THE STATE OF CYBERCRIME GOVERNANCE IN ETHIOPIA

By Halefom Hailu

INTRODUCTION

Like many other countries, Ethiopia has embraced ICTs and ICT-based services as key enablers for social and economic development. Various additional efforts to significantly increase internet connectivity speeds and access are underway. Greater bandwidth will mean more than faster and better internet access, as greater bandwidth can also facilitate faster and better means of launching cyber-attacks and more opportunities for criminals to exploit naïve users.

This article will attempt to explore the efforts and initiatives being made by the government in fighting cybercrime from three cyberspace governance perspectives: cyber security-related policies and strategies, legislative frameworks, and institutional arrangements. Additionally, recommendations will be provided on what plans and measures the government can implement in pursuit of a safer and secure Ethiopia.

1. INFORMATION REVOLUTION AND THE NEW FORM OF CRIME: CYBERCRIME

In his book *The Third Wave*,¹ Alvin Toffler separates the history of the world into three waves: the agricultural wave, the industrial wave, and the information wave. Currently, the world is in “the third wave” of information technology.

Over forty percent of the world’s total population currently has access to the internet,² and more people are logging on every day. Nowadays, cyberspace has become so omnipresent that

---

² Available at: [http://www.internetlivestats.com/](http://www.internetlivestats.com/)
some have begun to employ the language of nationhood to describe it. If cyberspace were a country, it would be the largest and most populated country in the world.³

It is estimated that, by the year 2017, mobile broadband subscriptions will approach seventy percent of the world’s total population and, by the year 2020, the number of networked devices will outnumber people by six to one, transforming current conceptions of the internet.⁴

Technology is, however, neutral, and can empower those who build and those who destroy alike. As with every new invention, technology will always have its optimists who only see its potential to do good and its critics who only see its potential to do evil. Criminals have always been watchful of the possibilities of new technologies. Cyberspace thus presents us with not only great promise, but also with its potential to be transformed into a safe haven for criminals. Just as legitimate computer-based activities penetrate most aspects of life, the most confidential information held on computer systems is at the mercy of hackers and identity thieves.⁵ Furthermore, almost all traditional crimes can also be perpetrated from the online environment.

Millions of people are victims of cybercrime every day and suffer trillions of dollars in loss worldwide. As never before, and at insignificant cost, ordinary citizens can cause calamitous harm to individuals, companies, and governments from places unknown.⁶ The threat of cybercrime has reached the level of national security concern. For example, US President Obama declared that the “cyber threat is one of the most serious economic and national security challenges we face as a nation” and that “America's economic prosperity in the twenty-first century will depend on cyber security.”⁷ The UK government also declared that cyber security had become a ‘tier 1’ priority alongside international terrorism and major national

---

⁴ UNODC ‘Comprehensive Study on Cybercrime’ (February 2013).
incidents. In many cases, ICTs that are vital to national and economic security are subject to disruption from a number of causes originating from within a nation or outside its borders—cybercrime is the dark side of the information age.

But what constitutes cybercrime? Though it is one of the most pressing contemporary global issues and features considerably in political, legal, media, public, and academic discourse, the term cybercrime has no universally accepted definition. Defining cybercrime appears, therefore, to be a necessary evil within the community of people involved in researching, investigating, and prosecuting its occurrence. There are a number of interchangeable expressions and terms used to describe cybercrime, such as computer crime, internet crime, e-crime, digital crime, high-tech crime, online crime, and electronic crime.

There are even debates on the need for a definition of cybercrime. The metaphor of *old wine in new bottles* aptly depicts the argument that cybercrime is just a variant of traditional crime, and that there is no need to define a new category of crime. On the other hand, there are arguments seeking for a specific definition of cybercrime. This argument takes the view that, though some computer crimes could be prosecuted under existing criminal laws, computer networks enable the commission of entirely new types of crime such as hacking and denial of service attacks, which do not fit under any existing crime categories.

As this debate is ongoing, there neither an internationally recognized or standardized definition of cybercrime, nor is there a uniform usage of the term. Despite this, most proposed cybercrime definitions have a common denominator that involves the central role played by computer systems in the commission of cybercrime, i.e. computer systems are used as means to commit crime or are the targets of crime. This paper will use a working definition of cybercrime that considers it an act that covers the entire range of crimes involving computers, computer networks, or other digital technologies either as the crime’s target or its instrument.

---

11 Ibid.
2. CYBERCRIME IN ETHIOPIA

2.1. ETHIOPIAN CYBERSPACE PICTURE: INFORMATION SOCIETY AND INFRASTRUCTURE

Despite the fact that Ethiopia is still lagging behind compared to many developing countries, ICT penetration and usage is steadily growing. The potential for ICTs to increase economic growth and reduce poverty is well-supported, and Ethiopia has begun to embrace ICT use in its entire social, economic, and political structures. The government has made ICT development one of its strategic plan priorities.\(^\text{12}\)

Since this commitment, ICT penetration and usage in the country has grown steadily. The Ministry of Finance and Economic Development, in its Annual Progress Report for fiscal year 2011/12 Growth and Transformation Plan, reported that:

The number of mobile subscribers and telecom density for mobile lines increased from 10.7 million and 12.85 % in 2010/11 to 17.26 million and 20.4 % in 2011/12 respectively. Similarly, the coverage of wireless telephone service increased to 90 percent in 2011/12 even if the plan was to reach 63 %, while the number of subscribers and telecom density for fixed line declined from 0.854 million and 1.03 percent in 2010/11 to 0.805 million and 0.95 % in 2011/12 respectively. Generally, the total subscribers base has increased to 20.73 million at the end of 2011/12, of this internet subscribers has covered 2.661 million including mobile internet subscribers in the fiscal year.\(^\text{13}\)

There has also been a staggering increase in social networks users. Ethiopia’s young generation is logging in online every day. Recent reports show that as of 2012, there were over one million Facebook users, with forty-five percent of users between the ages of 18-40.\(^\text{14}\) According to a recent research paper from Trend Micro Incorporated, Ethiopia is in the top ten on the list of African countries with the largest number of Facebook users.\(^\text{15}\)

---

\(^{12}\) The FDRE National Information and Communication Technology Policy and Strategy 2009, section 1.


