ST. MARY'S UNIVERSITY COLLEGE

FACULTY OF LAW

COMPUTER CRIMES
UNDER THE ETHIOPIAN CRIMINAL CODE
CHALLENGES AND PROSPECTS

BY

CHERINET MULATU DAGO

JULY, 2008
ADDIS ABABA

COMPUTER CRIMES
UNDER THE ETHIOPIAN CRIMINAL CODE
CHALLENGES AND PROSPECTS

BY: CHERINET MULATU DAGO

ADVISOR: ELIAS N. STEBEK

Submitted in partial fulfillment of the requirements for Bachelor Degree of Law (LL.B) at the Faculty of Law St. Mary's University College

JULY, 2008
ADDIS ABABA

ACKNOWLEDGMENTS

A great deal of time and effort has been devoted to appear this thesis in its final form and I take this opportunity to express to all those, who have shown me their kind co-operation.

First and for most, I would like to tank my Advisor Ato Elias Nour for the time taken in reading both drafts and Final version of this paper and for his valuable comments and suggestions that were given.

It is also my pleasure to tank my brother Ayalew Mulatu for his commitments and patience while editing this paper. Like wise I would like to tank my uncle Gedamu Tekele for his general comment and suggestion that were given.

Moreover, thanks are extended to my mother and my sisters to all my families for their grateful assistance and moral support in all different manners.

Last but not least, I want to express my gratitude to those who are not mentioned their name in this acknowledgment, to their kind assistance and co-operation and valuable comments. Their assistance was critical to the preparation of this thesis.

Table of Contents

INTRODUCTION

Chapter 1

COMPUTERS IN GENERAL

Chapter 2

THE ETHIOPIAN CRIMINAL CODE PROVISIONS AND THE COMPUTER

Chapter 3

CHALLENGE TO CONTROL COMPUTER CRIME IN ETHIOPIA

Chapter 4

COMPUTER SECURITY IN COMBATING COMPUTER CRIMES AND THE PROSPECT

Statement of Declaration

I here by declare that the paper is my original work, and I will take full responsibility for any failure to observe the conventional rules of citation.

Name: CHERINET MULATU DAGO

Signature:

INTRODUCTION

Computer, perhaps the most creative and powerful invention in the humankind's history, was invented in 1946 in the United States. As soon as the computer was created the whole world had to confront and try to overcome a new challenge-computer crime.[1]

The definition of computer crime, in a certain sense, is flexible, depending on whom you speak to, the definition can encompass anything from those activities which would require a system programmer's skills to perpetrate right through to any activity in which a computer is somehow involved.[2] But this crime, against information on computers, is beginning to claim attention in most countries around the world, in different ways. However, the existing laws regarding computer crimes are likely to be unenforceable due to different reasons.[3] The problems that make the crime unenforceable were various. For instance, lack of instant knowledge about the crime, luck of jurisdiction regarding on web based crime, and luck of attention to the crime was the main reasons that worth mentioning.

When we see the victims of such crime, we must put in mind that the targeted victims of such nature of the crimes. For instance, those who believe but simply, have not been awakened by the Nature of the crime and slow down experience of the crime from governmental authorities, non governmental bodies, trade organizations and individuals are the target victims.

By considering this fact, the Year 2004 Ethiopian criminal code, gives due attention to the crimes of computer. And it considered, as if it is the best provisions to control the crimes that are related to computers. However, promulgating such nature of criminal provisions needs more potential and capacity than any other crime. And have more challenges in order to implement the law too.

Therefore this paper planned to show the nature computer crime in general and give explanation on the specific provisions of the criminal code provisions. And also, attempt to show the challenges to Control the crime. In addition, it shows the importance of computer security measures in Ethiopia and the prospect regarding combating computer crimes in the country.

[1] http://www.fsu.edu/.htm, which contains computer crimes in general (Accessed on 25, Jan 2008 G.C)

[2] http://www.fsu.edu/~crimdo/TA/hao/computer%20crime2.htm (Accessed on 25, Jan 2008 G.C)

[3] www.mcconnellinternational.com, Accessed on 25, Jan 2008 G.C)

CHAPTER ONE

COMPUTERS IN GENERAL

We are living in an information age dependent upon digital information. Digital information is electronic information, the result of computer processing. Every type of job relies upon getting information, using it, managing it, and relaying information to others. Computers enable the efficient processing and storage of information. We do not think of a computer merely as the machine with the keyboard and the mouse, although that might be true for some types of computers.

Almost all of us are involved in some fashion, with computers on the daily basis. They are in the cars we drive. The televisions we watch the clocks that tells us the time, the microwave ovens that heat up food and, of course, in the machines that populate many of our desktops. Without computers, life would certainly be a lot different. Computers, however, are relatively new on the human scene. We can measure civilization in thousands of years and the industrial revolution in hundreds. Yet computers have only been around for tens of years. This relative newcomer has been quick to take hold, dig in, and proliferate.[1]

Most people know that a computer is a fast calculator, but it is much more than that. It is a machine which performs fast calculations plus performs burdensome chores such as choosing, copying, moving, comparing and performing other operations on alphabetic, numeric and other symbols which represent data (raw material of information).[2]

Today Computers plays a major role in the modern society. And all computers have certain common characteristics irrespective of their type and size. Computers are not just adding machines; they are capable of doing complex activities and operations. They can be programmed to do complex, tedious and monotonous tasks too.[3]

[1] S.CHAND'S AND D.P. NAGPAL, "Computer Fundamentals" S.CHAND AND COMPANY LTD, (2004), (Page1)

[2] Ibid

[3] R. Sarvana Kumar, R. Parames Waran, T. Jayalakshmi (2005), *"A Text Book of Information Technology"* S. Chand and Company Ltd, (Page 8)

1.1 USES OF COMPUTERS

Let's ask a simple question and answer about personal computer. What are the uses of computers in daily life? But one can give different answers by saying to Email friends, to check out news online, to play games, to write reports and papers or to upload pictures, communicate with business partners or he/ she can answer they use computer to prepare presentation. However we can say that by using computer we can accomplish a multifarious function with in a short period of time.

People use computers in many ways. Stores use computers to keep track of products and check you out at the cash register. Banks use computers to send money all over the world. Computers help teachers keep track of lessons and grades. They help students do research and learn. Computers let you hook up to networks (many computers hooked together). They let you hook up to a worldwide network called the Internet.[4]

Scientists use computers to solve research problems. Engineers use computers to make cars, trucks, and airplanes. Architects use computers to design houses and other buildings. The police use computers to track down criminals. The military uses computers to make and read coded messages.[5]

The computer is a truly amazing machine. Few tools let you do so many different tasks as computers do. Whether you want to publish newsletter design a building or play games, you can do it with a computer.[6] But in general, computers have the ability to provide new time dimensions for the working day and for the human concept. They provide efficient and effective controls over human errors, provide large capacities to store information and the capability to rapidly access this information, perform complex and repetitive calculation rapidly and accurately, hold program of a model which can be explored in many different areas, make decisions of the basis of given condition. They can correct and modify certain parameters automatically, provide meaningful information to the user and able to draw and print graphs, and

[4] . Microsoft ® Encarta ® 2007. © 1993-2006 Microsoft Corporation.

