conducts investigation and prevention works with the aim of maintaining and ensuring peace and security of the public as well as the state.[201] In addition of powers and duties stipulated in its Establishment Proclamation No. 720/2011, FPC also vested the power to investigate computer crime incidents in conjunction with public prosecutors. Pursuant to proc no. 720/ 2011, the FPC is empowered to investigate crimes in relation with computer systems and information network.[202] The computer crime proclamation also empowers the police to follow up alleged cyber crimes either by themselves or by establishing specialized units. As article 23 (1) clearly stated, the police is one of the two institution designated as investigatory organ of the government in relation with computer crimes. Thus, every cyber crime incidents are prevented, investigated and apprehended by the joint work of FPC and FAG.[203]

Federal Crime Investigation Office is the specific office within FPC specifically tasked to investigate all crimes under the jurisdiction of the federal government. FCIO is composed of a number of divisions working on various criminal aspects. Among these divisions, Cyber Crime investigation Division is a division tasked with the investigation of cyber crime incidents that are requested either by the federal or state law enforcement organs. The division was established in

[198] Id, sub art 5
[199] Id, art 38(2)
[200] Id, art 41(2)
[201] Ethiopian Federal Police Establishment Proclamation, 2011, Federal Negarit Gazette, Proc. 720, 18th year, No. 2, preamble, par 1
[202] Id, art 6(5(b))
[203] Computer Crime Proclamation, (n 21), art 23

2004 with the support of the USA Federal Bureau of Investigation (FBI).[204] Nationally, the division was supported and trained by the INSA for the effective investigation and prevention of cyber crimes. In Ethiopia, this division is the only division that works on cyber crime cases and every cyber crime related investigations and follow ups passes through this division.[205] The division is composed of only 5 active member within which 1 of them are the team leader.

2.3.5. Other Concerned Institutions

In addition to the above institutions, there are institutions such as Minister of Foreign Affairs; Minister of Innovation and Technology; and Federal High Court (FHC) having some sort of powers and functions in relation with the prevention, detection and investigation of cyber-related crimes. Pursuant to the cumulative reading of article 4(17) and 11(2(c)) of proc no 1234/ 2021 with article 40 of computer crime proclamation, the FHC is entitled the first instance jurisdiction over any computer crime matters.[206] Thus, any cyber crime and related cases will be entertained in federal courts as it is designated as a federal matter by the above mentioned laws. Given the high importance of engaging in mutual legal assistance (MLA) initiatives and agreements for the better achievement of cyber crime investigation and prevention work, the Minister of Foreign Affairs is vested powers having MLA in cyber crime implication.[207] Proc no 1097/ 2018 empowers MFA to: coordinate all relations of other government organs with foreign states and international organizations;[208] and negotiate and sign, upon approval by the government, treaties that Ethiopia enters into with other states and international organizations; and affect all formalities of ratification of treaties.[209] Thus, on the basis of such powers, MFA is expected to accelerate the countries involvement in MLA initiatives in collaboration with other concerned organs designated to such tasks. Minister of Innovation and Technology (MIT) is established through proc no 1097/ 2018 with the aim of maintaining sustainable development by

[204] Iyasu, Cybercrime in Ethiopia, (n 14), P. 51

[205] Ibid

[206] Federal Courts Proclamation, 2021, Federal Negarit Gazette, Proc. 1234, 27th year, No. 26, art 4 (17) and 11(2(c)) and Computer Crime Proclamation, (n 21), art 40

[207] A Proclamation to provide Definition of Powers and Duties of the Executive Organs of the Federal Democratic Republic of Ethiopia, (n 196), art 15

[208] Id, sub art 8

[209] Id, sub art 3

creating an enabling environment for innovation.[210] The minister, chiefly, mandated to determine standards to ensure the quality, safety and security of information technology services in coordination with the concerned bodies and monitors their implementation as well as support capacity building in ICT.[211] Thus, MIT works with the above mentioned concerned organs in the prevention of cyber crime incidents so as to ensure the preservation of the safety and security of ICT services.

[210] Id, art 20

[211] Id, sub art c

CHAPTER THREE:
LEGAL AND PRACTICAL CHALLENGES TO THE EFFECTIVE PREVENTION AND INVESTIGATION OF CYBER CRIME - FINDINGS AND DISCUSSIONS

INTRODUCTION

The term "effectiveness" is defined as the degree to which the targeted objectives are met. In this chapter, factors that hindered the effective prevention and investigation of cyber crime incidents are identified and substantiated. Thus, findings of this thesis focus on the legal gaps and practical challenges to the effectiveness of the prevention and investigation of computer crime in Ethiopia.

3.1. Legal Challenges

3.1.1. Ambiguities on the Definition of "Computer Crime"

Crutchfield once stated that the process of defining crimes is one step ahead to control or prevent its occurrence.[212] Thus, every attempt to regulate cyber crime across the globe starts with giving definition for the term. In Ethiopia, though the regulation of computer crimes dates back to the 2004 Criminal Code, the term computer crime has got its definition in the 2016 computer crime proclamation.[213] Even if the legislator made a great move towards defining the term Cyber crime, the definition still lacks clarity and hampers the effective prevention of the crime.

Under article 2 (1) of the proclamation, it is stated that:

> In this Proclamation unless the context otherwise requires: "Computer crime" means a) A crime committed against a computer, computer system, computer data or computer network; b) A conventional crime committed by means of a computer, computer system, computer data or computer network; or c) Illegal computer content data disseminated through a computer, computer system, or computer network;[214]

This definition lacks clarity and opens door for interpretations. The ambiguity within this definition arises from the second line of definition related with conventional crimes.

[212] Crutchfield R., Crime: Readings (n 63), P. 7
[213] Computer Crime Proclamation, (n 21), art 2 (1)
[214] Ibid

According to the definition,

> A conventional crime committed by means of a computer, computer system, computer data or computer network.[215]

Such a definition is very problematic and open doors for various formats of interpretation. Among the difficulties of this broad definition, it would, for instance, cover traditional crimes such as murder, if perchance the offender used a keyboard to hit and kill the victim. In what instance could the murder or any kind of body injury be considered as computer crime. In its narrower interpretation, it talks about ordinary crimes committed through the instrumentality of software part of a computer which is referred as computer system and the network such as fraud, theft, and others.

Unless the legislator provided the definition in a clear and precise manner, the involvement of the hardware part of a computer in the commission of any of conventional crimes would result the commission of computer crime. From the international best practice perspective, such a definition is very broad and impact every facets of prevention and reduction of the computer crimes. In a number of legal instruments including but not limited to Budapest convention,[216] such category of computer crime is referred as computer-related crimes consisting computer-related fraud, forgery, identity theft and the like. In addition to lack of definitional clarity, Ethiopian government's failure to work hand-in-hand with the international community worsens the problem in this regard.

3.1.2. Lack of Sufficient Coverage of Crimes

Indeed, the new computer crime proclamation has come up with a long list of criminal activities and is deep in criminalizing such acts. And this proclamation compared with its predecessor - the 2004 criminal code, it is more comprehensive and organized in governing both the substantive and procedural as well as evidentiary issues of cyber crimes. However, it is still not adequate enough to be all-inclusive cyber crime law and cover acts criminalized in other jurisdictions and in laws having international nature.

[215] Computer Crime Proclamation, (n 21),, 2nd paragraph

[216] Convention on Cybercrime, 2001, Council of Europe, European Treaty Series - No. 185, articles 2-5.; at https://rm.coe.int/1680081561 [Last accessed at 15/7/2014]

The proclamation doesn’t criminalize crimes such as racist and xenophobic content, revenge pornography, IPR crimes and crimes related with large-scale cyber attacks. Some writers argues that some of these crimes are exists in the proclamation and other laws currently applicable in Ethiopia.[217] For instance, they argue that racist and xenophobic content crimes are criminalized under the Hate speech and Disinformation proclamation and 14 of computer crime proclamation. However, from the perspective of having comprehensive and up-to-date legal framework, criminalizing such complex crimes in scattered manner and through interpretation isn’t adequate.

The proclamation failed to criminalize the act of revenge pornography. Revenge pornography is defined as *“sexually explicit images or videos, made with consent of the depicted individual, posted online and make accessible without that person’s volition especially as form revenge”*[emphasis added].[218] The criminal element of this act is the publication of images or videos on the internet and make accessible to anyone through their computer system and network with the intent to cause distress the victim. This act is criminalized in a number of countries:[219] in England and Wales (section 33 of criminal justice and courts act 2015); Germany (general data protection regulation 679/2016); France (digital public act); Canada (section 162.1, criminal code through bill C-13); and Israel (prevention of sexual harassment law). But, there is no legal stipulation criminalizing this act in our country including proclamation 958/2016. This new computer crime proclamation only address obscenity and child pornography under art 12 in deep and broad manner and shows how much focus is given for the prevention of such acts. But, even if the victim seems the person whose images or videos posted only, its danger and impact, in the current state of social media usage in our country, is unspeakable.