\(^{14}\) INSA, ‘Cybercrime in Ethiopia: conceptual study’ (May 2013) p.22.

subscriptions has also increased from 27,043 in 2011 to 30,372 in 2012.\textsuperscript{16} According to the Australia-based telecoms research company Budde Com, Ethiopia’s broadband market is set for a boom following massive improvements in international bandwidth, national fiber backbone infrastructure and 3G mobile broadband services.\textsuperscript{17} Recent reports show Ethiopia’s international internet bandwidth is better than many other African countries, as the country has been working towards improving its international bandwidth through international fiber optic links via Djibouti, Kenya, and Sudan.\textsuperscript{18} Ethiopia is Africa's second most populous country and, owing to the huge investments into the ICT sector being made by the government, there is a huge potential user base that could make Ethiopia the ICT hub of Africa in the very near future. Several ICT infrastructure development projects are underway, such as the construction of the EthioICT-Village, which is expected to generate ICT-related jobs for approximately 300,000 employees.\textsuperscript{19}

In addition to the development of infrastructure, the government of Ethiopia is also trying to promote and facilitate the extensive use of ICT and internet supported services. To this effect, the government adopted the e-Government Strategy in 2010, which planned the release of 211 e-services.\textsuperscript{20} Based on this strategy, a government portal has been launched, and several government agencies are providing their services online through the government portal. Such government agencies include the Ministry of Agriculture (MoA), Ministry of Foreign Affairs (MoFA), Ministry of Urban Development and Construction (MUDC), Food, Medicine and Health Care Administration and Control Authority (FMHACA), Agency for Government Houses (AGH), and Transport Authority.\textsuperscript{21}

\textsuperscript{16} FDRE Ministry of Communications and Information Technologies and ITU, ‘An Assessment of ICT Penetration and Usage’ (October 2012) P.7
\textsuperscript{18} FDRE Ministry of Communications and Information Technologies and ITU, ‘An Assessment of ICT Penetration and Usage’ (October 2012) P.7.
\textsuperscript{19} Available at: http://www.mcit.gov.et.
As digitalization and business automation increases, computer networks are becoming the nerve system of critical infrastructures. Now in Ethiopia, the use of ICTs is being embraced in the banking and financial sector. Though cash is still the most dominant medium of exchange, electronic-banking has begun to grow in Ethiopia. Electronic fund transfer was legally recognized for the first time in 2011. At this time, almost all banks in Ethiopia have core banking systems, mobile banking, and ATM services. The Ethiopian Commodity Exchange is also pushing out trading prices for key commodities countrywide through mobile phone messaging and internet-based services.

But reliance on computer systems and other digital technologies comes with vulnerability to cybercrime and cyber-attack. Therefore, as Ethiopia connects to the global network, it becomes vulnerable to cybercriminals operating in cyberspace.

2.2. The Reality of Cybercrime in Ethiopia

At the end of 2013, TREND Micro Incorporated published a report entitled “Africa: A New Safe Harbor for Cybercriminals?” In this report, TREND gave three reasons for identifying Africa as a potential cybercrime safe haven: 1) the availability of faster and more affordable internet access, 2) the expanding internet user base, and 3) the lack of cybercrime laws. The United Nations Conference on Trade and Development (UNCTAD) indicated that developing countries have become staging grounds for attacks by cybercriminals due to the greater prevalence of unprotected systems. Africa as a continent is therefore vulnerable to a range of online criminal activities and becoming a major source of cybercrime in the global information society. Furthermore, Africa has been criticized for lagging behind in curbing the threat of cybercrime.

Ethiopia is no exception. On one hand, the country is experiencing a massive increase in internet access, and its internet user base is expanding. On the other hand, cybersecurity

---

22 National Payment System Proclamation No.718/2011 art.19.
governance is at its embryonic stage, and much needs to be done. This creates an environment that could make Ethiopia a safe harbor for cybercrime.

As discussed above, the government of Ethiopia is working on the development of ICT infrastructures and ICT-based services. Better and faster ICT services, however, open opportunities for cybercrimes. The pervasiveness of mobile phones throughout the country, the introduction of new services such as mobile money, and financial services such as ATMs will also provide new opportunities for cybercriminals.

Despite the fact that no country can be immune to the threat of cybercrime, there is no consolidated report that shows the exact prevalence and impact of cybercrime in Ethiopia and to what extent the Ethiopian information society is vulnerable. This is partially due to the fact that companies and individual users do not report cybercrime incidents, do not keep organized records, and, in some cases, are not even aware that they are targeted by cybercriminals. Records from intelligence and law enforcement agencies are often either improperly recorded or inaccessible. Ethiopian-specific literature on the extent of cybercrime activities is also nonexistent. The inadequacy of the available statistics could lead to the over- or under-estimation of the threat of cybercrime to Ethiopia.

This report attempts to extract a better picture of cybercrime in the country based on a survey of institutions in Addis Ababa and their experience with cybercrime.

**Survey Results**

For the survey, data were collected from a set of questionnaires distributed to forty institutions familiar with the uses of ICT. Of the forty institutions, thirty-five responded, giving a response rate of 87.5%. Respondents were from both private and government institutions including seventeen banks, twelve ICT institutions, and six other institutions such as federal government agencies, media, and transport. The purpose of the questionnaire was to investigate the reality of cybercrime at the organizational level and examine how the institutions are vulnerable to the threat of cybercrime. The questionnaires covered four categories, encompassing areas such as:

- Reality and prevalence of cybercrime;
• Preparation of organizations to deal with cybercrime incidents;
• Reporting of incidents; and
• Perceptions on legislative, policy, and law enforcement measures.