[5] . Ibid

[6] . Leon and Mathews Leon,(1999) " Fundamentals of Information Technology" Leon Press, Chennal and vikas publishing House Pvt. Ltd. New Delhi (page 1.4)

also they verify and accurately work by means of parity check. i.e. it counts the number of characters it has in storage to makes sure that there is no loss of data during processing.[7]

1.2 THE KEY COMPUTER TERMINOLOGY IN THE ETHIOPIAN CRIMINAL CODE PROVISIONS

A. COMPUTER DATA

A computer is an electronic machine, operating under the control instructions stored inside its memory. As an aid in problem solving, It accepts data both numeric and non numeric, process and presents it in the desired form.[8]

Data refers to a collection of organized information, usually the results of experience, observation or experiment, or a set of premises. This may consist of numbers, words, or images, particularly as measurements or observations of a set of variables. Raw data are numbers, characters, images or other outputs from devices to convert physical quantities into symbols, in a very broad sense. Such data are typically further processed by a human or input into a computer, stored and processed there, or transmitted (output) to another human or computer. Raw data is a relative term; data processing commonly occurs by stages, and the "processed data" from one stage may be considered the "raw data" of the next.[9]

B. COMPUTER NETWORK

The text book of information Technology written by R. Sarvana Kumar and other define Network on the following manner. “Net work is nothing but techniques, physical connections, and computer programs used to link two or more computers.” Network users are able to share files, printers, and other resources, send electronic messages and run programs or other computers.

As to the internet free encyclopedia called Wikipedia, interpretation Computer networks may be classified according to the scale: Personal area network (PAN), Local Area Network (LAN),

[7] . Cited at note 3, “A Text Book of Information Technology”, (Page 9)

[8] . Cited at note 3, “*A Text Book of Information Technology”*, (Page 9)

[9] . http://en.wikipedia.org/wiki/Data (Accessed on 01, Apr, 2008 G.C)

Campus Area Network (CAN), Metropolitan area network (MAN), or Wide area network (WAN). These different Networks are also explained in brief on this free encyclopedia of Wikipedia web page. These are:-

1. Personal area network (PAN) is a personal area network (PAN) is a computer network used for communication among computer devices close to one person. Some examples of devices that may be used in a PAN are printers, fax machines, telephones, PDA's or scanners.

2. Local Area Network (LAN) A network covering a small geographic area, like a home, office, or building. For example, a library will have a wired or wireless LAN for users to interconnect local devices (e.g., printers and servers) connects to the internet.

3. Metropolitan area network (MAN), A Metropolitan Area Network is a network that connects two or more Local Area Networks.

4. Wide area network (WAN) A WAN is a data communications network that covers a relatively broad geographic area (i.e. one city to another and one country to another country) and that often uses transmission facilities provided by common carriers, such as telephone companies.

C. COMPUTER SYSTEMS

A computer system is a combination of various components. It performs the system functions in input, processing, output, storage and control.

For instance, Hardware is those components or physical pieces that make up the computer. Hardware is those things you can touch. These shows different pieces of the computer's hardware: monitor, speakers, mouse, CDROM, hard drive, keyboard, CPU, RAM, Processor, etc. Each piece plays a role in the operation of a computer. And also, on a computer system, there is software that makes our computer do things for us.

Software's consist of computer programs, which are sequences of instructions for the computer. The process of writhing programs called Programming and individuals who perform this task are called Programmers.[10]

The computer without software would be like a home entertainment system with no tapes, CD's, or movies - you have the machine, but there's nothing to play on it.[11]

[10] Efraim Turban, R. Kelly Rainer, jr, Richard E. Potter, "Introduction to information technology (2nd edition)" (2003), John Wiley and sons. Inc. (Page 95)

[11] "Introduction to Computers", A Workshop for San Diego State University Faculty and Staff, 2000.San Diego State University.

But in general when we see a computer system, The Computer is able to do nothing until it is instructed by software. Besides, computer hardware is nothing without the support of such software’s. This software enables the user to give order to the computer in any task that is designed to be performed.

1.3 COMPUTER CRIMES

Why the great concern about computer crime? First, history teaches that criminals will frequently abuse new technologies to benefit themselves or injure others. Automobiles are an apt example. Designed to provide transportation for law-abiding individuals, the automobile soon became a target (e.g., car theft, carjacking), a tool (e.g., the getaway car in a bank robbery), and a weapon (e.g., hit-and-run). Clearly, computers are following the same route.[12]

Computer crime denotes the use of computers by individuals in one of three ways. First, a computer may be the target of the offense. In these cases, the criminal's goal is to steal information from, or cause damage to, a computer. Second, the computer may be a tool of the offense. This occurs when an individual uses a computer to facilitate some traditional offense such as fraud or theft (for example, a bank employee may use a computer program to skim small amounts of money from a large number of bank accounts, thus generating a significant sum for personal use). Third, computers are sometimes incidental to the offense, but significant to law enforcement because they contain evidence of a crime. Narcotics dealers, for example, may use a personal computer to store records pertaining to drug trafficking instead of relying on old-fashioned ledgers.[13]

There are number of ways in which computers can be used for crime. For instance, they used to commit "real-world" crimes, such as forgery, fraud or copyright piracy or they used to damage or modify other computerized systems and others.

A computer crime research center of the United States November 26, 2005 article defines computer crimes as, Fraud achieved by the manipulation of computer records. Such as, spamming, computer security systems, unauthorized access to or modification of a programs,

[12] . Scott Charney and Kent Alexander, “COMPUTER CRIME”, Computer Crime Research Center, 2001-2002

[13] . Ibid

Intellectual property theft, including software piracy, Industrial espionage by means of access to or theft of computer materials, Identity theft where this is accomplished by use of fraudulent computer transactions, writing or spreading computer viruses or worms, Salami slicing is the practice of stealing money repeatedly in extremely small quantities, denial-of-service attack, where company websites are flooded with service requests and their website is overloaded and either slowed or crashes completely, making and digitally distributing child pornography.

Also the same is true under the famous Internet Encyclopedia called Wikipedia about the definition what computer crimes are? And it defines that, Computer crimes are, cyber crimes, e-crimes, hi-tech crimes or electronic crimes generally refers to criminal activity where a computer or network is the source, tool, target, or place of a crime.

1.3.1 FEATURES OF COMPUTER CRIMES

Computer crime is a highly intelligent crime. It presents itself from several aspects. First, the offenders of computer crimes are usually computer experts or technicians with high intelligence. Second, the offenders always use a highly intelligent method to commit the crime. And third, the crimes are always well conceived and prepared. Some of the crimes even had a schedule covering several years.

Besides, Computer crimes taking place at present mainly focus on two areas. One is focusing on secret information storage systems such as invading on important political, military, technological database centers. The other is focusing on financial systems. And this makes it very complicated stuff in order to control the action in a simple manner.[14]

Other related issue about computer crime is that, Computer crime is always well concealed. Because, since the victims of computer crimes are usually intangible targets, such as electrical data…. the consequences of computer crimes are usually not conspicuous. Therefore, computer crime is hard to be unearthed. In addition to that, since a computer crime always happens in several seconds and is not confined by time and space, it also increases the possibility of a successful computer crime.

[14] . Dr. Cecil Greek, computer crime New Media course by, school of criminology and criminal justice of Florida state university (1996)

When we also see the other feature of such crime, Computer crimes are relatively occur much more damage than the other traditional forms of crime like theft. And besides, Computer crime is hard to be detected and investigated. Because, For one thing the computer crime is always executed by unnoticeable methods and therefore difficult to be detected, for another thing, the

1.3.2 COMPUTER CRIME CATEGORIES

Computers are tools that make crimes easier. For instance, Fraud, False inputting, Fake, Forgery, Impersonation and Theft of information also consider as a crimes of computer.