With regards to intellectual property rights protection, it seems that the government leaves the matter to the 2004 copyrights and neighboring protection proclamation.[220] And, the broad interpretation of article 14 of proc no 410/2004 suggest that IPRs in relation with computer programs or software’s are protected.[221] But, it is very far from covering the current

[217] Kinfe, Micheal, ‘Some Remarks on Ethiopia’s New Cybercrime Legislation, (n 57), P. 455

[218] Marthe Goudsmit, *Revenge pornography: a conceptual analysis understanding a crime of disclosure*, Master’s thesis, Leiden university, Master of Philosophy, 2017, P. 23

[219] Country-wise legislation on “revenge pornography” laws; https://cis-india.org/internet-governance/files/revenge-porn-laws-across-the-world/view [last accessed at 5/9/2022]

[220] Copyrights and neighboring protection proclamation, 2004, Fed. Neg. Gaz., proc no 410, 10th year No. 55, art 14 [Hereinafter: Copyrights and neighboring protection proclamation]

[221] Copyrights and neighboring protection proclamation, (n 220)

developments in the areas of computer programs or software and the usage of computer system and networks. The new computer crime proclamation, starting from its definition, also lacks direct stipulation prohibiting illegal acts related to IPRs. Most importantly, there is no provision in the computer crime proclamation prohibiting illegal acts of unauthorized reproduction of products of fifth generation computers systems such as semiconductor topographies, computer databases and the like. Countries such as Germany, France, Denmark, USA, Spain, Sweden, and the United Kingdom developed laws dealing with such products and among other punishes the infringement of a circuit layout rights.[222] In Ethiopia, we are witnessing the high level of technological development in all areas of computer software and computer-related technology including artificial intelligence. But, the legal framework in this area is inadequate and affects the effective prevention of illegal cyber-enabled or cyber related activities against IPRs.

3.1.3. Inadequacy of Laws on Filtering and Blocking mechanisms

In addition to lack of sufficient coverage of newly developed criminal activities, there is also a gap in developing filtering or/ and blocking mechanisms as to some serious criminal activities. From the international best practice perspective, the development of cyber crime laws also supported with the enactment of adequate legislation creating obligation on crucial service providers or other specialized organs to filter or/ and block some cyber crimes which the criminals can rarely be traced, investigated and prosecuted.

One of these crimes, for example, is the crime stipulated under article 12 of 958/2016 which deals about the prohibition of production, sale, distribution, making available or possession without authorization any picture, poster, video or image having pornographic and obscene or indecent nature. Nowadays, due to the use of virtual currencies and anonymous payment, and the use sophisticated encryption technology to protect information stored on their hard disks by the perpetrators, challenges the investigation and prosecution process. In addition, criminals also employ anonymous online currencies with the intent to restrict the ability of law enforcement to identify suspects by following money transfers.

However, in Ethiopia, cyber crime laws focuses on as to how to investigate and prosecute cyber crime incidents but no legal mechanism developed as to how, who and what to be blocked,

[222] Critical look at the regulation of cybercrime; available at: https://www.ie-ei.eu/IE-EI/Ressources/file/biblio/Criticallookattheregulationofcybercrime [last accessed at 6/9/2022]

filtered and taken down. The presence of such kind of procedural law in relation to illegal, offensive and harmful content cyber crimes is of a great importance in the prevention and reduction of crimes problematic to easily investigate and prosecute. The only mechanism by which such illegal and harmful contents are blocked or filtered is when the government instructs Ethio-telecom to block the website totally. However, such procedure is not supported by a comprehensive and organized law and mostly, brings its own controversies. Besides, the number of telecom service providers also increasing after the privatization of telecom service and non-governmental organizations also taking part in providing services. Due to this fact, these telecom service providers may not easily accept any decision to block websites.

The only mandate of service providers in this regard is the duty to report stated under article 27 of 958/2016. As per this provision service providers are mandated to report the commission of crimes listed in the proclamation when they knows the dissemination of illegal content data. Thus, the absence of adequate or known procedural law that governs the manner by which illegal content data blocked, filtered and taken down brings a challenge in the effective prevention of cyber crimes.

3.1.4. Failure to be Part of International Legal Initiatives

One of the peculiar features of cyber crime is its cross-border nature. As the commission of cyber crime relies on the availability of computer system and network, cyber criminal who live in one country can disrupt or suppress computer system/ data or disseminate any illegal content in another country. Due to this nature of the crime, the need to develop a common legal regime to combat in a similar context across the globe paves the way for the development of international legal framework on cyber crime. One of the comprehensive legal instruments in this regard is the Budapest convention on cyber crime. The AU convention on cyber security and personal data protection is also another important instrument fostering organized response for cyber crime in the African continent.

In Ethiopia, despite the government's attempt to enhance the international cooperation scheme through incorporating important provisions across legislation, there is still a problem with regard to being part of international and regional legal initiatives on cyber crime. In connection with international cooperation, some important provisions are provided under the

2016 Computer Crime proclamation.[223] As per CCP, the Attorney General is authorized to engage in cooperation and agreement with another country concerning assistance on exchange of information, joint investigation and extradition.[224] The government also proposes a comprehensive international cooperation framework within DCPEC on exchange of information, joint investigation, transfer and execution of judgment and extradition in criminal matters.[225]

However, this framework is limited to cooperation and mutual legal assistance which can be created through bilateral agreement between Ethiopian government and foreign states. And there is no willingness up until now to be part of multilateral legal assistance initiatives. Until now, Ethiopia is not a party to AU Convention on Cyber Security and Personal Data Protection which countries including Ghana, Chad, Rwanda, Zambia and others are parties. In similar vein, Ethiopia is still not either a party or signatory of Budapest convention which is opened for ratification by states across the globe. This researcher is of a view that effective prevention and investigation of cyber crime needs an international cooperation which overrides limitations exists in unilateral and bilateral initiatives to combat such a crime having an international character. And these two initiatives do not provide an adequate framework for mutual assistance and international cooperation. Because the government is expected to engage in a number of treaties with a different countries and it requires a huge capital and human resources along with complex diplomacy. Besides, there exist, different legal systems between countries; variations in national cyber crime laws; differences in the rules of evidence and criminal procedure (how to obtain digital evidence, search and seizure rules…) and differences in approaches to data protection and respect for individual rights and freedoms. Therefore, being part of international initiatives, potentially, answers these problems and has a potential to create harmonization in the laws of member states with a view to make the prevention and investigation process effective.

3.2. Practical Challenges

3.2.1. Limited Abilities of Law Enforcement Officials

One of the most crucial parts of cyber crime investigation and prevention activity is the capacity of law enforcement personnel's dealing with the process of investigation, prosecution

[223] Computer Crime Proclamation, (n 21), art 42 and Draft Criminal Procedure and Evidence Code art 396, 406, 408 and 410
[224] Id, article 42
[225] Draft Criminal Procedure and Evidence Code, (n 223) Book nine, Chapter one

and prevention of cyber incidents effectively and efficiently. As it is repeatedly discussed before, the nature of cyber crime is very different from other kinds of crime. Depending on its sophisticated and complex nature it is not an easy task for law enforcement authorities to verify the commission of the crime and to start the investigation and prosecution process as soon as possible and effectively accomplish these tasks. Due to these reasons, law enforcement authorities working of the prevention, investigation and prosecution of cyber crimes need to have a capacity or ability to understand, interpret, manage, and control the existing advanced technologies along with the digital evidences that are very relevant for the investigation and prosecution of cyber crime incidents.

According to the data gathered from the interviews and questionnaires, Ethiopia's law enforcement officials lack the necessary capacity to effectively investigate and prevent computer crime incidents. Pursuant to Bedlu Y., chief officer at Federal crime investigation cyber crime investigation unit, despite the existence of minimum number of man power, existing cyber crime investigators lack the special capacity required for the effective prevention and investigation of cyber crime incidents especially large scale crimes perpetrated against critical infrastructures.[226]

In addition to that, Due to the prevalence of information and communication technology both in the commission of cyber crimes and in criminal investigations, cyber crime investigations need highly talented and capable investigators. However, investigators in Ethiopia in general and those working at INSA specifically are short of adequate capacity to conduct cyber related investigations in an effective manner and it causes limitation in the effectiveness of the prevention of cyber crime in the country.[227]

Thus, both of the respondents underline the existence of limited abilities of law enforcement officials in connection with effective cyber crime investigation and prevention. Criminal investigation in relation with computer crime is composed of both the traditional and modern investigation techniques and tools. Investigation that can be performed using traditional techniques doesn't require special ability in the tackling of cyber related criminal incidents. However, as it is accustomed in many developed legal systems, cyber crime investigation

[226] Interview with Ato Bedlu Yohannes, police officer and cyber crime investigation unit leader at Federal crime investigation office, *on the capacity of police officers to conduct cyber crime investigation*, August 4, 2022

[227] Interview with W/rt Serkalem T., cyber crime legal officer at INSA, *on the capacity of officers to conduct cyber crime investigation (digital forensic investigation)*, August 10, 2022

requires the establishment of specialized unit which is full of capable man power having special abilities in the identification, collection, acquisition and preservation of digital evidence as well as tackling and defending any attempt to commit cyber crime.