Regarding the reality and prevalence of cybercrime, respondents were asked to indicate the forms of cybercrimes that were frequently or infrequently perpetrated against their respective institutions. It was found that all respondents experienced a number of cybercrime incidents. Computer viruses, worms, malware, or other malicious attacks (57.1 %), website defacement (40%), illegal access (17.1%), and spam (14.7%) were the most frequently perpetrated cybercrimes against the institutions. The respondents also indicated a range of infrequently occurring cybercrimes such as causing damage to computer data (62.9%), denial of service (DOS) (45.7%), and system interference (45.7%). Overall, the survey results demonstrate that cybercrime is a legitimate problem in Ethiopia. When one takes into account institutions’ lack of capability regarding cybercrime detection, it is valid to presume that cybercrime in Ethiopia is more prevalent than what is revealed in this survey.

A majority of the respondents (77.1%) also said that they do not have any organizational structure specifically dedicated to dealing with cybercrime threats. Only 8.6% of the institutions (three banks) have specialized teams responsible for cybersecurity incidents. These results demonstrate that cybersecurity governance is neglected by the majority of the institutions involved in the survey. The results may indicate that institutions as a whole are ill-prepared to deal with cybercrime.

The survey was also used to examine to what extent Ethiopian cybercrime incidents are reported to law enforcement agencies. As the survey reveals, most cybercrime against the institutions goes unreported. While more than half of the institutions said that they do not report at all, 25.7% said they report only major cyber-attacks, most of them related to banking fraud. The question is, therefore, what make institutions reluctant to report cybercrime? The survey provides some reasons for this reluctance, including the general belief that law enforcement is not capable of dealing with cybercrime (37.1%) and fear of adverse publicity (25.7%). Institutions are reluctant to disclose information on any cyber-attack for research
purposes for fear that news of an attack would destroy their reputations. There are even organizations (11.4%) who believe that the solutions for cybersecurity incidents are technical and hence out of law enforcement jurisdiction.

The Ethiopian government is currently forming cybersecurity policy measures with scattered pieces of legislation concerning cybercrime issues. In order to effectively protect themselves from cyber-attacks, organizations are expected to take full advantage of the current cybersecurity measures in the country. Unfortunately, the survey revealed that many institutions are not aware of the existing cybersecurity governance measures. For instance, out of thirty-five institutions, 57.1% said there is no national cybersecurity policy and strategy, and 22.9% responded that they were not sure whether Ethiopia has a cybersecurity policy and strategy, though such a policy and strategy exists. Only 20% were aware of the national cybersecurity policy and strategy. A similar result was found when the respondents were asked to evaluate the adequacy of Ethiopia’s existing legal framework to assist with the apprehension and prosecution of cybercriminals. While 22.9% of the institutions found the existing legal framework insufficient, 65.7% responded that no cybercrime law existed in Ethiopia. When asked if they perceived law enforcement as well-equipped (with expertise, tracing, detection and investigation tools, etc.) to counter cybercrime, most respondents answered in the negative.

**Technical Reports**

Other sources also show that cybercrime is a substantial threat to Ethiopia. For instance, KasPersky recently identified Ethiopia as the seventy-ninth most cybercrime-ridden country in the world.\(^{26}\) In a recent research paper, Trend Micro Incorporated identified the top ten most malicious URLs hosted in Ethiopia.\(^{27}\) As cybercrime occurs across boundaries and impacts users in different countries, it is inevitable that Ethiopia will be both the source and a victim of the problem.

---

\(^{26}\) Available at: <http://cybermap.kaspersky.com/>
Cybercrime is a real and growing threat to Ethiopians and the Ethiopian economy, and thus requires a comprehensive and systemic response. In the following section, this report examines how the Ethiopian government is responding to cybercrimes with special emphasis on three major cybercrime governance concerns: cybersecurity-related policies and strategies, legislative frameworks, and institutional arrangements.

3. THE STATE OF CYBERCRIME GOVERNANCE IN ETHIOPIA

3.1. POLICY MEASURES

3.1.1. THE NATIONAL ICT POLICY AND STRATEGY 2009

In 2009, the Ethiopian Government adopted a general ICT policy and strategy with cybersecurity implications. The ICT policy recognizes the need for the promotion of cybersecurity and more resilient network infrastructures. ICT security is identified as one strategic focus of the policy with the following specific objectives:

- To secure and safeguard the national electric communications system (national, institutional, and individual security);
- To enhance user confidence and trust within the public, as well as to protect both data and network integrity;
- To prevent, detect, and respond to cybercrime and misuse of ICT so as to contribute to the fight against national, regional, and international crimes such as fraud, organized crime, and terrorism;
- To address national security implications arising from the widespread application of ICT within the economy and society; and
- To build overall implementation, crime’s prevention, and controlling capacity of government bodies in charge of ICT policy implementation and monitoring.\(^{28}\)

\(^{28}\)Ibid.
3.1.2. The GTP 2010/11-2014/15

The growth and transformation plan (GTP) was formulated by the government in 2010 with the objective of enhancing the country’s vision of becoming a middle-income economy by 2020-2023. The development of ICT and telecommunication infrastructure is one of the strategic pillars of the GTP. To further this strategic pillar, the GTP states that the government is committed to ensuring the security of ICT service and protecting systems from cybercrime by creating an appropriate institutional framework (policy, law, and regulation) as well as developing organization and human resource capability.29

3.1.3. The National Information Security Policy 2011

The National Information Security Policy 2011 is the most important document regarding Ethiopian cybersecurity, for it is the first cyber-specific policy. It recognizes that Ethiopia is vulnerable to cybercrime and calls for a sense of urgency in reducing the threats and vulnerabilities. The policy also recognizes that cybersecurity is an integral part of national security, organizational security, public peace and security, and of the protection of basic rights and freedoms of citizens.30 The policy seeks to achieve the following major goals:

1. Build national capability for coordinated prevention, detection, response, and deterrence against threats and minimize the damage, cost, and recovery time from attacks that do occur;
2. Enable the country to use information as a means for implementing peace, democratization, social, and economic development programs;
3. Ensure the confidentiality, integrity, availability, and authenticity of national information assets;
4. Transform Ethiopia into an information-secure society that supports the development of a trustworthy and competitive information infrastructure.31

30 The FDRE National Information Security Policy 201, section 1
31 Ibid.
In furtherance of these goals, the policy identifies seven strategic pillars, including the adoption of appropriate legal and regulatory frameworks, the raising of public awareness, the promotion of information security education and training, the fostering of national cooperation and coordination, the promotion and strengthening of international cooperation, the enhancement of R&D towards self-reliance, and the protection of critical information infrastructures. Each strategic pillar has specific objectives and detailed implementation strategies.