The Ethiopian criminal code Article 706, also defines Computer crimes as “accessing, taking or using computer services with out authorization” or As Article 707 and 708 shows “causing damaging data or intentional disruption of a computer system or net work”. However, this doesn’t show the clear views of computer crimes. And as far as the writer understands the Ethiopian criminal code provisions contains the very important initial points of computer words like computer systems and computer networks. And such words are very essential for various computer related crimes like computer manipulation, computer sabotage, computer extortion, computer hacking, computer Espionage and other computer crimes like software piracy.

And therefore we could say that the few article provision of computer crime under the Ethiopian criminal code seems like it contains a wide bundled explanation regarding the crime that we are taking about. Though, knowing what constitutes a computer crime helps no one unless there is an understanding of how some of these types of Crimes are committed. Therefore, I will provide some general information on some types of computer crime however.

Some of the most common computer crimes category includes the following:-

Computer manipulation

Manipulation is a set of an act that is planned to have a certain goal like, to dishonestly get people to do or act in a way which they might not have freely chosen on their own or Present reality the way one want others to see it rather than the way it "really is., "Hide behind a "mask" and let people see you in an acceptable way when in reality you are actually feeling or acting in an ``unacceptable" way for these people.[15] But in general we can conclude that Computer manipulation is an act which is planned to get what ones wants from others even when the others are not willing initially to give it. And in order to achieve the result, the doer of the act uses a false name or false identification.

Computer sabotage

Sabotage is a deliberate action aimed at weakening an enemy, oppressor or employer through subversion, obstruction, disruption, and/or destruction.[16] When we see the case regarding computers; it has also the same meaning except including the word computer as means of a weapon to commit such nature of a crime.

Computer extortion

Extortion is a criminal offense, which occurs when a person either unlawfully obtains money, property or services from a person, entity, or institution through coercion or intimidation or threatens a person, entity, or institution with physical or reputation harm unless he is paid money or property.[17] And the same is true regarding computer extortion too. However, computer extortion is very difficult to trace and to control in contrast with those common crimes of coercion or intimidation.

Computer hacking

Computer hacking is more difficult to define. Computer hacking always involves some degree of infringement on the privacy of others or damage to computer-based property such as files, web pages or software.[18] It involves a person or a group of individuals who possess technological know-how and are willing to take the risks required to become a true "hacker".

Computer Espionage

The transformation of the Internet into the "information highway" has forever changed the way in which information is gathered. The Internet, as the library of world knowledge, has become

[15] http://library.thinkquest.org/C007091/uses.htm (Accessed on 07, Mar 2008 G.C)

[16] Ibid

[17] http://en.wikipedia.org/wiki/Extortion (Accessed on 17, Apr, 2008 G.C)

[18] http://www.ed.uiuc.edu/wp/crime/hacking.htm (Accessed on 17, Apr, 2008 G.C)

the repository of information needed to fuel economies of the world's superpowers. The keys to this "fountain of knowledge" are high-speed Internet access, advanced networking to share information quickly, and massive computer power to analyze billions of bits of data to discover the secrets hidden inside.

Powerful Internet browsers and "agents" are even now traveling through cyberspace into the computers and networks of both the suspecting and unsuspecting to record their secrets. A clever computer programmer in the immediate future will unleash electron based "cyber-agents" to recover more vital information in a day than any human being could recover in his lifetime.[19]

Therefore we can conclude that, computer espionage is a human intelligence through computers and use to break or open the confidential secrets without permission of the holder of the information.

Software piracy

Software piracy is the mislicensing, unauthorized reproduction and illegal distribution of software, whether for business or personal use. Pirated software hurts everyone—from software developers to retail store owners, and ultimately to all software users. Furthermore, the illegal duplication and distribution of software has a significant impact on the economy.[20]

19.http://www.cnn.com/SPECIALS/cold.war/experience/spies/melton.essay/ (Accessed on 17, Apr, 2008 G.C)

20. http://www.microsoft.com/piracy/ (Accessed on 17, Apr, 2008 G.C)

CHAPTER TWO

THE ETHIOPIAN CRIMINAL CODE PROVISIONS AND THE COMPUTER

The Ethiopian penal code 1957 and the 2004 Criminal Code have similar frame work of organization regarding the categorization of the crime. They include general part of the law. i.e. offences and the offender and criminal punishment and its application. And also it includes the special part of the law. i.e. offence against the state or against national or international interest, offence against the public interest or the community, offence against individual and the family, and at last they also include the Code of Petty Offences under their wide valuable frame work of the code. However, the previous code of 1957 didn't include computer crime and it is oblivious why the previous code didn't include computer crime.

As we know, computers are the result of the modern society technological achievements. And we can say they can do anything. But, what are computers good at? Storing information? And is it really hard to fight computer crimes?

The answer to the entire above question is, "Yes." Computers are very, very good at storing and displaying information of all types, good at providing a way to send and receive data, and as we all know, also good in processing numbers. But none of those things are what really sets computer as a powerful engine in crime protection. Instead, what really makes computers powerful forces in our daily lives is that they can be programmed to do things with all that information. And that's the big difference that we should be paying attention to and one can have a big impact on how to use them.[1]

Though, we can clearly see that there is lack of movement on the government side, since its creation computer has become increasingly important and helpful in different spectrum. The law as we see today (this time) in computer technology has not been able to evolve as quickly as the rapidly expanding technology. This lack of movement on the part of governments shows a lack of understanding with the area. Therefore, due to an increase of use of computer the government to obliged to move with this ground. But however, no one couldn't predict that

[1] http://www.clickz.com (Accessed on 05, Apr, 2008 G.C)

Computers as a weapon for committing criminal offences and become a danger for the well being of the society as we know now.

But when things change, and people mind highly dependant on these machines on the collection, storage, transmission and connecting of personal data. This endangers the personality rights of citizens. Therefore, the need to keep and protect on the use of information technologies become vivid. And therefore, such pre-computing environment didn't get any chance to include such provisions on the 1957 Penal code of Ethiopia.

The Ethiopian Criminal Code 2004 includes the computer crime under its special part of the frame work and under the group of offences against property. Under this, Art 662 states "Any interference with property and economic rights or rights capable of being calculated in money forming a part of the property of another shall be punished in accordance with the following provisions, except where the interference is of such minor importance as to be subject to the provisions and sanctions regarding petty offences."

Therefore, it is a clear fact that computer crime is a kind of crime that has done to make harm on the rights of other persons property and economic rights. And besides, as the provisions of the law Art, 662/2 state, public and private properties are protected under the law and also, when damage to the right in property is constituted under the meaning of the code provisions any injury or prejudice suffered in comparison with the normal situation in the absence of the crime.

So, leads to the question that, when is the time that we are concluding compute crime is occurred? And what important provisions about computers are included under the new Ethiopian criminal code of 2004?

The code tries to solve such kinds of question and other related problems regarding computers and I will try to answer the question on the following column as I get them from the Code 2004. Computer related points.

2.1 COMPUTER CRIME UNDER THE ETHIOPIAN CRIMINAL CODE 2004

Crimes committed against the computer are relatively new offences that relate to the computer, the materials contained therein and its uses as a processing tool. This is to ensure that owners and users of the computer and electronic systems will continue to enjoy their usage with minimal incursion into their socio-economic well being or personal space as a result of the anti-social behavior of others who seek or facilitate illegitimate access.