In Ethiopia, the establishment of special investigation unit with special capacity is just theoretical and there is no practical application of the establishment of special investigatory unit(s). The current police officers in the federal crime investigation office are very few in numbers and have limited ability in connection with identification and collection as well as acquisition of computer crime evidences. Not only the police officers, the public prosecutors also lacks the necessary technical and content based capacity in the understanding, interpreting and filing digital evidences especially in relation with data stored in cloud, encrypted files and data concerning anonymously committed offences.[228]

Furthermore, the other respondent from INSA's digital forensic division underscores the fact that Though investigators of digital evidences have the basic skill and knowledge in relation with cyber crime investigations, the absence of updated and skill-oriented trainings for the investigators create limitations on their capacity to effectively identify and collect evidences and transfer it to the concerned authority.[229]

In similar vein, in Ethiopia there is a shortage of man power trained specifically about modern crime investigation techniques and the proper employment of modern and sophisticated tools relevant to the identification and collection of digital evidences. Due to these reasons, we, as institution, have faced challenges in getting qualified personnel's and we have tried to build up their capacity through trainings and experience sharing platforms. But, we have found that it is not enough to have an effective investigatory scheme.[230]

Moreover, the above stated responses clearly reflect that the capacity of law enforcement authorities is one of the main factors that creates hindrances against the effective prevention and investigation of cyber crime in our country. The absence of cyber based education in lower

[228] Interview with W/rt Mignot K., Public prosecutor at Organized and Trans-national as well as National Affairs Criminal Matters Directorate (Ministry of justice), *on the capacity of public prosecutors to conduct cyber crime related investigation and prosecution*, August 21, 2022

[229] Interview with Ato Fufa, Head of digital forensic division at INSA, *on the capacity of officers to conduct cyber crime investigation (digital forensic investigation)*, August 15, 2022

[230] Interview with Ato Fufa, Head of digital forensic division at INSA, (n 229)

levels, the shortage technological advanced equipment as a country and the institutional unwillingness and unpreparedness to provide high quality trainings for all concerned bodies causes limitation in capacity of law enforcement officials.[231] In this regard, the answers of respondents from both FCIO and Digital forensic division reflects the fact that there is a shortage of capacity building programs, like trainings or workshops, for police officers in our institution specially for those working on computer and related crimes.[232] Besides, it was once that Ethiopian police commission provides training for police officers regarding cyber crime and modern investigation techniques in collaboration with Interpol.[233]

In conclusion, the fight against computer crime especially the prevention and investigation process intensely demand the availability of capable and qualified human resources not only to identify, collect and acquire digital information's relevant for the investigation but also to understand how it works, what it really means, how the modern technologies operates and what to do with such a sophisticated and complex criminal investigation process. In Ethiopia, limited abilities of law enforcement authorities challenge the effectiveness of computer crime prevention and investigations.

3.2.2. Lack of Strong Institutional Cooperation

The proper prevention and investigation of cyber crime chiefly demand the existence of effective collaboration as between government institutions. Most of computer crime incidents require strong and very quick information sharing and technical cooperation between those institution having the required information and technical expertise. In this regard, computer crime proclamation under article 23(2), 25(6) indicates INSA and any service provider will be requested for their collaboration in the investigation process.[234] But, there are also other institutions that would be communicated for the delivery of information and other technical supports. These institutions include banks, financial intelligence center (FIC) and private organizations.

[231] Ibid, Interview with W/rt Serkalem T., cyber crime legal officer at INSA, (n 241) and Interview with Ato Bedlu Yohannes, police officer and cyber crime investigation unit leader at Federal crime investigation office, (n 226)

[232] Questionnaires respondent

[233] Interview with Ato Birhanu D., Director of economic and financial related crime investigation office, *on the capacity of officers and the delivery of capacity building programs to conduct cyber crime investigation (digital forensic investigation)*, August 15, 2022; and also: Interview with Ato Bedlu Yohannes, police officer and cyber crime investigation unit leader at Federal crime investigation office, (n 226)

[234] Computer crime proclamation, (n 21), article 23(2) and 25(6)

However, there is no effective collaboration between these institutions. According to one of the interviewee from FCIO, currently there is a high rate of identity theft and computer fraud crime specifically in Addis Abeba city and the proper investigation requires the collaboration from banks where the victim is a customer or where the ATM is situated.[235] But, these banks have tiresome administrative structure and very let to give necessary information. Besides, investigative police officers, sometimes, are forced to wait weeks and months to gain access of relevant pictures or videos captured through ATM machines or security camera of super markets or hotels and any other documents very essential for the identification and collection of evidences.[236]

In addition to that, collaboration from financial intelligence center is also very weak and intensely bureaucratic. One of the interviewee noted that institutions especially FIC follows very complex chain of command and it is very challenging to easily or timely gather necessary data or evidences. What makes the problem worse is that the digital evidences in relation with computer crime are very volatile and destroyable and unless the cooperation is very quick, strong and trustworthy, the prevention and investigation process is going to be challenged and this is what is happening in Ethiopia.

The existence of strong cooperation is crucial as between Information and Network Service Administration and federal crime investigation office. One of the main reasons why INSA's collaboration makes crucial is the need to get assistance from digital forensic examinations. As we all understand, almost all computer related crime investigation need the involvement of expertise skill and knowledge on forensic.[237] The cooperation is not limited to forensic examinations but it also includes technical and knowledge based support in the deployment of special investigation techniques, if any. Conducting surveillance or interception in the real time investigation process highly requires modern technology for the timely and precise collection of digital evidences.[238] However, the assistance and cooperation from INSA is not satisfactory and even sometimes they tries to refuse the request for assistance without a reasonable grounds to do

[235] Interview with Ato Bedlu Yohannes, police officer and cyber crime investigation unit leader at Federal crime investigation office, (n 226) and Interview with Ato Birhanu D., Director of economic and financial related crime investigation office, (n 233)
[236] Ibid
[237] Interview with w/ro Hana T., cyber crime legal officer at INSA, *on the importance and practical application of inter-institutional assistance on criminal investigation, August 10, 2022*
[238] Ibid

so.[239] Or, the requested assistance is delivered several weeks or months later and this causes the delay in the investigation process and opens a door for the destruction or lost of necessary evidences.[240]

Additionally, the absence of strong institutional assistance scheme causes the difficulty in the effective prosecution and conviction of cyber criminals through limiting the speed of evidence collection and acquisition process.[241] Besides, it also opens the way for difficulty in data preservation of some confidential evidences. In the same vein, Mignot also noted that, currently, it is only 5 or 6 cases that have been effectively adjudicated and prosecuted. However, there are many cases reported by police officers and returned back to further investigation.[242] This is mostly because of the weakness of and the unclearness of the evidence collected. As per the investigative police officers response to the questionnaires, almost all of investigations are dependent on the cooperation they received from other institutions. But they are not satisfied in its time consuming nature and unwillingness of some specific individuals within these institutions holding critical decision making power as well as the absence of the culture of working together.[243] The other respondents also mentioned that expertise's at INSA and professionals at Ethio-telecom as well as other institutions considers the assistance request and the task they are going to perform as additional burden which is apart from their duty. And, this results reluctance and unwillingness to collaborate in the prevention and investigation process.

3.2.3. Confusion on the Investigative Power

Cyber crime investigatory power is clearly stated under article 23 of computer crime proclamation. Pursuant to sub article 1 of this provision:

> The public prosecutor and police shall have joint power to investigate criminal acts provided for in this Proclamation. And the public prosecutor shall lead the investigation process.

[239] Interview with Ato Bedlu Y., police officer and cyber crime investigation unit leader at Federal crime investigation office, (n 226) and anonymous respondent, infra note 240

[240] Interview with Anonymous respondent, Police officer within cyber crime investigation unit at Federal crime investigation office, *on the practice of cyber crime investigation and assistance and collaboraton with other governmental and non-governmental institutions*, August 4, 2022

[241] Interview with W/rt Mignot K., (n 228) *on the cooperation between investigative organs and with other institutions*, August 21, 2022

[242] Questionnaires respondent

[243] Interview with Ato Bedlu Yohannes, police officer and cyber crime investigation unit leader at Federal crime investigation office, (n 226) and Interview with Anonymous respondent, police officer within cyber crime investigation unit at Federal crime investigation office (n 240)

Accordingly, the public prosecutor and police have joint cyber crime investigatory power. Even if both institutions hold the power jointly, the public prosecutor takes the leading position in the investigation process. Here in this provision, INSA is precluded from the power distribution and allowed only as assistant for the technical issues of the investigation.[244] Besides, the administration, INSA, also authorized to conduct sudden searches and other investigatory and preventive activities.

> Where there are reasonable grounds to believe that a computer crime is to be committed and it is necessary to prevent and control the crime, ("…") the administration may conduct sudden searches, conduct digital forensic investigation, provide appropriate security equipment or take other similar measures on computers, computer systems or infrastructures ("…")[245]

Pursuant to this article, the chief power given for INSA is directly linked with the digital forensic investigation which other investigatory institutions cannot engaged with and taking cyber related security measures including provision of security measures for the prevention and investigation of computer crimes.

However, the practical application of such powers is quite the opposite of what is provided under the proclamation. On ground, the investigatory police officers and digital forensic investigators are the main actors in the field and the public prosecutors set aside themselves from the investigation process.[246] According to Hana T., police officers in FCIO always transfer criminal cases for digital forensic division staffs which should be investigated by their own investigators and which do not necessarily require forensic examination. And sometimes, police officers wait until the digital forensic investigators refer the cases and this causes delay to take proactive preventive measures.[247] In another occasions, forensic investigators engaged in investigative activities beyond their power limits. Because of these practical confusions, the effectiveness of cyber crime investigation and prevention process is highly affected.