3.1.4. The Criminal Justice Policy 2011

In 2011, the Ethiopia government adopted a new criminal justice policy. This policy recognized that Ethiopia is vulnerable to cybercrime and called for formulation of comprehensive national strategy, adoption of appropriate legislations, promotion and strengthening of international cooperation, and establishment of progressive capacity building programs for all organs responsible to prevent, detect, investigate, and prosecute cybercrimes. It is also recognized under this policy that new investigation techniques were required to respond to these new threats. Such new investigation techniques include interception of private communications with court warrants and without court warrants under exceptional circumstances provided by law.

The Ethiopian government is ready and committed to responding to the threat of cybercrime, at least at the policy level.

3.2. Institutional Regulatory Mechanisms

The adoption of legal and policy frameworks means nothing unless those frameworks are effectively implemented. This calls for the establishment of robust and specialized institutions. In the Ethiopian context, the government is working on the establishment of institutions dedicated to ensuring cybersecurity. As of yet, INSA is the only institution prominently featuring in the regulation of cybersecurity in Ethiopia. INSA was established in 2006 by the Council of Ministers Regulation No. 130/2006 and re-established in 2011 by Council of Ministers Regulation No. 250/2011 and Proclamation No. 808/2013. Now INSA is the sole cybersecurity organ in Ethiopia. Its objective is to ensure that information and computer-based key

---

32 Ibid.
34 Ibid.
infrastructures are secured, so as to be enablers of national peace, democratization, and development programs.\textsuperscript{35}

INSA is responsible for handling those cybersecurity issues with national security and critical infrastructure implications. Cybercrime is not, however, only a national security concern. It affects individuals and business of all levels, which requires either the expanded responsibility and outreach of INSA or the establishment of other specialized units, especially within critical infrastructures. INSA is also responsible for the establishment of a national computer and computer network emergency readiness and response team.\textsuperscript{36} Based on this power, INSA established Cyber Emergency Readiness and Response Team known as ETHIO-CERT in 2012.

The 2011 national information security policy states that Computer Emergency Response Teams (CERTs) should be established at the national level, in all critical infrastructures, and within government agencies. So far only ETHIO-CERT, which is now operating within INSA, is established. Furthermore, the policy required the establishment of specialized cybercrime units within police and public prosecutor departments, as well as the establishment of a specialized court bench. The telecom fraud offence proclamation No.761/2012 also required the establishment of a national technical task force. Despite these legal and policy declarations, however, these units have not yet been implemented. Law enforcement agencies do not have cybercrime units, no national technical task force is yet established, and there is no specialized court bench to hear cybercrime cases.

3.3. LEGAL FRAMEWORKS

3.3.1. THE FDRE CRIMINAL CODE 2004

Cybercrime-related legislation in Ethiopia is a recent development. The first legislative word on cybercrime in Ethiopia was the Criminal Code of the Federal Democratic Republic of Ethiopia 2004 (hereafter referred to as the Criminal Code), which came into existence as a revised version of the Penal Code of 1957. The Criminal Code criminalizes four malicious cyber acts:

\textsuperscript{35} Information Network Security Agency Reestablishment Proclamation No. 808/2013, art.5
\textsuperscript{36} Ibid, Art. 6 (6)
unauthorized access, causing damage to data, disrupting the use of computer services and misuse of computer devices.\textsuperscript{37} These provisions are incorporated in the Criminal Code under the chapter “Crimes Against Rights in Property,” meaning that the Criminal Code treats cybercrimes as property crimes. Now, however, technological developments have gone far beyond what the Criminal Code could have envisioned, changing the nature of cybercrime threats. Furthermore, given the dire impact of cybercrimes, the penalty clauses provided in the Criminal Code are too lenient.

In addition to this, enforcing anti-cybercrime laws in Ethiopia has become almost impossible. Despite the introduction of cybercrime provisions in the Criminal Code, prosecution based on these provisions is lacking. Could this mean that cybercrime has not yet infiltrated Ethiopia? This paper has already demonstrated that the answer is “no.” There are, however, several legal and practical constraints that hinder the investigation of cybercrimes and prosecution of offenders.

Even though the Penal Code of 1957 was replaced by the Criminal Code, and though the latter incorporates some cybercrime provisions, the Criminal Procedure Code Proclamation 1961 (hereinafter referred to as the Criminal Procedure Code), which was designed to enforce the Penal Code of 1957, was not amended. The rules in the Criminal Procedure Code are not suitable for use against cybercrime, as the Criminal Procedure Code was enacted in 1961, when the world was arguably unaware of cybercrime and computers were virtually unknown in Ethiopia. The incorporation of cybercrimes into the criminal code without amending its corresponding procedural aspect makes the investigation and prosecution of cybercrimes ineffective.

Further difficulty in fighting cybercrime lies with the capabilities of law enforcement. Law enforcement in Ethiopia is not yet equipped with the resources and expertise necessary for the investigation of cybercrimes and the prosecution of offenders. Instead, they rely on conventional investigation methods for fighting ordinary crime in order to identify, arrest, and prosecute cyber criminals. Cybercrimes, such as spam and malware, never entered the criminal

justice system, which shows that law enforcement in Ethiopia is not operating effectively in cyberspace. Very few cases, most of them relating to bank fraud, have reached the courts. These were either tried by extending the interpretations of old laws or closed for lack of evidence.

For example, in the case of Federal Ethics and Anti-Corruption Commission v. Michael Worku\(^3\) in 2012, the defendant was a bank clerk in Construction and Business Bank who used his privilege (access right) to create fictitious user IDs in order to transfer and withdraw 9.9 million Ethiopian Birr (more than 500,000USD) from different bank accounts. Though this was a cybercrime act, for the defendant created fake user IDs and hacked passwords, he was charged not under the computer-related provisions, but under Article 407 (1) (a) and (b) of the Criminal Code, which criminalizes abuse of power by public servants.