To begin with a bright picture of the computer crime new section of the Ethiopian C0riminal Code, we might need to see and to interpret these six Articles of the Code consecutively. They include, access, taking or using computer services without authorization (Art, 706), causing damage to data (Art, 707), Disrupting the use of computer services by an Authorized user (Art, 708), Acts committed to facilitate the commission of computer crime. (Art, 709), and also computer associated crime and concurrence means of the crime under Article, 710 and 711 consecutively.

2.1.1 ACCESS, TAKING OR USING COMPUTER SERVICES WITHOUT AUTHORIZATION

Article 706:- Access, Taking or Using Computer Services without Authorization.

(1) Whoever, without authorization, accesses a computer, computer system or computer net work, is punishable with fine.

(2) Whoever, without authorization, accesses a computer, computer system or computer network, and intentionally takes or uses or causes to be used data or computer services, is punishable with simple imprisonment or fine, or in serious cases, with rigorous imprisonment for not more than five years and fine not exceeding twenty thousand Birr.

(3) Where the crime is committed negligently, the punishment shall be simple imprisonment not exceeding three months, or fine not exceeding two thousand Birr.

On this provision of the law, we can see accessing, taking or using computer services without authorization seems a wrongful acts that is done intentionally. And when this happens, they are considered as if they are a serious one. Therefore, when the crime was made with the awareness or with the intention of a party, it is punishable relatively in a higher sense of punishment. However, when the crime is committed in a negligent state of mind the law states a simple punishment.

The article tries to show some important points, them are to be focused. For instance, when we talk about authorization, a private individual or a government organization might be the one who give this authorization to give it.

According to Art, 706/2 of the code, we can also say that not only because the person who access the computer without authorization is punished by taking or using for his personal gain. But also he has responsibility if he is the one who cause the information being use by other person benefit.

To show this on a simple illustration, Lets take x, y, and z irrespectively. As we all might guess, Computers help teachers to keep track of lessons and grades. Or they might help students do research and learn. Or computers let every one hook up to *networks* (many computers hooked together).

By putting this in mind, Lets take X who is a computer programmer and without the intention of damaging Y Company, He breaks the security code of the computer network and accesses the information without Y'S consent and permission. But, Mr. Z (Mr. X friend) accesses the data from the X computer too and uses it in a way of damaging Y Company.

In this case X, has a responsibility in either of the case. i.e either he use it for his personal benefit or happiness or by being a cause to a crime that was made by his friend Mr. Z

And at last, when we see Art, 706/3, of the code, it also shows negligent actions of such natures of the crimes but, it seems like we need to take a care regarding categorization either the action is made intentionally or negligently.

2.1.2 CAUSING DAMAGE TO DATA

Art, 707 of the provisions differ with the previous Article of 707 by a mere fact that, Art 707 provisions are about "causing a damage to the data by adding, altering, deleting or destroying" But, it is similar with other provisions of computer crime by the fact that in other cases of computer crime, we can say that all these criminals are entering to the computer network, computer system or computer data without authorization. But, Art, 707 specifically, answer the time that a computer system or network or data is being damaged.

Article 707:- Causing Damage to Data.

(1) Whoever, without authorization, accesses a computer, computer system or computer network and intentionally causes damage by adding, altering, deleting or destroying data, is punishable with simple imprisonment for not less than three months, or fine.

(2) Where the crime is committed:

(a) in order to devise or execute any scheme or artifice to steal, defraud, deceive or extort or wrongfully control or obtain money, property, computer services or any data; or

(b) In serious cases even in the absence of the scheme provided for under sub-article 2(a), the Punishment shall be rigorous imprisonment for not more than five years, and fine not exceeding twenty thousand Birr.

(3) Where the crime is committed negligently, the punishment shall' be simple imprisonment not exceeding three months, or fine not exceeding two thousand Birr.

Besides, Article 707 also shows that intentional damages of a computer network or system without authorization by adding, altering, deleting or destroying will be punishable with rigorous imprisonment. Especially when the case is related with stealing, defraud, deceive or extort or wrongfully control or obtain money, property, computer services or any data the law try to see it in a very special manner. But before we go any deep further, let's put these words with simple practical examples and explanations.

Adding and Altering a computer network/ system, more interrelated with defrauding**,** deceiving or extort or wrongfully control or obtain some thing. For instance, the telephone network hackers today predominantly use manipulation techniques (i.e. they Alter or present something in a way that is false but personally advantageous) which allows phone calls at the expense of other network participants. This is made possible by breaking into badly protected voice-mail-systems, the direct-dialing functions of which are exploited. This method of Altering others information for their personal advantage creates economical damage to the honest user of the network system.[2]

Deleting or destroying a computer data: - When we think about deleting or destroying the computer data, we first think about computer virus first. Because, these viruses are designed to modify, damage, destroy, record, or transmit information within a computer system or network without the permission of the owner. Generally, they are designed to infect other computer programs or computer data, consume resources, modify, destroy record or transmit data, and disrupt normal operation of a computer system.

The code Art, 707 /2 and Art 707/3 also shows the punishment is going to be given either in the form of imprisonment or in fine. Besides, it also shows, as if a negligent committeeman of such nature of a crime is punishable for the act that is done in a negligent manner.

2.1.3 DISRUPTING THE USE OF COMPUTER SERVICE BY AN AUTHORIZED USER

How can be a computer disrupt? Or being upset? Are these questions in order to show this section in brief? To begin with a simple idea, As we point out earlier, computers are a programmable machines and any program that are designed to disrupt the well being of the normal action of the computer might be considered as disrupting one, unless the user it self authorized such action by some other its own reasons.

[2] http://www.uplink.com.au/lawlibrary/Documents/Docs/Doc122.html Accessed on 01, Apr 2008 G.C)

Article 708.- Disrupting the Use of Computer Services by an Authorized User.

(1) Whoever, without authorization, accesses a computer, computer system or computer network, and intentionally disrupts the use of the computer by an authorized user, is punishable with simple imprisonment not exceeding three years or fine.

(2) Where the crime is committed negligently, the punishment shall be simple imprisonment not exceeding three months, or fine not exceeding two thousand Birr.

The Encarta Dictionaries of 2007 defines the word Disrupt in the following manner: It means, to interrupt the usual course of a process or activity or to destroy the order or orderly progression of something. And also other different materials define the word disrupt on similar bases of definition. However, the code Article 708 provision uses the word Disrupt to the use of computer service users that disrupt computer, computer systems or computer networks without authorization.

For instance, the Famous school of "Somerset Hill", Computer class acceptable use policy definition shows that, disrupting the use of compute service includes "Any school managed or owned computer equipment or systems, including, but not limited to, networks, hard drives, servers, peripherals, printers, networking systems, devices, modems, all electronic documents, video, voice and data networks, routers, storage devices, and classrooms equipped with such.[3]

In addition to what is explained above, this policy also tries to show what unauthorized user is, and it also defines that, any individual, with or without authorization, who utilizes the District's computing system from any location.

And other source of the material defines disrupting computer services as takes the form of a Denial of Service attack or a distributed denial of Service Attack. Denial of service attacks attempt to deny a user or users of a network the resources normal availability. The most common methods of Denial of service and Distributed Denial of Service attacks are carried out by way of undue bandwidth consumption, computer resource theft, exploiting flawed programming, and traffic redirection. In order to carry out such attacks, one need not be a technical wizard because these are easy to use programs which facilitate Denial of service and Distributed Denial of service attack

[3] http://www.shsd. Org/acceptable_use_of _computer.htm (Accessed on 01, Apr 2008 G.C)

Interruption of computer services provisions thus seek to proscribe conducts that are intentionally or recklessly disrupts or degrades computer services, or denies computer services to an authorized user. Thus, interruption of computer services provisions may be used to specifically prosecute those responsible for Denial of Service attack or a Distributed Denial of Service Attack. [4]

When we see the computer disrupting section under Article 708 of the code, it is a clear fact that it includes such computer technologies of electronic mail communications. But if one disrupts computer and other forms of services without authorization, such unacceptable and illegal behavior of violation will serve as a just cause for taking punishment either in imprisonment or in fine. Besides, Art 708 also shows that, negligent acts of such forms of a crime are also punishable.