In conclusion the power of investigatory institutions stated under the provisions of the proclamation, particularly in relation with digital forensics and criminal acts investigation, is

[244] Computer Crime Proclamation, (n 21), art 23(2)

[245] Computer Crime Proclamation, (n 21),article 26(1)

[246] Interview with Ato Bedlu Yohannes, (n 226) and Interview with Anonymous respondent, police officer within cyber crime investigation unit at Federal crime investigation office (n 240), *on the practical difficulties in cyber crime investigation and prevention*

[247] Interview with w/ro Hana T., (n 237), *on the practical difficulties in cyber crime investigation and prevention*

confused as between the police and INSA. The reluctance and inactive behavior of public prosecutors power and the unwillingness and inability to engage in to the investigation process worsen the existing problems. Because of this, practically there is joint power between police and public prosecutors. Paradoxically to the CCP, the police and INSA are the only organs investigating computer crimes and public prosecutors role is limited to the prosecution of cyber criminals.[248] Digital forensic investigators are busy on reactive cyber crime investigation rather than their official mandates to actively engage with proactive or preventive cyber crime investigative actions. Such practical confusion creates a gap in the proper investigation of reported cases and challenges its effectiveness.

3.2.4. Lack of Adequate Investigative Tools and Equipment

The prevention and investigation of cyber crime is chiefly technical and require the existence of modern and advanced information technology equipment. More importantly, cyber crime investigators need the availability of digital devices and software programs that require the use of specialized tools to have effective investigation process.

In Ethiopia, though the government's attempt to combine INSA and investigatory police officers solves some of the problems, the inadequacy of equipment or tools in cyber crime investigative division is still hindered the investigation of cyber crimes. Currently, the division is under facility and surprisingly, from the four active investigators only two of them have effectively working computers (lap tops) and there is one extra desktops which serves for the whole staffs in that office.[249] As per the responses of polices for the questionnaires, all of them mentions the fact that they are obliged to use their own mobile phone to collect very essential digital evidences. Besides, police officer within cyber crime investigation unit have been repeatedly requests the provision of GPS device for the purpose of tracking cyber criminals through their mobile phones or personal computers.[250]

Additionally, though INSA's digital forensic lab is organized in a better set up than the cyber unit division of FCIO, it is still short of some very important equipment for the effective

[248] Interview with W/rt Mignot K., (n 228), *on the practical difficulties on the application of joint power of cyber crime investigation*

[249]Interview with Anonymous respondent, police officer within cyber crime investigation unit at Federal crime investigation office (n 240), *on the practical difficulties in cyber crime investigation and prevention*

[250] Interview with Ato Bedlu Y., (n 226), *on the practical difficulties in cyber crime investigation and prevention*

computer forensic investigation. According to the interviewee in digital forensic division, there are best materials available in the market such as ‘EnCase’, ‘Computer forensic hardware’, ‘Logicube’, Forensic write blockers’. There are also other materials but the above listed are highly advanced and very efficient to use. However, they are not provided to us yet and limit our effectiveness.[251]

In short, cyber crime investigation and prevention is highly challenged because of the shortage of necessary tools and equipment both in digital forensic division and cyber crime investigation unit. The identification, collect, acquisition and preservation of digital evidences requires the presence of technologically equipped man power and institutions. Given the existing shortage, some volatile digital evidences are not well preserved and even lost. And the recovery of these evidences requires another technology which currently available but outdated and needs upgrading these materials. Thus, investigative tools and equipment’ shortage hindered the effectiveness of the prevention and investigation of computer crime in Ethiopia.

3.2.5. Shortage of Man Power and Brain Drain

The other problem for the effective prevention and investigation of cyber crime in Ethiopia is the existence of minimum number of human resources in all investigatory institutions and the transfer and leave of qualified and hardworking man power from their post. One of the parameters of the strength of preventive and investigative activities is the number of human resources. If there is a minimum number of working man-power, the effectiveness and quality of the work would be very limited.

The federal police commission crime investigation office cyber crime investigation division has only 5 active member within which 1 of them are the team leader.[252] Currently, this number has decreased to 4 because of the personal problem of one of the member.[253] Thus, the federal cyber crime investigations have been conducted by 4 police officers. According to the interviewee in the unit, the minimum number of active working man power causes limitations in

[251] Interview with Ato Fufa, (n 229) *on the practical and institutional challenges to cyber crime investigation and prevention*

[252] Interview with Ato Birhanu D., Director of economic and financial related crime investigation office, (n 233), *on the human resources and institutional hindrances for cyber crime investigation*

[253] Interview with Ato Bedlu Y., (n 226), *on the practical and institutional difficulties in cyber crime investigation and prevention*

our capacity of investigating reported cases promptly and efficiently.[254] The interviewee also noted the fact that, nowadays there is a lot of cases, both severe and pity, investigated and it takes several months' even years to complete the investigation and transfer it to the public prosecutor. This is mainly because cases mostly investigated as a unit and only in some occasions that individual investigator police officer investigates cases by his own.[255]

Pursuant to the response of police officers for the questionnaires, all of them mentioned the problem of absence of sufficient number of police officer and the need to increase their number. In similar vein, according to the respondents in the digital forensic division, the number of forensic investigators is few compared to the cases brought to their attention and with the view to effectiveness of investigation of computer crime cases.

With regard to public prosecutors, though there is limited number of cases adjudicated or prosecuted and most of the cases are in the hands of the investigative police officers, the problem here is the absence of separate human resource allocation for cyber crime investigation and prosecution. Currently, cyber crime cases is being investigated and prosecuted under the directorate named as "Organized and Trans-national as well as National Affairs Criminal Matters Directorate" - **"የተደራጁና ድንበር ተሻጋሪ እንዲሁም ሀገራዊ ጉዳዮችን የሚመለከቱ ወንጀሎች ጉዳዮች ዳይሬክቶሬት"**. Thus, there is no specific prosecution office for cyber crime investigation and prosecution.[256] Public prosecutors conduct their prosecution process in the same manner and with the same office designated for other crimes having trans-national and organized nature. Besides, these prosecutors are not sufficiently trained with the investigation and prosecution of cyber crime cases. In conclusion, the minimum number of appropriately trained staffs in the investigatory organs serves as significant obstacle to effective prevention and investigation of cyber crime.

Brain drain or the transfer of trained and skilled investigators or workers is the other significant factor for the limitation in effective investigation and prevention of computer

[254] Ibid

[255] Ibid, Interview with Ato Birhanu D., Director of economic and financial related crime investigation office, (n 233)

[256] Interview with W/rt Mignot K., (n 228), on the practical and institutional challenges against cyber crime investigation and prevention

crime.[257] One of the unique features of computer crime is that information and communication technology is endlessly evolving. Given this nature of the crime, officials and investigators working in this area must be lifelong learners and continuously engage in capacity building trainings to remain current on technology and secure the post and to be permanent in that office. According to the interviewee from FCIO, one of the problems in our office is the leave of experienced staffs either by the promotion to the higher position in another institution or due to the economic and other interest issues.[258] Because of the existing economical crisis, staffs opt to leave the governmental organs and join other private sectors to engage in another profession. Specially, investigators working at INSA mostly join other private sector working on ICT related fields or won scholarships and leave the country within which most of them are never returned.[259] Besides, staffs shit to one office to another office or post is also accelerates the problem. If one of the staff performs well in his duties, it has been taken culture to shit that staff to another position and left the former office without skilled and experienced officer or professional. Then, it takes long period of time to replace by another staff and the new member need trainings and adaptation to the nature of the investigation of computer crime which is rarely provided by the government.[260] Given the evolving nature of the crime and the danger faces our country, what the government should do is quite the opposite. Unless the government gives due attention to these offices and hire talented and interested professionals and create satisfactory working condition to staffs in these institution, it going to be much difficult to fight cyber crime in the coming years. In short, both of the above factors, minimum numbers of man-power and brain-drain causes the ineffectiveness in the prevention and investigation of computer crime in Ethiopia.

Summary

In the preceding discussions, an attempt has been taken to identify and examine the legal and practical or/ and institutional hindrances against the effective prevention and investigation of computer crimes in Ethiopia. Both primary and secondary sources of data are employed to

[257] Interview with w/ro Hana T., cyber crime legal officer at INSA, (n 247) and Interview with Ato Fufa, Head of digital forensic division at INSA, (n 253)

[258] Interview with Ato Bedlu Y., (n 253)

[259] Interview with w/rt Serkalem T, cyber crime legal officer at INSA, (n 231) and Interview with Ato Fufa, Head of digital forensic division at INSA, (n 251)

[260] Ibid and Interview with Ato Bedlu Y., (n 253)

collected data. Accordingly, the main legal and practical challenges include: Lack of sufficient coverage of crimes; Inadequacy of laws on filtering and blocking mechanisms; Failure to be part of international legal initiatives; Limited abilities of law enforcement officials; Lack of strong and timely institutional cooperation; Lack of adequate investigative tools and equipment and shortage of man power. Despite the government's attempt to create full-fledged and comprehensive preventive and investigatory legal and institutional frameworks, cyber crime investigation and preventive process is surrounded by a number of hindrances that makes every cyber crime related measures ineffective. Unless the concerned governmental organs assess these challenging factors and take appropriate measures that best resolve the existing problems, cyber crime continues a major challenge to the government and the public in general and the security of critical governmental and non-governmental institutions would fall in the hands of cyber criminals. To this effect, in the coming chapter the researcher draws a conclusion of the relevant issues discussed in the preceding chapters and forward proper recommendations.