In the case of Federal Public Prosecutor v. Abraham Benti and Wendwesen Girma\(^4\), and Federal Public Prosecutor v. Mesele Yohannes,\(^5\) the defendants committed different cybercrimes by breaking into banking networks, misusing access codes (passwords), and withdrawing funds from cash machines using stolen PIN numbers. But these perpetrators were charged with “aggravated fraudulent representation” under Article 696 of the Criminal Code.

Other cybercrime-related cases were closed by the public prosecutor’s office due to lack of evidence.\(^6\) The reliance on vague interpretations of existing laws is not due only to the lack of appropriate laws, but also to law enforcement’s failure to enforce the existing cybercrime-related provisions.

3.3.2. Other Legislations with Cybercrime Implication

Three other pieces of legislations with cybercrime implications are also in force. They include the National Payment System Proclamation No.718/2011, the Registration of Vital Events and

\(^3\) Federal High Court File No.85025
\(^4\) Federal High Court File No.0075/05
\(^5\) Federal High Court File No.113949
\(^6\) Public prosecutor file No. 049/03 and file No. 296/04

Proclamation No.718/2011 was enacted with the objective of regulating and overseeing the national payment system of the country so as to ensure its safety, security, and efficiency. This law was enacted at a time when some banks in Ethiopia were introducing electronic payment systems such as ATMs.

The National Payment System Proclamation No.718/2011 was the first legislation to recognize electronic fund transfers and electronic signatures in Ethiopia. Despite this recognition, however, the law does not address the cybersecurity issues inherent to the electronic financial system. Only Article 35 of the law deals with unlawful acts and criminalizes forgery and fraud-related activities, specifically forgery of and fraud with payment instruments. The wording of Article 35, however, seems to deal only with conventional financial-related forgery and fraud crimes. This proclamation insufficiently addresses the full range of cybercrime activities emerging in the financial area.

The second legislation, Proclamation No. 760/2012, introduces the National Electronic Identity Card System. Even though the issuance of the electronic identity card has not yet begun, this law has very important provisions that deal with cybersecurity issues. Article 65 of the proclamation deals with some cybersecurity issues by stating that “information shall be protected from electronically designed attacks, theft, or from other similar criminal abuse (emphasis added).”

Article 66 provides punitive clauses for five to twenty-five years of rigorous imprisonment for cyber-related malicious activities such as the forgery, falsification, or unlawful accessing of identity cards or certificates of registration of vital events. Even though Articles 65 and 66 of this law make relevant provision for cybercrime issues, this law specifically deals with data related to vital events and national identity cards, and the full range of cyber-related criminal activities are not yet comprehensively addressed.

42Article 19 and Article 23 (3)
The third piece of legislation is Telecom Fraud Proclamation No. 761/2012, which criminalized the interception of, access of and interference with telecommunication networks, services, or systems without authorization. The law also outlawed the manipulation or duplication of SIM cards, credit cards, subscriber identification numbers, or data.43 This legislation, however, was rushed into law without public discussion and has been severely criticized on the grounds that it incorporates vague terms and overly punitive provisions.

These pieces of legislations deal with certain cybercrime issues in Ethiopia, but it is important to underscore the fact that none of these legislations comprehensively combat cybercrime. Either they are piecemeal legislations incorporated in other laws or they are too specific to be of use in all cybercrime cases. Thus, Ethiopia urgently needs comprehensive cybersecurity-specific laws. Recent measures indicate that the Ethiopian government is aware of the inadequacy of the current legislation and has been alarmed with the increase in the number of cybercrime attacks in the country. Accordingly, newer and more comprehensive cybercrime legislation has been drafted and is now under public discussion. Basic features of the new legislation are examined below.

3.3.3. The Draft Cybercrime Law

The cybercrime law was drafted by INSA and is currently under public consideration, and is expected to be approved by the parliament soon. The draft cybercrime law recognizes in its preamble that ICTs are vulnerable to various cybercrimes and other security threats that can impede the overall development of the country and endanger individual rights.44 It is also cognizant of the fact that the laws presently in force are not in tune with technological advancements and are not sufficient to prevent, control, investigate, and prosecute cybercrime.45 Accordingly, the draft cybercrime law has repealed the cybercrime-related provisions of the Criminal Code, as the draft cybercrime law is more comprehensive.46

43 Article 10 (1)
44 Preamble of the draft cybercrime law.
45 Ibid.
46 Draft cybercrime law Article 44.
1. Basic Principles of the draft cybercrime law

A. Principle of techno-neutrality

As clearly indicated in the explanatory report to the draft cybercrime law, a technology-neutral approach was adopted in drafting the substantive provisions, the justification being that using technology-neutral language allows the law to be applied to both current and future technologies involved in the commission of cybercrime. As Uchenna Jerome Orji stated in his recent book, Cybersecurity: Law and Regulation, this approach is the prevailing standard of international cybersecurity legislation, including the Council of Europe Convention on Cybercrime.

The Draft African Union Convention on the Establishment of a Credible Legal Framework for Cybersecurity in Africa 2011 also obliges member states to adopt the approved language of choice of international cybercrime legislation models. It seems that, in accordance with these international cybercrime legislation models, the draft cybercrime law has adopted technology-neutral language as a guiding principle. In addition to complying with international model laws, the adoption of a technology-neutral approach in the draft cybercrime law also makes its enforcement effective, as it will be comprehensible by laypersons and will not become obsolete with technological changes.

B. Principle of intentionality

Different jurisdictions require different approaches as regards the mental state of perpetrators. Whilst most countries view intention as a requisite for cybercrime acts, others hold that cybercrime can be committed both intentionally and through reckless behavior. In the draft cybercrime law, the intentionality requirement is incorporated into each substantive

47 “Technology-Neutral Approach” is a legislative drafting approach which focuses on the types of crime or types of behavior rather than on a particular type of technology used to commit the crime. This approach is adopted by international cybercrime model laws such as the Council of Europe Convention on Cybercrime and its purpose is to prevent newly enacted laws from quickly becoming outdated because of technological advancements.