2.1.4 ACTS COMMITED TO FACILITATE THE COMMISION OF THE COMPUTER CRIME

Article 709.- Acts Committed to Facilitate the Commission of Computer Crimes.

> *Whoever, with intent to further the commission of one of the acts specified in the preceding three Articles, imports, produces, sells, offers for sale, distributes, buys, receives or possesses instruments, secret Codes or passwords, is punishable with simple imprisonment or fine or both.*

Various systems are employed to control behavior of criminals, including rules codified into laws, planning people to ensure they comply with those laws, and other strategy and practices designed to prevent different crimes.

The code Article, 709 is not stating about the person who directly commit the action of a crime. Instead it talks about the person who facilitates the commission of a crime. And therefore it gives a clear warning to such persons that imports, produces, sells, offers for sale, distributes, buys, receives or possesses instruments, secret codes or passwords in order to commit computer crime.

[4] http://www.ists.dartmouth.edu/TAG/ajt/statutes-states-ics.htm (Accessed on 01, Apr 2008 G.C)

When we talk about such persons in particular we must think the purpose of such provisions first. Art, 709 provisions seems a pre-emptive, harm-reduction provision that use as a threat of punishment to those that plan to engage in the behavior of such an action that causes harm. And in this case it seems like that the law becomes more concerned on this matter moreover because it usually believes that cost to not criminalizing outweighs the cost of criminalizing it. And besides, it clearly suggest as if criminalizing such persons may also provide future harm reduction even after a crime. For instance, assuming those imprisoned for committing crimes are more likely to cause harm in the future.[5]

2.1.5 <u>OTHER CRIME COMMITED BY COMPUTER AND CONCURRENT CRIME</u>

Different cases involve in the use of computer technology in traditional crimes. For example, Computer crimes that we have seen above did not only serve for the purpose of gaining economic benefits, but they were also used for attacks on life. When such cases happened we don't have to oblige to use such provisions of computer crime. Instead, as the law provides we can use the relevant provisions of the crime criminal code section. Or either, as the nature of the case we can also punish the doer of the action in a manner of concurrent crime that is committed as to the relevant provisions of the code.

Article 710.- Other Crimes.

> *Where one of the other crimes provided for under this Code is committed by means of a computer, the relevant provision shall apply.*

Crimes are committed using different means of materials. For instance, In Ethiopia many individuals commit intellectual property crimes not only because they can be relatively easy to commit (such as copying music) but also because they believe they will not be prosecuted. Besides, most offences in relation to copyright are much of civil offences, and therefore require legal action to be instigated by the owner of the copyright that is being violated.

And therefore as the case Art, 710 For Example, If a person copying a copyrighted music on his computer for commercial purpose and get caught, In such a case, as the provision of Art, 710

[5] http://en.wikipedia.org/wiki/Crime Accessed, on 19, May 2008 G.C)

states, one must not consider whether the crime is computer related crime or not. Instead, there are provisions that govern such kinds of Copy right infringement action on more relevant manner. Therefore, as Article 710 of the criminal law indicates, when a crime occurs that is committed by means of a computer, the relevant provisions of the code regarding Copyright infringement shall apply to punish the action of the criminal.

Article 711.- Concurrence of Crimes.

> *Where any crime committed by means of a computer, has resulted in the commission of another crime punishable under this Code, the relevant provision shall apply concurrently.*

Let's put this Article 711, in a simple Example. A British hacker, who in 1994 accessed the information system of a Liverpool hospital because he simply wanted to see "what mess can be caused with the computer", among other things, he changed the medical prescriptions for the patients: A nine-year-old patient who was "prescribed" a highly toxic mixture stayed alive only because a nurse re-checked the prescription.[6]

In this case when we see the action of the hacker in accordance with the provision of the Ethiopian criminal code of 2004, the hacker who access the computer without authorization is clearly violated Art, 707/1 of the code i.e "*whoever, without authorization, accesses a computer, computer system or computer network and intentionally causes damage by adding, altering, deleting or destroying data, is punishable with simple imprisonment for not less than three months, or fine"*

Besides Article, 707/1 of the code the hacker also violates the criminal code of the country because, he endangers life, person or health of a person.

And Art, 571 of the code stated under the title of "Exposure of the life of another" i.e. "*Whoever intentionally puts another in imminent danger of death, is punishable, according to the circumstances of the case, with rigorous imprisonment not exceeding three years, or with simple imprisonment for not less than three months."*

Therefore, when we see the action of this hacker, he violated both Art, 707/1 and Art 571 thus, as the provisions of Art, 711 of the Code shows, when such two crimes are applied concurrently, we must use the relevant provisions of the code in a concurrent manner.

[6] http://www.uplink.com.au/lawlibrary/Documents/Docs/Doc122.html Accessed on 01, Apr, 2008 G.C)

CHAPTER THREE

CHALLENGE TO CONTROL COMPUTER CRIME IN ETHIOPIA

The past several decades brought an increase in the availability of electronic resources in variety of ways. With this inclement on the availability of electronic resources come a new form of criminal activity that takes the lead of electronic resources, namely computer crime. Currently, in the world this new form of crime rapidly increasing and creates a new and ongoing challenge to law enforcement agencies at all levels in how to prevent, investigate, and prosecute these crimes.[1]

Criminals can cause harm to computers and to the society in a wide variety of ways. For example, when we see the Ethiopian criminal code computer crime provisions, an intruder who gains unauthorized access to a computer, computer system or computer network can intentionally causes damage by adding, altering, deleting or destroying data. Alternatively, intruders can steal, defraud, deceive or extort or wrongfully control or obtain some amount of money or property. Or it controls the computer services or an important data. I.e. initiate a "denial of service attack" that floods the victim computer with useless information and prevents legitimate users from accessing it.

In a similar way, those criminals also cause the means of disruption on the normal use of the computer by spreading a virus or worm that can use up all of the available communications bandwidth on a corporate network, making it unavailable to employees. In addition, when a virus or worm penetrates a computer's security, it can delete files, crash the computer, install undesired software, or do other things that impair the computer's integrity.

Therefore, that is why we call Computer crime as a high intelligent crime, and it is more challenging one. First, the offenders of computer crimes are usually computer experts or technicians with high intelligence. Second, the offenders always use a highly intelligent method to commit crime. Third, the crimes are always well conceived and prepared. Some of the crimes even had a schedule covering several years. In addition to that, since a computer crime always happens in several seconds and is not confined by time and space, it also increases the possibility of a successful computer crime.[2]

The challenge here is not stating such forms of a crime or creating awareness to the law enforcement bodies. Instead, when we come up to the implementation procedure, such crimes

[1] Michael Kunz & Patrick Wilson, Computer Crime & Computer Fraud, University of Maryland, Department of Criminology & Criminal Justice Fall, 2004

[2] Kang Shuhua (1991). "Criminology" Beijing: Peking University Press.

are hard to be detected and investigated. There are two main reasons. The first one is, computer crime is always executed by unnoticeable methods and therefore difficult to be detected. The other main reason is the law enforcement practitioners lack knowledge in computer technology and also luck of computer experts who can detect this crime with shortage or unavailability of resource to fully prosecute the crime. And therefore, the seizure of evidence and further prosecution are difficult to accomplish.