CHAPTER FOUR:

CONCLUSION AND RECOMMENDATIONS

4.1. CONCLUSION

Among different kinds of crimes in the 20th and 21st century, cyber crime is a crime that is mainly use and facilitated by the electronic devices and networking system. Cyber crime, given its complex and limitless evolving nature, is considered as one of serious crimes challenging the socio-economic and political as well as security system of the global community. The challenge also relates to understanding the nature, scope, topology and impacts of the crime. Due to this, defining cyber crime is still problematic issue and has got no agreed definition globally. However, several attempts are being made to understand the crime by revealing its characteristics and providing a range of acts of crimes consisting cyber crime nature. This crime is also uses interchangeable names such as: cyber crime; computer crime: Cyber crimes; digital crimes and others. Generally, cyber crime can be defined as any criminal conduct that relates to attacks on or/ and with computers, computer data, computer networks and other information and communications technology.

Despite the absence of clear and reliable information on the extent of the problem of cyber crime, currently these crimes become a subject that poses a very real and tangible threat to the socio-economic and political matters of the global community. The scale and complexity is wide ranging and reached the level of a global threat than any other crime. The prevalence of information and communication technologies and the low-level detection rate in most of countries due to low reporting, absence of comprehensive legal system, weak investigatory scheme and weak international collaborations play a significant role in the prevalence of cyber crimes. To this effect, almost all states across the globe sought the development of adequate legal and institutional frameworks and works on the effective prevention and investigation cyber crimes in their boundaries.

Given the high level of computer crime commission specifically in relation with identity theft, computer fraud, revenge pornography, dissemination and consumption of pornographic and erotic images and videos, forgery, and other crimes and other cyber attacks perpetrated from other countries against critical governmental and public infrastructures as well as companies, cyber crime has become a subject that poses a very real and tangible threat to the socio-economic, security and political matters in Ethiopia as well. Due to this, the government has enacted a proclamation and empowers a number of institutions to investigate, detect and prevent the commission of such crimes. Nevertheless, the investigation and prevention of cyber crimes is challenged by a number of difficulties and has not been effective as expected.

The chief legal gaps and practical and institutional hindrances for the ineffectiveness of cyber crime investigation and prevention are: the 2016 computer crime proclamation specifically is not adequate enough to cover all acts of cyber crime in a comprehensive manner. Though it tries to address almost all crimes, acts such as racist and xenophobic content, revenge pornography, IPR crimes and crimes related with large-scale cyber attacks. The proclamation left some of these acts totally and some others to be governed by other laws scattered here and there. This makes the proclamation less comprehensive and organized. Besides, the law also lacks clarity in defining the crime itself and lacks strength in its deterrent effect. The second line of definition stated in article 2 of the proclamation makes the definition somewhat vague in terms of whether it tries to include the use of the hardware part of a computer to commit a given conventional crime (for instance: body injury). Thus, the way the legislator opts to express computer related cyber crimes is not appropriate and opens door for criticism and interpretation. Furthermore, the absence of laws dealing with the prevention of some serious acts of computer crimes through filtering and blocking the transfer or dissemination of the content of those serious crimes is the other major legal gaps. Acts such as child pornography, indecent and obscene images and videos, racist and hatred speeches or text or pictures or videos and any other crimes must be filtered and blocked totally. And, there is no law on this regard and from the socio-cultural and psychological perspective, the absence of this important legal mechanism causes ineffectiveness in the prevention of computer crimes. The existence of weak involvement in the international cyber crime legal initiatives also causes problem in the effective prevention and investigation of cyber crime. Due to the shortcomings in the bilateral legal assistance scheme with each country in the globe and other non-governmental international organizations, multilateral cooperation on the basis of international legal initiatives is the best option especially in the case of cyber crime. But, the government failed to be part of international legal initiatives and this limits the country's effectiveness in collaboration with other country and its positive impact on the prevention and investigation of computer crimes.

Besides, the existing cyber crime investigators in Ethiopia have limited ability in connection with identification and collection as well as acquisition of computer crime evidences. The limitation also related with the necessary technical and content based capacity in the understanding, interpreting and filing digital evidences especially in relation with data stored in cloud, encrypted files and data concerning anonymously committed offences. Besides, the existence of poor inter-institutional cooperation between government and non-government institutions and confusions as to investigating power as well as shortage of man power and necessary equipment are the other challenges in Ethiopia. Despite the clear stipulation of the law, public prosecutor's failure in actively engaging in investigation and the more concentration of power by INSA and the less technical and human capacity of police commission results in confusion of investigative power between these institutions. The reluctance and unwillingness of institutions to collaborate with investigating officers coupled with the poor working together culture and politicization grown in Ethiopia challenges the effectiveness of prevention and investigation of computer crime. Due to weak institutional collaboration, investigation takes long period of time and mostly it is ineffective in identifying, collect and acquire necessary information or evidences. Moreover, though the identification, collect, acquisition and preservation of digital evidences requires the presence of technologically equipped man power and institutions, cyber crime investigation and prevention in Ethiopia is highly challenged because of: the shortage of necessary tools and equipment both in digital forensic division and cyber crime investigation unit, and minimum numbers of and brain-drain of skilled and experienced man power.

4.2. RECOMMENDATIONS

On the light of the study conducted and on the basis of the above conclusion, the researcher suggested the following recommendations for the effective investigation and prevention of computer crimes in Ethiopia.

4.2.1. Concerning Computer Crime Proclamation

The FDRE government legislative organ, with a view to rectify the existing problems and to come up with a more comprehensive law and through taking the lessons from other countries, should amend the existing computer crime proclamation. With this amendment,

- The government should criminalize all acts of computer crime and should gather crimes having cyber crime nature governed here and there and embark strong and unified governance of computer crimes.
- With a view to create a clear picture as to what computer crime looks like and to have vague-free understanding by law enforcement authorities and academicians, the government should develop new and all inclusive definition for the term computer crime.

4.2.2. Concerning Cooperation and Collaborations

International cooperation

Computer crime is a common problem to all countries around the globe irrespective of their political, military, security and economic status. Because of this, the international community works together so as to facilitate and strengthen the investigation and prevention of the crime through (international) regional and sub-regional legal initiatives. Up until now, Ethiopia is not a party to any initiatives. Thus, the government should sign and ratify the Council of Europe convention on cyber crime and AU convention. Indeed, there are mutual legal assistance initiatives on the basis of bilateral treaties. However, ratifying multilateral conventions is very necessary and solves the problem exists on bilateral MLA initiatives.

Inter-institution collaboration

The other important element in computer crime investigation and prevention is the access of relevant digital and non-digital information and evidences as soon as possible. Law enforcement authorities, most of the time, may not have an access to every sort of evidences by themselves. To this effect, this researcher recommends that both governmental and non-governmental institution should collect and share information directly or indirectly related with the investigation of a given criminal act immediately whenever they are requested. Appropriate measures should be taken to eradicate more stern bureaucracies and administrative mischief that is against the culture of working together and create difficulties on law enforcement organs in the effectiveness of computer crime investigations. The longer the time that these institutions respond for the request and transfer the requested evidences the less cyber crime investigation and prevention become effective. Thus, institutions having cyber crime information or evidence should work hand-in-hand with law enforcement organs in the fight against cyber crime.

4.2.3. Concerning Cyber Crime Investigative Organs

Given the existing confusion as between investigating institutions and the gap in implementing or discharging what is stated under the proclamation, cyber crime investigation and prevention is highly affected and become ineffective. In order to solve these problems, this researcher recommends that:

- The government should enact directive or regulation that provides cyber crime investigating power as between the public prosecutor, police commission and INSA or other organs in a clear and precise manner. With this directive or regulation, there should be clear cut and detailed power distribution between investigating organ in the manner that provide a clear distinction between joint and separate investigation process.
- The government, with this directive or regulation, should devise a mechanism to follow up and monitor the day-to-day activity of investigating institutions and hold accountable for any failure to discharge their function before a competent judicial organ within the nation.

4.2.4. Regarding Law Enforcement Authorities and other Technical Issues

The backbone of every criminal investigation especially cyber crime investigation and prevention is the existence of adequately trained and experienced law enforcement officials having interest and talent in understanding what he/ she is doing along with the presence of appropriate investigating and/ or preventive tools and equipment sufficiently. Thus, this researcher recommends that:

- The government, in collaboration with national and foreign institutions working on cyber crime investigation and prevention, should provide adequate, updated and continued trainings and workshops for law enforcement authorities. This includes short term free scholarships whether to take specialized trainings or studies on the subject matter with strong follow-ups.
- The government should create a suitable and conducive working environment through providing interesting salaries and compensation as well as economic security for officials working at INSA and FCIO-CCID. Besides, promotions or transfer of staffs from these organs should follow after the recruitment of other interested and qualified personnel.
- The government should also take appropriate administrative and budgetary measures to solve human resource problems and to recruit and add cyber crime investigators and forensic professionals as much as possible.
- Appropriate investigating tools and equipment should be provided for law enforcement officials or investigating institutions. Once the government stands to fight cyber crimes, there should not be any obstacles and shortages in the provision and distribution of necessary tools and equipment. Besides, equipment relevant for surveillance and other investigatory purpose should be installed and private organizations should also be supported for installing these security equipment.