48 Ibid.


provision. The justification stated in the explanatory report to the draft cybercrime law is that the risk of criminalizing reckless activities may be greater than the advantage, as this may result in unintentionally punishing the innocent conduct of ordinary computer users.

C. Limits on the Criminal Liability of ICT Intermediaries for Third Party Content

Every online transaction involves technical intermediaries. It is a widely recognized principle (seen, for example, in the EU Directive on Electronic Commerce 2000) that technical intermediaries should not be held criminally responsible in the event that it unknowingly distributes or hosts unlawful content created or uploaded by third party users. The draft cybercrime law also adheres to this principle, exempting internet service providers (intermediaries) from criminal liability for unlawful content created or uploaded by third party users. There are, however, some specific conditions under which service providers can be held criminally liable for third party content. According to Article 16 of the draft cybercrime law, an online service provider can be criminally liable if:

(1) It is directly involved in the publication or edition of the content, or
(2) Upon obtaining actual knowledge that the content is illegal, it failed to take any measures to remove or disable access to the content, or if
(3) Upon obtaining notice from competent administrative authorities to remove or disable access to the content data, it failed to take appropriate measures.

Accordingly, a service provider cannot face criminal liability under the draft cybercrime law if it was an innocent disseminator or if it only transmitted data without knowledge of content.

D. Principle of internationality

In cyberspace, distance is not a concern, and thus cybercrime can be perpetrated from anywhere in the world. Adequately fighting these crimes requires international cooperation.

\[51\] Explanatory Report to Draft cybercrime law (INSA, 2013) p.4
\[52\] Ibid.
\[53\] Ibid Article 16.
\[54\] Ibid Article 16 (1-3).
The draft cybercrime law is designed in cognizance of this requirement and declares under Article 25 that:

The investigatory authority shall cooperate with competent authorities of another country in taking appropriate measures to provide assistance in matters concerning cybercrime, including the exchange of information, joint investigations, extradition, technical assistance in accordance with this Proclamation, and agreements to which Ethiopia is a party and within the limits of the country’s legal system.55

Despite recognition of the need for international cooperation, the draft cybercrime law does not address the details of cooperation, unlike international cybercrime models such as the Council of Europe Convention on Cybercrime.

2. Criminalization

The first part of the draft cybercrime law deals with definitions of set of terms and phrases, but the draft cybercrime law does not provide any definition for what constitutes cybercrime. It instead categorizes and criminalizes set of malicious activities. Though it does not have provisions that criminalize offences related to the infringement of copyright and other related rights, the draft cybercrime law adopted the Council of Europe Convention on Cybercrime mode of classification. Accordingly, the draft cybercrime law, in its second part, classified the substantive provisions into three categories of cybercrime acts:

Section one (Articles 3 through 8) includes provisions for crimes such as illegal access, illegal interception, interference with computer systems, damage to computer data, and misuse of computer devices. The explanatory report states that section one of the draft cybercrime law is designed to protect the confidentiality, integrity, and availability of computer systems, networks, and data from malicious attack.56

Section two (Articles 9 through 11) is about “computer-related forgery, fraud, and theft,” which are ordinary crimes already listed in the Criminal Code. The explanatory report justified the

---

55 Ibid Article 42
56 Explanatory Report to Draft cybercrime law (INSA, 2013) p. 9
incorporation of these crimes in the draft cybercrime law, stating that the provisions in the Criminal Code are not sufficiently address situations involving computer networks.\(^{57}\)

The third section (Articles 12 through 16) covers content-related cybercrimes such as child pornography and child grooming, cybercrimes against liberty and reputation of persons (under which headings fall such crimes as cyber stalking, online harassment, blackmailing, and defamation), dissemination of spam, and cybercrimes against public security. As these criminal categories directly relate with competing interests such as the freedom of expression, they need to be narrowly interpreted. International standards require that any interference with freedom of expression must meet strict requirements provided by law.\(^{58}\) Unless strict requirements are followed, law enforcement may interpret these provisions vaguely so as to deny discussions of matters of public concern.

### 3. Procedural Provisions

The criminalization of malicious acts is not an end unto itself. Appropriate mechanisms for investigation and prosecution of the offences must be laid down. The new technological environment poses challenges not only to substantive law but also to procedural and investigative techniques. Procedural mechanisms and investigative techniques must keep abreast of the technological environment. In this regard, the draft cybercrime law goes one step further, incorporating all the procedural aspects of cybercrime as provided in international cybercrime models such as the Council of Europe Convention on Cybercrime and the International Telecommunication Union (ITU). In addition to the traditional procedural mechanisms, the draft cybercrime law entrusts law enforcement authorities with new, computer-specific powers (Articles 21 through 36), which include the preservation order of stored computer data, production order, access, search and seizure of computer data, and real-time collection of computer data. The explanatory report states that these procedural and

---

\(^{57}\) Ibid p. 20

\(^{58}\) See the Council of Europe Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems 2003(ETS No. 189)
investigative techniques are applicable to all types of computer data in general and to traffic data, content data, and subscriber data in particular. The definitions of traffic data, content data, and subscriber data are also provided in sub-Articles 5, 6, and 7 of Article 2 respectively. As these new measures entrust the investigatory authority with new powers, there is a need for balance with other competing interests such as the right to privacy. It is important, therefore, to examine these new investigative powers and how the draft cybercrime law attempts to balance them with basic human rights.

Under Article 29 (1), the draft cybercrime law empowers the investigatory authority to order a person to preserve specified computer data in that person’s possession or control for up to three months and to keep such an order confidential. This provision lacks independent judicial review. In the explanatory report, two justifications are provided for such arrangement. These are:

1. Due to the volatile nature of computer data, preservation orders must be given quickly and should not wait for the legal process, and
2. The preservation order does not compel the disclosure of any computer data, and thus there are no privacy concerns.

Article 29 (1) of the draft cybercrime law states that the investigatory authority can exercise the power of a “preservation order” only if the following cumulative prerequisites are met: the computer data must be necessary for cybercrime investigation, the computer data to be preserved must be for a specific case or computer data must be specified, and the investigatory authority must have reasonable grounds to believe that specific data is vulnerable to loss or modification. It can be argued that these requirements are limitations on the investigatory authority and thereby play a balancing role between individual privacy and investigative powers.