For instance, I try to interview some law enforcement personnel's at the Federal police and at the Federal Prosecutor office, it seems like there is nothing known or nothing done in order to control the coming situation of computer crime. But, I don't want to conclude such personnel's doesn't know how dangerous computer crime is. Instead, it appears to me that they gave it simple room in contrast with other forms of crime.

When we see this fact aside of the American federal Bureau of investigation case study, in 1980 only one in 22,000 computer criminals goes to prison. And the computer criminal is less likely to get caught than the bank robber-and less likely to get convicted, if caught. Estimates of detected computer crimes are as low as one per cent. And in 1984, a survey by ***American Bar Association*** reported that 25 per cent of its respondents had suffered "known and verifiable losses due to computer crime during the last twelve months. And the average loss was 500,000 dollars, and that 89 per cent of the cases are never taken to judicial process of the remainder and convictions obtained are only 18 per cent. Still there are some people have suggested that the whole matter has been ridiculously over-blown.[3]

The Ethiopian information and communication technology security and standard policy, regarding security standards shows that, "Since information security and standards constitute integral parts of the process of ICT development, the Government will give priority to the creation of a safe and secure ICT environment as well as appropriate standards. The Government is committed to taking measures aimed at putting in place systems and guidelines within the framework of this policy**"**

Besides, 2004 criminal code also includes such new forms of a crime in a sense securing the ex-ICT security standards, and also it seems like that the criminal code is recognizing the emerging

[3] 3. Cornwall, Hugo (1987). Data theft: computer fraud, industrial espionage and information crime. pp.46, London: Heinemann Professional Press.

problems resulting computer crimes in proof detecting and prosecuting them. Besides, the Code also tries to cover all forms of a crime that computer crime cover. However, things are more challenging regarding various points. For instance, the challenges that we will face in all parts of the law enforcement bodies regarding education and other related point is considered as an issue.

The challenges regarding the legislature body and challenges regarding the legislation that created to punish offenders, the professional organizations that combat computer crime, the resources that are available to educate the public about computer crimes, and other related reasons for law enforcement agencies are considered as a challenge to control such forms of crime in Ethiopia. In addition to what is explained above about the problem there are some question which comes in our mind in creation awareness.

1. What will be the needs to control such special, highly technological crimes of computers from happening? And, how could be challenging to prosecute these crimes for a developing country like us? (Ethiopia), and what are the factors that make us stop from putting special mechanism and controlling such forms of crime?" And "what are the factors that make us prevent from building a peaceful environment regarding such nature of crimes? And how will they be challenging for the police to perform their task and how also be challenging for the prosecutors and judges? And what has to be expected from the society at large regarding the nature of these crimes? And other related issue will be discussed to show the scope of the challenge that we will face in all parts of the law enforcement organs.

3.1 THE LAW INFORCEMENT BODY

Law enforcement body is a term used to describe either an organization that enforces the laws of one or more governing bodies, or an organization that actively and directly assists in the enforcement of laws. In doing so, the law enforcement bodies assist the governing bodies to provide governance for their subjects.[4]

[4] Lishan Adam, "Information and Communication Technologies in Ethiopia: Past, Present and Future Potential for Social and Economic Development" Ethiopian Information Technology professional Association Workshop, 2 March 1999

Militaries, civilians, local and federal police has the statues of such law enforcement bodies. Besides for instance, in Ethiopia the law enforcement bodies can be responsible for the enforcement of laws affecting the behavior of people or the general community. For instance the Federal police have a duty to control such forms of crime and have also a duty to enforce such laws throughout the country. And also the Ethiopian science and technology commission is also a coordinating body for science and technology (S&T) in the nation and it aims to create conditions conducive to the development of the organic growth of a viable scientific and technological system in the country.[5]

When we see these practice according to Ethiopian law, the last eight years has seen a dramatic growth in information technology in Ethiopia like Developing IT service private companies, growing import of computers, introduction to the Internet, recognition of government of the fundamental roles of information and communications technology there by proposing a national information and communication development plan, and the national information policy, the ongoing phased liberalization of telecommunications and the energy sector, establishment of computer science unit and information science school are some of the promising activities. Despite these developments, the impact of information and communication technologies on the quality of life of Ethiopians remains law. The technology has not yet diffused to the social fiber of the society.[6] Hence the agency for the technological development in Ethiopia has to make lots of developments in creating lots of developments in awareness on the subject matter.

As the agency put it, Computer technology development in Ethiopia is the country's largest development goals and objectives. But however, such form of developments without clear understanding brings its own problems regarding difficulties in investigating these crimes and in controlling the whole parts of the crime. Besides, since its creation, the computer has become increasingly important creating awareness in the society. The law in the past years has not been able to evolve its methods in detecting preventing these crimes as quickly as the rapidly expanding technology.[7]

5. Teferi Kebede, Information technology in Ethiopia, 1994
6. http://en.wikipedia.org/wiki/Law_enforcement_agency

7, Internal Investigations (Federal Bureau of Investigation) Retrieved on 2008-02-12.

This lack of movement on the part of governments shows a lack of understanding with the area. Though, Preparation is the only technique that the government has to take regarding how to investigate these crimes, gathering evidence and having sufficient preparation in creating awareness on the society and prosecuting the criminals must also be included in order to minimize the effect of the crime.

However, when we see the lack of computer crime investigation skill to law enforcement organs and the lack of understanding to the crime at hand, it is clear that without basic knowledge of computer crime investigation and computer forensics experts which investigate computer crime, the police and the prosecutor office will face a challenge on the investigation of the crime and criminals who are highly intelligent computer experts with a high classic skills.

Besides with out a certain preparation to the coming situation and plan to include some sort of protective mechanisms it is a clear fact that such form of a crime is more challenging than any other criminal investigation. Therefore, in the case of our country the first line of body that should be trained on these matters is the police force. Because, it is the police who charged with the regulation and control of the affairs of a community and it is also the duty of the organ to maintain order, enforce the law, and prevent and detect crime. Especially with respect to maintenance of order, law, health, morals, safety, and other matters affecting the public welfare, it is the police that are responsible for the prevention and detection of such crimes. Therefore, the police forces must be equipped with sufficient experts on the resources including educated force to deter the crime.

But in the case at hand, without learning an element of computer crime training and raising awareness of the existing officers and staff, it just like a dream (more challenging) throughout the force to promote awareness and knowledge in order to prevent such forms of a crime.

Moreover, it also be noticed that Bing a well trained police officer with so many talents and intelligence doesn’t only bring the desired results in all the cases that he or she detect and investigate the crime. Instead, some modern crimes, for instance, computer crimes are more challenging by their nature and the police have to prepare for those challenges.

Though, A predominantly knowledge will come to change via information based skill and knowledge. Otherwise, Computer crime will become the challenging problem in the near feature to our nation. And with recent culture of using computers and training of the public, crimes committed by computers will increase.

3.1.1 LACK OF RESOURCES

It is a fact that law enforcement resources in any fields of a crime are allocated based upon the number of *reported* crimes. And it is also a fact that computer crime is not a hot problem at hand to our nation. Having this in mind, one can conclude that, instead of allocating computer detectives on the area that is not exist, it would be better to assign police officers for the case of burglary or other hot crimes to help decrease the problem.