Bibliography

I. Secondary sources

i. Books

1. Catherine D., *Practical Research Method*, Magdalene Road, United Kingdom, 2002
2. Jenner B., *A Companion to Qualitative Research*, 2nd ed., Sage Publications Ltd, 2004
3. John C., *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*, 4th ed., Sage Publication Inc., Thousand Oaks, 2014
4. Kumar, Cyber Law, A view to social security, 2009;
5. Mike M. and Wing H., *Research methodology for law*, Edinburgh university press, 2007;
6. Crutchfield R., Crime: Readings, Pine Forge Press, California, 2000;
7. Parker Donn, *Fighting Computer Crime: A New Framework for Protecting Information*, New York, 1998; and
8. Steven, Malby et al, Comprehensive Study on Cybercrime, (draft report) UN New York, 2013.

ii. Journals (Articles)

1. Adam M. Bossler and Tamar Berenblum, 'Introduction: new directions in cybercrime research', Journal of Crime and Justice, 2019, Vol. 42, No. 5, PP. 495–499;
2. Ahmet Nuredini, 'Challenges in combating the cyber crime', Mediterranean Journal of Social Sciences, 2014, vol. 5, no. 19, PP. 592-599;
3. Bejatovic Stanko, 'Special methods of revealing and investigating criminal offences committed by organized crime', *Journal of Criminology and Criminal Law*, 2006, vol. 44, PP. 43-72;
4. Cameron, S. D. Brown, 'Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice', *International Journal of Cyber Criminology*, 2015, Vol. 9, PP. 55–119;
5. Charles K. and Ahmed B., 'Understanding and Applying Research Paradigms in Educational Contexts', *International Journal of Higher Education*, Vol. 6, No. 5;
6. *Charney*, Computer Crime: Law Enforcement's Shift from a Corporeal Environment to the Intangible, Electronic World of Cyberspace, *Federal Bar News*, 1994, Vol. 41, Issue 7;

7. Divy Shivpuri, 'Cyber Crime: Are the Law Outdated for this Type of Crime', *International Journal of Research in Engineering, Science and Management*, 2021, Vol. 4, PP. 44-49;
8. Salimi Farsam, 'Cybercrime Threats, Offences and Special Investigation Measures from a European Perspective', *New Zealand Yearbook of International Law,* 2017, vol. 15, PP.47-60;
9. Halefom, Hailu, 'The State of Cybercrime Governance in Ethiopia', *Article published on ResearchGate*, 2015, PP. 1-34;
10. Johannes, Xingan, 'Cyber Crime and Legal Countermeasures: A Historical Analysis', *International Journal of Criminal Justice Sciences,* 2017, Vol. 12, PP. 196-207;
11. Kinfe Micheal, 'Ethiopia's new cybercrime legislation: Some reflection', *Computer law and security review*, 2017, Vol. 33, PP. 250-255;
12. Kibreab Adane, 'The Current Status of Cyber Security in Ethiopia', *The IUP Journal of Information Technology*, 2020, Vol. XVI, No 3, PP. 1-13;
13. Kejal Chintan, 'Cyber Crime and its Categories', *Indian journal of applied research*, 2013, Vol. 3, PP. 130-133;
14. Kelly J. Harris, 'Computer Crime: An Overview', *National Consortium for Justice Information* and *Statistics*, 1995, PP. 1-6;
15. Kinfe Micheal, 'Some Remarks on Ethiopia's New Cybercrime Legislation' *Mizan law Review*, 2016, Vol. 10, No.2, PP. 448-458;
16. Liao Ming, 'Process of Legalizing Special Investigative Techniques in China', *The Frontiers of Law in China*, 2015, Vol. 10, No. 3, PP. 510-536;
17. Misgana Yifiru, 'Assessment of Cybercrime Governance in Ethiopia Since 2004', *New Media and Mass Communication*, 2021, vol. 96, PP. 1-8;
18. Stefan Budjakoski, 'Use Vs abuse of special investigative measures in detecting severe form of crime in republic of Macedonia', *European Scientific Journal,* 2014, Vol. 1, PP. 345-352;
19. Temesgen, Aschenek, 'The Quandary of Cyber Governance in Ethiopia', *Journal of Public Policy and Administration*, 2019, Vol. 3, No. 1, PP. 1-7;

20. Toon Moonen, ‘Special Investigation Techniques, Data Processing and Privacy Protection in the Jurisprudence of the European Court of Human Rights’, *Pace International Law Review Online Companion,* 2010, vol. 1, No. 9, PP. 97-136;
21. Peter Nyeste, ‘The principles of the use of the special investigative techniques’, *Національний університет,* 2018, vol. 17, No.1, PP. 1-11;
22. Vijaykuma Shrikrushn, ‘The concept of cyber crime’, *Global Journal of Enterprise Information System*, 2011, vol. 3, PP. 72-84;
23. Wondemagegn Tadesse, ‘Legal Research Tools and Methods in Ethiopia’, *Journal of Ethiopian Law*, 2012, Vol. 25, No.2; and
24. Worku Yaze, ‘The Use of ‘Special Investigation Techniques and Tools’ in the Fight against Serious Crimes: Legal Basis and Human Rights Concerns in Ethiopia’, *Journal of Ethiopian law,* 2015, VOL. XXX, PP. 81-111.

II. Legal Instruments

i. Treaties, Declarations and Resolutions

A. Treaties (Conventions)

1. African Union Convention Cyber Security and Personal Data Protection, 2000, guided by the constitutive act of African union; at https://au.int/sites/default/files/treaties/29560-treaty0048__african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf [Last accessed at 15/7/2014];
2. Convention on Cybercrime, 2001, Council of Europe, European Treaty Series - No. 185; available at https://rm.coe.int/1680081561 [Last accessed at 15/7/2014];
3. Convention on combating transnational Organized crime, 2000, UNGA treaty series, res. 55/25; available at: https://www.unodc.org/documents/middleeastandnorthafrica/organized-crime/UNITED_NATIONS_CONVENTION_AGAINST_TRANSNATIONAL_ORGANIZED_CRIME_AND_THE_PROTOCOLS_THERETO.pdf [last accessed at 21/6/2022].

B. Protocols

1. Additional Protocol to the Convention on cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, council of Europe, European treaty series no. 189, 2003, available at https://rm.coe.int/168008160f [last accessed at 11/6/2022];
2. Optional Protocol to the United Nations Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, UN, treaty series, vol. 2171, 2000, available at https://www.ohchr.org/Documents/ProfessionalInterest/crc-sale.pdf [last accessed at 11/6/2022];
3. Draft Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, approved by Committee of Ministers on 17 November 2021.

C. Directives

1. Economic Community of West African States directive C/DIR. 1/08/11 on fighting cyber crime with ECOWAS, 66th ordinary session of the council of ministers, 2011; available at https://issafrica.org/ctafrica/uploads/Directive%201:08:01%0on%20fighting%20Cyber%20Crime%20within%20ECOWAS.pdf [last accessed at 16/6/2022]

D. Resolutions

1. UN General Assembly Resolution 60/177; available at https://www.unodc.org/documents/commissions/CCPCJ/Crime_Resolutions/20002009/2005/General_Assembly/A-RES-60-177.pdf [last accessed at 13/6/2022];
2. UN General Assembly Resolution 55/63 on Combating the criminal misuse of information technologies; available at https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf [last accessed at 13/6/2022];
3. UN General Assembly Resolution 56/121 on Combating the criminal misuse of information technologies; available at https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_56_121.pdf [last accessed at 13/6/2022];
4. UNGA resolution 58/199 on Creation of a global culture of cyber security and the protection of critical information infrastructures; available at https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf and UNGA 57/239 Creation of a

global culture of cyber security; available at https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf [last accessed at 13/6/2022];

5. ECOSOC Resolution 2004/26, on International cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes; available at https://www.unodc.org/documents/commissions/CCPCJ/Crime_Resolutions/2000-2009/2005/ECOSOC/Resolution_2004-26.pdf [last accessed at 13/6/2022];
6. ECOSOC Resolution 2004/42, on Sale of internationally controlled licit drugs to individuals via the Internet; available at https://www.unodc.org/documents/commissions/CND/Drug_Resolutions/2000-2009/2004/ECOSOC_Res-2004-42.pdf [last accessed at 16/3/2022]; and
7. Resolution 16/2, available at: https://www.unodc.org/documents/commissions/CCPCJ/Crime_Resolutions/2000-2009/2007/CCPCJ/Resolution_16-2.pdf [last accessed at 13/6/2022].