59 Art. 2 (3) defined Computer data as “any content data, traffic data, computer program or any other information in a form suitable for processing by means of a computer system”.
60 Explanatory Report to Draft cybercrime law (INSA, 2013) p.20
61 Draft cybercrime law, Article 29(2)
62 Explanatory Report to Draft cybercrime law (INSA, 2013) p.26
Another investigative power as provided under Article 30 of the draft cybercrime law is the “production order.” According to this provision, the investigatory authority is empowered to order a person to submit specified computer data in that person’s possession or control. Unlike the preservation order, a production order requires the disclosure of data and is therefore privacy sensitive. The draft cybercrime law has accordingly made this investigative power subject to judicial warrant.63

Article 31 of the draft cybercrime law also entrusts the investigatory authority with specific powers to search or otherwise access computer systems, networks, computer data, or computer-data storage media. This investigative power refers to both physical and virtual search or access and is subject to prior judicial warrant.64 The draft cybercrime law recognizes that data that is physically stored in another computer system or storage device can be legally accessed through the searched computer system by establishing a connection with other distinct computer systems. Investigatory authorities have the power to extend a search to that other computer system without requesting a separate search warrant.65 The process of searching computer data, systems, networks, or any other computer data storage device is not an easy task. In the execution of this investigative power the investigatory authority may, for example, face technical difficulties, such as encryption, that may hinder the investigation process. To uncover these practical problems of search, seizure, and access, international cybercrime model laws such as the Council of Europe Convention on Cybercrime 2001 adopted a new investigatory power that enables competent law enforcement agencies to order any person with knowledge of a system’s function or protective measures to, when reasonable, disclose this information in order to enable search, seizure, or access.66 The draft cybercrime law also adopted this approach under Article 31 (4). This provision is, however, problematic, in that it is not clear whether or not the order includes the accused. If it is interpreted in such a way as to include the accused, it contravenes the constitutional guarantee against self-incrimination.

63Article 30 (1)
64Article 31 (1)
65Article 31 (2)
66Council of Europe Convention on Cybercrime 2001(ETS No. 185) Art. 19 (4)
Real-time collection of computer data, which is useful to obtain computer data that exists only in transient communications, is another new investigative measure adopted by the draft cybercrime law. This investigative power is also subject to independent judicial review, because the real-time collection or interception of computer data is privacy-sensitive. Under exceptional circumstances, however, the draft cybercrime law allows the real-time collection or interception of computer data without prior court warrant.

4. Conclusion and Recommendations

Though it has not been yet fully integrated into everyday aspect of life, the use of ICTs and ICT-supported services are embraced by the Ethiopian government, individuals, and businesses. As the government of Ethiopia continues developing ICT infrastructures and ICT-based services, reliance on these services will continue to grow. Reliance on computer systems and other digital technologies brings an increased vulnerability to cybercrime and cyber-attack. The Ethiopian government is aware of the threats from cyberspace and is working towards curtailing these threats though policies, institutions and legislation. These efforts, however, are still at their initial stages and inadequate for the ever-changing cyber environment and the growing threat of cybercriminals.

The current state of affairs of cybersecurity in Ethiopia should not be allowed to continue, because cybercrime is thriving. To strengthen cybersecurity governance in Ethiopia, comprehensive work must be done. This report provides the following recommendations:

- Cybercriminals take advantage of jurisdictions that lack comprehensive legal frameworks on cybersecurity in general and cybercrime in particular. Ethiopia must speed up its comprehensive proposed cybercrime law while avoiding the piecemeal and scattered legislation approach, which slows down enforcement and interpretation.

- Laws alone will not suffice in preventing or investigating cybercrime. The Ethiopian law enforcement authorities ought to be adequately equipped with the necessary legal, technical, and human resources. Law enforcement officials should be updated on
emerging trends of cybercrimes by participating in regular and special cyber-training courses.

- Combating cybercrime is an extraordinarily difficult task that requires coordinated and focused efforts. Specialized units within law enforcement agencies should be established to effectively detect, investigate, and prosecute cybercrimes.

- Among the problems in detecting and investigating cybercrime lies the fact that those victims of cybercrime do not always notice that they are being victimized. The author suggests that the Ethiopian government and law enforcement agencies should promote cybercrime awareness and establish effective means to offer tips for safety online and provide timely information regarding cybercrime to the public. It is also recommended that the Ethiopian government establish accessible, user-friendly reporting mechanisms.

- Finally this report recommends for the topicality of the issue of cybercrime across all stakeholders including law enforcement, academia, business, civil society, and end users. In this regard, the government should support research, forums, and workshops held on the issue of cybercrime.
REFERENCES

Books

Cases

1. *Federal Ethics and Anti-Corruption Commission v. Michael Worku* (Federal High Court File No.85025)
2. *Federal Public Prosecutor v. Abraham Benti and Wendwesen Girma* (Federal High Court File No.0075/05)
3. *Federal Public Prosecutor v. Mesele Yohannes* (Federal High Court File No.113949)
4. *Federal Public Prosecutor v. Morisnda Kiyote* (Federal First Instance Court File No. 085/04)
5. *Federal Public Prosecutor v. Nahom Asefa* (Federal First Instance Court File No. 584/04)
6. *Public prosecutor file No. 049/03 and file No. 296/04*

International laws

1. Council of Europe Convention on Cybercrime 2001 (ETS No. 185)
3. ITU Toolkit For Cybercrime Legislation 2010

National laws and policies

2. Draft cybercrime law 2013
5. The Criminal Procedure Code Proclamation 196
7. Telecom Fraud Proclamation No. 761/2012.
8. The FDRE Growth and Transformation Plan 2010/11-2014/15

Reports/ Literatures/ Articles/ Journals
3. Explanatory Report to Draft cybercrime law (INSA, 2013)
4. FDRE Ministry of Communications and Information Technologies and ITU, “An Assessment of ICT Penetration and Usage.” (October 2012)
10. ITU “Global cyber security agenda (GCA) high-level experts group (HLEG) global strategic report.” (Geneva, Switzerland, 2008)
22. UNODC “Comprehensive Study on Cybercrime.” (February 2013).
23. World Bank, “Ethiopia Economic Update II: Laying the Foundation for Achieving Middle Income Status.” (June 2013)

Websites

APPENDIX:
APPENDIX A- CONSENT FORM

RESEARCH PROJECT: THE STATE OF CYBERCRIME GOVERNANCE IN ETHIOPIA
Researcher: Halefom Hailu

e-mail: halefom03@gmail.com

I_________________ (print name) consent to participate in the research titled “THE STATE OF CYBERCRIME GOVERNANCE IN ETHIOPIA.” 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 used or published without my written permission.