Law enforcement executives familiar to the issue of computer crime still face financial challenges. Training police officers to investigate digital crime is an expensive proposition. In these times of public economic constraint, police chiefs are unwilling to spend their limited funds on anything that will not provide a sure and noticeable return.

A properly trained computer crime investigator may require extensive ongoing professional education to maintain up-to-date skills.[8] Because computer companies introduce many new hardware and software products each year, staying ahead of the educational curve can be a huge task. Furthermore, no single investigator can know how to operate every system.[9] A number of officers must be trained to specialize in a variety of stage.

As if training costs were not enough to discourage the average police chief from investigating digital crime, there is always the cost of equipment to be considered as well.[10] The specialized hardware and software required for the forensic examination of computers can easily run to tens

[8] *See generally* Staff of Senate Comm. on Gov't Affairs, Permanent Subcommand on Investigations, 104th Cong., Security in Cyberspace (Comm. Print 1996) [hereinafter Security in Cyberspace].

[9] . Ibid

[10]. Supra note, 8

of thousands of dollars.[11] Digital evidence storage rooms, spaces without magnetic interference, must be established to prevent the break-down and destruction of digital evidence.

Because of the above mentioned reasons and other problems, the trained in Ethiopia regarding computer crimes prevention seems non existent and because, the police receive no complaints about computer crime, there appears to be that computer crime is not a problem to our nation.
In fact at the time of interview with these law enforcement bodies like, The Federal police commission and The Federal prosecutor office they all agree that, As if computer crime will not occur here in Ethiopia and has not become a problem in their particular activity yet. Because of this as they all agree, they didn't allocate any resource to combat the crime that is considered ideal to their mind. But however, as to the view of this essay writer, a wiser police manager and prosecutor, however, would not confuse invisibility with non-existence.

3.2 PROSECUTION AND JUSTICE SYSTEM

Criminal law is generally defined as those of society's rules which are enforced by coercive means, and punishable by a variety of penalties. More specifically, criminal law involves the punishment of behavior defined as "criminal," to provide both specific and general deterrence, and to provide retributive justice to the wronged party or survivors.[12]

Justice and law enforcement are vital to the state to safeguard the rule of a country, to regulate state security and to keep secure the interests of the people and social stability at large. And in a sense of such speculation, The Ethiopian criminal code (2004) defines and punishes both crimes against the individual and crimes against the laws of nations.[13]
And when we see the legal actors regarding the legal provisions of the code, we find those organs which stood together for national judicial system of the country. The prosecutor are the one that are responsible for presenting the case against an individual, and the judges are the one who interprets and applies all the laws that the prosecutor brings in order to secure the law of the land.

[11] Michael Noblett, *Computer Analysis and Response Team (CART): The Microcomputer as Evidence,* 19 Crime Laboratory Dig. 11 (1992).

[12] David J. Audlin, (1992) "Crime, Culture and Law Enforcement" Florida State University School of Law.

[13] The Criminal code of the Federal Democratic Republic of Ethiopia, Book III and Book IV,(Art, 238-374 and Art, 375-537)

And when we come to the main part of this article, we will ask one important question with regard to this organ related to computer crime. How come such organ could be the challenge in relation with computer crime provision implementation in Ethiopia?

To answer this question, First of all justice apparatus hinges much on the existence of qualified human resources at every organ that constitutes the justice machinery. In this regard judges should be armed with the required legal skill so that they can discharge the task that comes before them to the highest degree possible.[14] On the other hand the prosecutor also needs qualified human resources that are trained to perform the necessary legal skill in order to discharge their task properly. But however, when we see the basic legal skill by it self doesn't make a person fully capable of executing new tasks all the time. Though, it is believed that, the nature of the crime, and the way of handling things are much more difficult from those crimes that they handle before.

Without short or long term service training regarding computer crime, either in regional state or in highest level of these offices lack of skilled manpower will be the biggest challenge in order to combat computer crime in Ethiopia. Besides, Additional formal training, workshops and seminars should be conduced for judges and prosecutors regarding how they give the service to the public and how they handles such kind of a task and others. Furthermore, research papers on various legal provisions and new legal developments of such kind of crime cases has to be shown in order to upgrade the legal skills of those organs. Other wise, the challenge in regard with computer crime by such parts of state organs will be more challenging.

3.3 CIVIL INSTITUTIONS

Computer crimes are to be distinguished from computer-enabled crimes. They relate to crimes against computer hardware as well as the digital contents contained within it such as software and personal data. Computer crimes have an adverse effect on the integrity and trust in information technology infrastructure such as computer or telecommunications networks and in the security of transactions conducted through them. That is why the new Ethiopian criminal code 2004 legislation criminalizes such computer-related crimes.[15]

[14] . http://www.ethiopianembassy.org/judiciary.shtml

[15]. Warren B. Chik* (2006) "Challenges to Criminal Law Making in the New Global Information Society", www.law.ed.ac.uk/ahrc/complaw/docs/chik.doc

But however, criminalizing an action and controlling it has much difference regarding action towards controlling the situation. For instance, among different parts of the society, civil society institutions might also be the challenge in order to control computer crime in Ethiopia.

The other important point need to be discussed on this point is the question of what are civil society institutions. And how will be the challenge in the prevention of computer crime in Ethiopia?

First of all to clarify my point as it is defined, Civil society is composed of the totality of voluntary civic and social organizations and institutions that form the basis of a functioning society as opposed to the force-backed structures of a state (regardless of that state's political system) and commercial institutions.[16] For instance, charities, clubs (sports, social, etc.),consumers/consumer organizations, cooperatives, cultural groups, environmental groups , non-governmental organizations (NGOs), professional associations, religious organizations, support groups , trade unions are the one who are included on these civil society institution group.

It is believed that civil society organizations facilitates better awareness and a more informed citizens who make better choices in societal values and hold the law more accountable as a result. And the increasing significance of information in the post-industrial information society is also is caused by the development and expansion of information *technology*. The development of the *technological* society and of *technology* law is, therefore, the first major force of change.[17]

When we come to the point of our topic, we will find these civil society awareness to the crime of such nature and protection procedure that they have followed in order to combat the crime. Now a days most organization in Ethiopia use computer in order to store their useful data and most secure organizational secret. But however, they are more concerned about network construction and maintenance than security matter. But, this is not only such organizations problem either. For instance in England, the biennial Department of Trade and Industry (DTI) Security Breaches survey reports that 62% of UK businesses had a computer security incident in

16. Civil society - Wikipedia, the free encyclopedia.html. http://en. wikipedia.org/wiki/civil society

17 .Civil society - Wikipedia, the free encyclopedia.html. http://en. wikipedia.org/wiki/civil society

the 2006.[18] These statistics may underestimate the real situation as many organizations or individuals may be unaware that the security of their computer has been compromised.

Businesses and other organizations also face risks through lack of user awareness. Even when they have taken computer security measures, the limited awareness of computer security among employees and their business partners also creates risk to the organization. However one must notice that, inadequately protected computers means they are easily targeted for unauthorized users.

3.4 PUBLIC AWARENESS OF THE LAW

As it is explained before, public awareness of the law is also the major component in deterring computer crime. To learn means much more than simply taking in new knowledge. It can be the taking in of new insights to change the way we think, new skills to change the way we act, new perspectives to change our attitudes, new awareness to change our priorities, new experiences to change our confidence, new relationships to change our lives.[19] If we accept that learning goes hand in hand with change, then we also accept that to facilitate change we need to facilitate learning.

Some people understand that the purpose of education is to inform, to share information, to tell people things. This understanding limits the potential for influencing change. On the other hand, when education is understood more as having a transforming role where people are set free from oppressive influences, then the potential for education to facilitate change is maximized.