E. Other Decisions and Reports

1. Explanatory Report to The Council of Europe Convention on Cybercrime 2001, (ETS No.185);
2. Handbook on the optional the Sale of Children, Child Prostitution and Child Pornography, UNICEF, 2009, available at https://www.unicef-irc.org/publications/pdf/optional_protocol_eng.pdf [last accessed at 11/6/2022]; and
3. Economic Community of West African States; available at https://ccdcoe.org/organizations/ecowas/ [last accessed at 16/6/2022].

ii. National Laws

A. Policies and strategy

1. Federal Democratic Republic Ethiopia national, ICT policy and strategy, 2009;
2. Federal Democratic Republic of Ethiopia, Criminal Justice Policy, Ministry of Justice, Addis Ababa, 2011;
3. አገር አቀፍ የተቀናጀ የወንጀል መከላከል ስትራቴጂ, በሚኒሰተሮች ምክር ቤት የፀደቀ, 2012

B. Proclamations

1. A Proclamation to provide Definition of Powers and Duties of the Executive Organs of the Federal Democratic Republic of Ethiopia, 2015, Federal Negarit Gazette, Proc. no 916, 22nd year, no 12;
2. Computer Crime Proclamation, 2016, Federal Negarit Gazette, proclamation no 958, 22nd year No. 83;
3. Copyrights and neighboring protection proclamation, 2004, Federal Negarit Gazette, Proc no 410, 10th year, No. 55;
4. Criminal Code of the Federal Democratic Republic of Ethiopia, 2004, Federal Negarit Gazette, Proc. No. 414;
5. Ethiopian Federal Police Establishment Proclamation, 2011, Federal Negarit Gazette, Proc. 720, 18th year, No. 2;
6. Federal Courts Proclamation, 2021, Federal Negarit Gazette, Proc. 1234, 27th year, No. 26;
7. Federal Attorney General Establishment Proclamation, 2016, Federal Negarit Gazette, Proc. 943, 22nd year, no. 62;
8. National Payment System Proclamation, 2011, Federal Negarit Gazzeta, Proc. No. 718, 17th year, No. 84;
9. National Intelligence and Security Service Reestablishment Proclamation, 2013, Federal Negarit Gazette, Proc. 804, 19th year, no. 55;
10. Proclamation to re-establish Information Network and Security Agency, 2013, Federal Negarit Gazette, proc. no 808, 20th year, no 6;
11. Registration of vital events and national identity card proclamation, 2012, Federal Negarit Gazzeta, Proc. No. 760, 18th year, No. 58; and
12. Telecom Fraud Proclamation, 2012, Federal Negarit Gazzeta, Proc. No. 761,18th year, No. 61.

C. Regulation

1. Information Network and Security Agency Establishment Council of Ministers Regulations, 2006, Federal Negarit Gazette, Reg. no 130, 13th year, no 5.

III. Researches and Dissertation

1. Abenezer Berhanu, *Developing National Cybersecurity Strategy for Ethiopia*, Master's Thesis, Tallinn University of Technology, School of Information Technologies, Department of Software Science, 2019 [unpublished]; available at: https://digikogu.taltech.ee/et/Download/06ef8980-4c08-94d1-7918a42e80a0 [last accessed at 5/4/2022];
2. Iyasu T. *Cybercrime in Ethiopia: Lessons to be Learned from International and Regional Experiences*, LLM Thesis, Addis Ababa University, School of Graduate Studies, 2018, [Unpublished, available at Law library];
3. Tewodros G., *Cyber Security Practices and Challenges at Selected Critical Infrastructures in Ethiopia*, Master thesis, Addis Ababa University, Department of Science in Information Science, [Unpublished, available at Law library];
4. Karri Wihersaari, *Intelligence Acquisition Methods in Cyber Domain: Examining the Circumstantial Applicability of Cyber Intelligence Acquisition Methods Using a Hierarchical Model*, Master's Thesis, National Defence University, Master of Military Sciences, 2015, [Repository: National Defense University Course Library];
5. Jan-Jaap Oerlemans, *Investigating cybercrime*, Doctoral dissertation, Leiden University, 2017,[repository: Leiden University];
6. Marthe Goudsmit, *Revenge pornography: a conceptual analysis understanding a crime of disclosure*, Master's thesis, Leiden university, Master of Philosophy, 2017.

IV. Lectures

1. Nega Ewnete, (Associate professor), *Advanced legal research Methodology*, Lecture delivered at School of Law, Bahir Dar university, October 2020;
2. Worku Yaze, (Asst. professor, PhD candidate), *Contemporary issues in criminal law*, Lecture delivered at School of Law, Bahir Dar university, February 24, 2021.

V. Others

1. Interview with Ato Bedlu Yohannes, police officer and cyber crime investigation unit leader at Federal crime investigation office, August 4, 2022;
2. Interview with W/rt Serkalem T., cyber crime legal officer at Information and Network Security Administration, August 10, 2022;
3. Interview with W/rt Mignot K., Public prosecutor at Organized and Trans-national as well as National Affairs Criminal Matters Directorate (MoJ), August 21, 2022;
4. Interview with Ato Fufa, Head of digital forensic division at Information and Network Security Administration, August 15, 2022;
5. Interview with Ato Birhanu D., Director of economic and financial related crime investigation office at Federal Crime Investigation Office, August 15, 2022;
6. Interview with W/ro Hana T., Cyber crime legal officer at Information and Network Security Administration, August 10, 2022;
7. Interview with Anonymous respondent, police officer within cyber crime investigation unit at Federal crime investigation office, August 4, 2022.

VI. Internet sources

1. Africa's evolving cyber threats: Africa center for strategic studies; at https://africacenter.org/spotlight/africa-evolving-cyber-threats/ [last accessed at 28/3/2022];
2. African Union, available at https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection [last accessed at 10/6/2022];
3. African Union, 'A global approach on cyber security and cybercrime in Africa', available at https://au.int/sites/defualt/files/newsevents/workingdocuments/31357-wd-a_common_african_approach_on_cybersecurity_and_cybercrime_en_final_web_site [last accessed at10/6/2022];
4. Ethiopia's intelligence office foils 787 cyber attacks-official, at http://www.apanews.net/mobile/unelnterieure_EN.php?id=4943340 [last accessed at 1/4/2022];
5. Digital 2021: Ethiopia; available at: https://datareportal.com/reports/digital-2021-ethiopia [last accessed at 24/3/2022];

6. Country-wise legislation on “revenge pornography” laws; https://cis-india.org/internet-governance/files/revenge-porn-laws-across-the-world/view [last accessed at 5/9/2022];
7. Critical look at the regulation of cybercrime; available at: https://www.ie-ei.eu/IE-EI/Ressources/file/biblio/Criticallookattheregulationofcybercrime [last accessed at 6/9/2022];
8. Carter, Computer Crime Categories: How Techno-Criminals Operate, FBI Law Enforcement Bulletin, 1995, page 21, available at: www.fiu.edu/~cohne/Theory%20F08/Ch%2014%20-%20Types%20of%20computer%20crime [last accessed at 20/5/2022];
9. Crimes related to computer networks, Background paper for the workshop on crimes related to the computer network, 10th UN Congress on the Prevention of Crime and the Treatment of Offenders, 2000, A/CONF.187/10, page 5; available at: www.uncjin.org/Documents/congr10/10e [last accessed at 20/5/2022];
10. Commission on Crime Prevention and Criminal Justice Twenty-eighth session; available at:https://www.unodc.org/documents/commissions/CCPCJ/CCPCJ_Sessions/CCPCJ_28/ECN152019_L3REv1_e_V1903716.pdf [last accessed at 13/6/2022];
11. Cornell law school; available at: https://www.law.cornell.edu/cfr/text/48/23.701 [last accessed at 28/5/2022];
12. CYBERTHREAT real-time map, at http://cybermap.kaspersky.com/ [last accessed at 9/5/2022];
13. Cyber crime, available at;https://www.techtarget.com/searchsecurity/definition/cybercrime [last accessed at 20/5/2022];
14. Cyber crime, available at https://www.techtarget.com/searchsecurity/definition/cybercrime [last accessed at 20/5/2022];
15. Cybercrime, available at https://illicittrade.org/cybervrime [last accessed at 23/5/2022];
16. Cybercrime and its impact on society, available at https://studycorgi.com/cybercrime-and-its-impact-on-society/ [last accessed at 12/6/2022];

17. INTERPOL report identifies top cyber threats, at https://www.interpol.int/en/News-and-Events/News/2021/INTERPOL-report-identifies-top-cyberthreats-in-Africa [last accessed at 24/3/2022];

18. Internet usage worldwide – statistics and facts, at https://www.statista.com/topics/1145/internet-usage-worldwide/ [last accessed at 24/3/2022];

19. Internet world stats: usage and population statistics; at https://www.intrnetworldstats.com/stats1.htm [last accessed at 24/3/2022];

20. Hamid Jahankhani, et al, 'Cybercrime classification and characteristics', researchget, 2014, available at https://www.researchgate.net/publication/280488873 [last accessed at 22/5/2022];

21. Humans of Data, available at https://humansofdata.atlan.com/2018, [last accessed 26/3/2022];

22. Joseph Aghatise, 'cyber crime definition', researchget, 2014, available at: https://www.researchgate.net/publication/265350281 [last accessed at 20/5/2022];

23. Maria Bada, 'The Social and Psychological Impact of Cyber-Attacks', Cybercrime Centre, 2019; available at https://arxiv.org/ftp/arxiv/papers/1909/1909.13256.pdf [last accessed at 12/6/2022];

24. Marco Gercke, 'Understanding cybercrime: phenomena, challenges and legal response', ITU, 2012, available at: www.itu.int/ITU-D/cyb/cybersecurity/legislation.html [last accessed at 20/5/2022];