Signed by ________________________________

Date ________________________________
## Appendix B - Survey

### A. Respondent profile
- ICT /Telecommunication
- Banking /Finance
- Other (federal government agencies, medias, and transport)

### B. Reality and prevalence of cyber crime
1. Please indicate all of the cyber security incidents (cybercrime) committed against your organization and the frequency with which they occur.

<table>
<thead>
<tr>
<th>Type of Cyber-Crime</th>
<th>Occur Frequently</th>
<th>Occur Infrequently</th>
<th>Has not occurred</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Illegal access (hacking, cracking, illegal intrusion into computer systems or other unauthorized use of computer data, system of network)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Virus, worm, malware or other malicious code</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Computer-related fraud (e.g. ATM fraud, telecom fraud), forgery, phishing (someone posing as your organization online in an attempt to gain personal data from your customer or employee)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Causing Damage to computer Data (disruption, destruction, detection, alteration, suppression modification, etc of data)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Identity theft</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Website defacement</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Illegal system interference (hindering, blocking, impeding, interrupting, or impairing the processing or functioning of your system)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. Denial of service (DOS)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9. Spamming</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
10. Theft of sensitive data

11. Illegal interception of computer data

2. Where is the threat of cyber security incidents (cybercrime) coming from (Source of incident)?

<table>
<thead>
<tr>
<th>Type of Cyber-Crime</th>
<th>Source of incident</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>insider</td>
</tr>
<tr>
<td>1. illegal access (hacking, cracking, illegal intrusion into computer systems or other unauthorized use of computer data, system of network)</td>
<td></td>
</tr>
<tr>
<td>2. virus, worm, malware or other malicious code</td>
<td></td>
</tr>
<tr>
<td>3. Computer fraud (e.g. ATM fraud), computer forgery, phishing (someone posing as your organization online in an attempt to gain personal data from your customer or employee)</td>
<td></td>
</tr>
<tr>
<td>4. Causing Damage to computer Data (disruption, destruction, detection, alteration, suppression modification, etc of data)</td>
<td></td>
</tr>
<tr>
<td>5. identity theft</td>
<td></td>
</tr>
<tr>
<td>6. website defacement</td>
<td></td>
</tr>
<tr>
<td>7. illegal system interference (hindering, blocking, impeding, interrupting, or impairing the processing or functioning of your system)</td>
<td></td>
</tr>
</tbody>
</table>
3. Please indicate all types of losses your organization experience as a result of cyber security incidents (cybercrime)?
   A. Operational losses (downtime)
   B. Financial losses (including Recovery, Detection, Containment, Investigation, Ex-post response and Incident mgmt expenses)
   C. Harm to reputation
   D. Theft of sensitive data
   E. Loss of intellectual property
   F. Other
   G. no losses experienced
   H. Don't know/ not sure

4. Has the number of cyber security events experienced by your organization in the past 12 months increase, decrease or remain the same, when compared to the prior 12 months?
   a. increase
   b. decrease
   c. remain the same
   d. not known

C. Capacity and preparation of organizations to deal with cyber crime incidents

5. How would you describe information (cyber) security policy within your organization?
   a. No policy at all
   b. Informal policy
   c. Formal policy is established

6. Have your organization established any specialized team dedicated exclusively to the detection, prevention tracing or/and investigation of cyber-crimes incidents?
   a. yes
b. no
   c. Don't know/ not sure

7. Does your organization have a formalized plan outlining procedures for reporting and responding to security events committed against your organization?
   a. Yes
   b. No
   c. Don't know/ not sure

8. Are cyber crime risks being reviewed by your Management?
   a. not at all
   b. annually
   c. Ad hoc basis
   d. frequently (less than annually)

9. How frequent does your organization perform formal cyber security test/audit?
   a. not at all
   b. annually
   c. Ad hoc basis
   d. frequently (less than annually)

10. Is your organization more prepared or less prepared to deal with (prevent, detect, respond, recover) cyber security threats today compared to 12 months ago?
    a. More prepared
    b. Less prepared
    c. Same level of preparedness

D. Reporting of incidents

11. Which type of cyber security incident (cyber crime) does your organization report to the law enforcement?
    a. all incidents
    b. only major incidents
    c. not reported at all
    d. Don't know/ not sure

12. Reasons for not reporting cyber security incidents to law enforcement.
    a) your organization believes cyber security incidents are outside law enforcement jurisdiction
b) Do not believe law enforcement is equipped to deal with cyber security incidents (cyber crimes)
c) Negative publicity (reputational damage)
d) Incident(s) were too small to report
e) Competitors would use news of intrusion(s) to their advantage
f) Other

13. How do you describe the reporting mechanism of cyber incidents in Ethiopia?
   a. there is no established reporting mechanism
   b. very effective
   c. effective
   d. not effective
   e. do not know

E. Perceptions on legislative, policy and law enforcement measures

14. Do you know the existence of national information (cyber) security policy in Ethiopia?
   a. yes
   b. no
   c. not sure

15. How do you evaluate the existing Ethiopian legal frameworks regarding cyber crime?
   a. sufficient
   b. partly sufficient
   c. not sufficient at all
   d. there is no cyber crime law in Ethiopia

16. How do you describe the capability of law enforcement to combat cyber crime (expertise, tracing, detection and investigation tools)?
   a. not equipped at all
   b. less equipped
   c. equipped
   d. very equipped
   e. not sure