25. Meserert Lakew, 'Computer Related Crime under Ethiopia: Comparative Study',…, PP. 1-42; at http:// www.abyssinialaw.com [last accessed 4/4/2022];

26. 40+ Cyber security Statistics and Facts For 2022, at https://www.websiterating.com/research/cybersecurity-statistics-facts/ [last accessed at 23/3/2022];

27. Saturation in qualitative research: exploring its conceptualization and operationalization; at https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5993836/ [last accessed at 30/3/22];

28. Status regarding Budapest Convention, available at: https://www.coe.int/en/web/octopus/country-wiki-ap/-/asset_publisher/CmDb7M4RGb4Z/content/ethiopia?_101_INSTANCE_CmDb7M4RGb4Z_viewMode=view [last accessed at 15/5/2022];

29. The computer is a crime machine, available at https://www.hg.org/legal-articles/the-computer-is-a-crime-machine-21217 [last accessed at 23/5/2022];
30. The Budapest convention and its protocols: available at https://www.coe.int/en/web/cybercrime/the-budapest-convention [last accessed at 26/5/2022];
31. The Budapest Convention on Cybercrime: a framework for capacity building, available at https://thegfce.org/the-budapest-convention-on-cybercrime-a-framework-for-capacity-building [last accessed at 27/5/2022];
32. United Nations conference on trade and development, Draft legal framework for cyber laws, 2008; available at http://repository.eac.int/handle/11671/1815 [last accessed at 16/6/2022];
33. What is computer crime? Available at https://www.geeksforgeeks.org/what-is-computer-crime [last accessed at 23/5/2022];
34. https://legaljobs.ic/blog/cyber-crime-statistics [last accessed at 11/6/2022];
35. https://www.pinsentmasons.com/out-law/news/extent-of-fraud-and-cyber-crime-laid-out-in-new-statistics [last accessed at 11/6/2022];
36. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016 [last accessed at 12/6/2022];
37. https://www.sbir.gov/tutorials/cyber-security/tutorial-1 [last accessed at 12/6/2022];
38. https://www.csis.org/analysis/economic-impact-cybercrime?amp= [last accessed at 12/6/2022];
39. https://www.africacert.org/ethiopia/ [last accessed at 29/6/2022];
40. https://www.coe.int/en/web/octopus/country-wiki-ap/-/asset_publisher/CmDb7M4RGb4Z/content/ethiopia?_101_INSTANCE_CmDb7M4RGb4Z_viewMode=view/ [last accessed at 29/6/2022];
41. https://ethiocert.insa.gov.et/web/guest/about-us [last accessed at 29/6/2022].

Annex

Annex – I - Interviews

BAHIR DAR UNIVERSITY

SCHOOL OF LAW

POSTGRADUATE PROGRAM

Criminal Justice and Human Rights Law program

This interview is meant for collecting data from respondents at INSA (legal officer and digital forensic division office), FDRE Ministry of Justice Federal Attorney General office, Organized and Trans-national as well as National Affairs Criminal Matters Directorate, and FDRE Police Commission crime investigation office to be used for LL. M thesis titled "*Effective Investigation and Prevention of Cyber Crime in Ethiopia: Assessment on the Legal and Practical challenges*" The information you give will be invaluable for the success of the research project. Hereby I assure you that all information obtained through this interview is to be used for academic purpose only and will be kept and stored with the highest order of confidentiality.

The researcher wants to, beforehand, forward his candid gratitude for your unreserved cooperation and willingness to contribute to the success of this work.

I. Interview Questions for Respondents from Information and Network Security Administration

- How do you explain the practice of investigation and prevention of cyber crime in Ethiopia?
- Do you think that the current cyber crime investigation and prevention is effective? Why/ why not?
- What legal challenges, do you think, hindered the effective the prevention and investigation of cyber crimes?
- What practical and institutional challenges, do you think, hindered the effective the prevention and investigation of cyber crimes?
- What measures should be taken to effectively investigate and prevent cyber crimes?

- Do you have any additional opinion related to the issue?

II. Interview Questions for Respondents from Federal Police commission

- How do you explain the practice of investigation and prevention of cyber crime in Ethiopia?
- Do you think that the current cyber crime investigation and prevention is effective? Why/ why not?
- If is not effective, what Practical and institutional factors, do you think, hindered the effective investigation and prevention of cyber crime?
- Do you think that the existing legislation dealing with the investigation and prevention of cyber crime are adequate or sufficient towards its effective implementation?
- Does your institution deliver capacity building trainings for police officers working on cyber crime investigation as to how effectively investigate and prevent cyber crimes?
- What measures should be taken to effectively investigate and prevent cyber crimes?
- Do you have any additional opinion related to the issue?

III. Interview Questions for Respondents Public prosecutor (MoJ)

- How do you explain the practice of investigation and prevention of cyber crime in Ethiopia?
- Do you think that the current cyber crime investigation and prevention is effective? Why/ why not?
- What legal challenges, do you think, hindered the effective the prevention and investigation of cyber crimes?
- What practical and institutional challenges, do you think, hindered the effective the prevention and investigation of cyber crimes?
- Pursuant to art 41 of proc no. 958/2016, does your institution request for or receive call for collaboration to or from another country for the sake of sharing information in cyber crime investigation?
- What measures should be taken to effectively investigate and prevent cyber crimes?
- Do you have any additional opinion related to the issue?

Annex -2- Questionnaires

BAHIR DAR UNIVERSITY

SCHOOL OF LAW

POSTGRADUATE PROGRAM

Criminal Justice and Human Rights Law program

This questionnaire is meant for collecting data from respondents at INSA digital forensic division, FDRE Ministry of Justice federal attorney general office Organized and Trans-national as well as National Affairs Criminal Matters Directorate, and FDRE Police Commission cyber crime investigation division, to be used for LL. M thesis titled "*Effective Investigation and Prevention of Cyber Crime in Ethiopia: Assessment on the Legal and Practical challenges*" The information you provide will be invaluable for the success of the research project. Please be honest and objective while filling the questionnaire. Hereby I assure you that all information obtained through this questionnaire is to be used for academic purpose only and will be kept and stored with the highest order of confidentiality.

N. B: Please do not write your name anywhere in the questionnaire.

☞ The researcher wants to, beforehand, forward his candid gratitude for your unreserved cooperation and willingness to contribute to the success of this work.

I. Open-ended questions for respondents from FDRE Ministry of Justice Organized and Trans-national as well as National Affairs Criminal Matters Directorate (Public prosecutors)

- Do you think that Ethiopian laws on cyber crime investigation and prevention is adequate and comprehensive? Why/ why not?
- What Practical and institutional factors, do you think, hindered the effective investigation and prevention of cyber crime?
- Have you ever taken trainings or educations as to how to effectively investigate and prevent cyber crimes? Do those trainings help you to improve your capacity of investigating and preventing computer crimes effectively?

- Have you ever conduct investigation and prevention process in collaboration with police officers and other concerned organs? If so, what difficulties do you observe?
- Do you have any additional opinion related to the issue?

II. Open-ended questions for respondents from Federal Police Commission (Police officers from cyber crime investigation division)

- Do you think that Ethiopian laws on cyber crime investigation and prevention is adequate and comprehensive? Why/ why not?
- What Practical and institutional factors, do you think, hindered the effective investigation and prevention of cyber crime?
- Have you ever taken trainings or educations as to how to effectively investigate and prevent cyber crimes? Do those trainings help you to improve your capacity of investigating and preventing computer crimes effectively?
- Have you ever conduct investigation and prevention process in collaboration with police officers and other concerned organs? If so, what difficulties do you observe?
- Do you have any additional opinion related to the issue?

III. Open-ended questions for respondents from INSA (digital forensic division)

- Do you think that Ethiopian laws on cyber crime investigation and prevention is adequate and comprehensive? Why/ why not?
- Have you ever taken trainings or educations as to how to effectively investigate and prevent cyber crimes? Do those trainings help you to improve your capacity of investigating and preventing computer crimes effectively?
- Have you ever conduct investigation and prevention process in collaboration with police officers and other concerned organs? If so, what difficulties do you observe?
- How do you express the existing cooperation with other countries in relation to cyber crime related investigation, prevention and other criminal issues?
- Do you think that the existing technological preparedness and infrastructure as well as capacity of professionals adequate to effectively investigate and prevent cyber crimes? Why/ why not?
- So, what other Practical and institutional factors, do you think, hindered the effective investigation and prevention of cyber crime?

Annex -3- Participants consent form

Research project: Effective Investigation and Prevention of Cyber Crime in Ethiopia: Assessment on the Legal and Practical challenges

Researcher name: Tinsae Seifu Alemayehu

I_________________ (print name) consent to participate in the research titled "*Effective Investigation and Prevention of Cyber Crime in Ethiopia: Assessment on the Legal and Practical challenges*" I understand that I am free to withdraw my participation in the research at any time and that if I do I will not be subject to any penalty or discriminatory treatment. The purpose of the research has been explained to me, and I have been given the opportunity to ask questions about the research. I understand that any information or personal details gathered in the course of this research about me are confidential and neither my name nor any other identifying information will be published without my written permission.

Signed by ____________________________________

Date __________________________