As we see in our country, weak educational infrastructure during the previous period of time, clearly damage the educational system. For instance, there was no coverage regarding the time technological advancement that we are reaching. But, however the future of growth of digital technology and a national information and communication industry cannot be realized without introducing new knowledge’s to the younger generations.

[18] Department of Trade & Industry, Information Security Breaches Survey: Technical Report, April, 2006 06/803

[19] http:// efc.co.nz/index.php3 Stephanie Cowan, Director, Education for Change Ltd. Dated: December 2000

When we see Education in computer or education in information technology at large, obviously there will be high cost of these technologies that often lead to the expression "we do not have chalks and proper bench, how do you dare thinking of computers". Experts agree that although the cost of information and communication technologies is high the cost of not applying them to social and economic development is much higher.[20]

Because of the different assumption regarding computer technology education, as we said it before controlling computer crime in Ethiopia will be a very challenging act. Besides, denial of education or implementing weak educational infrastructure also keep the next generation in the same cycle of poverty, way, civil strife. It also makes things more complicated and challenging toward the journey of a given goal of the society.

But, substantive progress in implementation of better education and progress in quality of life and development cannot be achieved without preparing people for new skill and knowledge in the society. This partially involves making an environment open for distribution of computers to schools, training the population in computer application, and in building a solid national computer, and communication science education. Advanced university training in computer communication systems, computer application system, information science, parallel and distributed systems, software engineering, simulation techniques, tools and telecommunication systems creation of a well known campus on the field and nation wide network and information systems in education have no substitute for national development.[21] Other wise, lack of formal knowledge regarding such new technologies of computer might not only be the block for development. Instead, it will also become a challenge in fighting computer crimes protection in Ethiopia.

Computer technology has become a fundamental part of daily activity and will likely be more so In the future. Unfortunately, Information Technology awareness in the public at large and the initiatives are still characterized poor. Because of this one can say there is limited awareness of

[20] Mansell, Robin and Uta When. (1998). Knowledge development. Oxford: Oxford University Press.

[21] Castells, Manuel. (1996). The Rise of Network Society. The Information Age: Economy, Society and Culture. London: Blackwell

computer security among home as well as business users. Inadequately protected computers can be easy targets for unauthorized users.

For instance, when we take this point out side of our country context, ‘Get Safe Online’ is a joint Government-industry initiative to provide computer security advice. Their studies show that users tend to assume they know how to remain safe online, but they do not demonstrate adequate skills when tested. Respondents rated computer security as a high priority, but over half admitted to little or no knowledge of safe practices. Although 75% had a firewall (Box 6), 86% did not follow recommendations to update their security software.[22]

3.5 WEAK EXECUTION OF THE POLICY AND LACK OF STANDARD

Full adaptation of the computer technology is the basic factor that makes the society move towards a better understanding of the technology. But however, we don’t only focus on the use of computer technology. Instead, we also need to analyze such technologies are also a destructive tool when placed in the hands of persons that makes evil. Therefore, without appropriate security the use of computers and the internet involve risks regarding loss of records, corruption of information, and malicious attacks on the user including individuals, businesses and government.[23]

But however, even if the Ethiopian Information Communication Technology policy regarding security standard shows the government ensure a safe use of the technology that is guided by appropriate standards and best practice. But, the practice in relation with the computer security has more to develop.

For example, when we see the national guidelines in separate, The Ethiopian Information Communication Technology policy (ICT standard) shows, the government has a duty to promote the development and adoption of the necessary standards and good practices to support the exploitation and application of ICT in the public and private sectors, and in the society at large.[24]

[22] Parliamentary office of science and Technology, Post note, October 2006 Number 271

[23] The Ethiopian information communication Technology, system security and standard,(5.10)

[24] .Supra note, 23

Based on the above point, it seems like there is Lack of strong national guidelines regarding the technology. And also when we talk about the policy, it also says as follows. “The government will standardize data collection, processing and data exchange procedures. And Take appropriate measures to ensure that ICT will be used in all sectors based on international interoperable standards.”[25]

However hard the policy contains the most important points in standardizing data collection and exchange, there’s no standard method of any activity that is used by the organization that is implemented. Instead all organization working on the fields of such computer security oblige to use their level of standard in order to keep their data collection, process and especially on the parts of their data security.

And therefore this implies that, when computer crime occurs it creates a loop that makes the crime more twisted regarding where and how the crime committed. And without the standard data security system it demarcated to keep, the security of any private or governmental organization secured can’t be known unless they demarcate their security level by their own well trained computer experts.

In general, as I tried to explain it on this paper, lack of weak execution of the information technology policy and lack of common standard regarding computer technology both on the organizational and individual level and other related fields directly or indirectly challenges the controlling of computer crimes in Ethiopia.

[25] .The Ethiopian information communication Technology, system security and standard (5.10.2.2 ICT Standards)

CHAPTER FOUR

COMPUTER SECURITY IN COMBATING COMPUTER CRIME AND THE PROSPECT

4.1 COMPUTER SECURITY

Computer security is a branch of information security applied to both theoretical and actual computer systems. Computer security is a branch of computer science that addresses enforcement of 'secure' behavior on the operation of computers. The definition of secure varies by application, and is typically defined implicitly or explicitly by a security policy that addresses confidentiality, integrity and availability of electronic information that is processed by or stored on computer systems.[1]

Computer security protects an organization's valuable resources, such as information, hardware, and software. Through the selection and application of appropriate safeguards, security helps the organization's mission by protecting its physical and financial resources, reputation, legal position, employees, and other tangible and intangible assets. Unfortunately, security is sometimes viewed as upsetting the mission of the organization by imposing poorly selected, annoying rules and procedures on users, managers, and systems. On the contrary, well-chosen security rules and procedures do not exist for their own sake they are put in place to protect important assets and thereby support the overall organizational mission.[2]

A text book written by S.chand’s and D.P.Nagpal on the area of computer security shows that, Computer security includes the policies, procedures, tools and techniques designed to protect a company’s computer assets from accidental, intentional, or natural disasters, including accidental input or output errors, theft, breakings, physical damage, and illegal access or manipulation.[3]

Security, therefore, is a means to an end and not an end in itself. For instance, preventing an act of theft of data and asset could simply stop by designing a perfect company’s security system.

[1] S.CHAND’S AND D.P. NAGPAL, “Computer Fundamentals” S.CHAND AND COMPANY LTD, (2004), (Page 466)

[2] .“An Introduction to Computer Security” The NIST Handbook Special Publication 800-12, National Institute of Standards and Technology,U.S. Department of Commerce (Page 21)

[3] Cited at note 1, “S.CHAND’S AND D.P. NAGPAL, “Computer Fundamentals” S.CHAND AND COMPANY LTD” (Page 466)

And that controls or protects the company’s information from a theft, unauthorized access, natural disaster and damage for a certain period of time. But, such protection has to be implemented in order to secure the well being of a company or public organization. For instance, most colleges in Addis Ababa administer their business processes depend upon computer automation. Besides, they also use computer for keeping their records, dependable, confidential, and also for quick access to reliable information too. Though, without computer security standard we can say, it is very hard to keep the college computer system in a perfect manner without abuse. Therefore, data security method, the policies, procedures, tools and techniques regarding computer security has to be implemented.

Besides, when we talk about computer security, it is important to distinguish the techniques used to increase a system's security from the issue of system's security status. In particular, systems which contain fundamental flaws in their security designs cannot be made secure without compromising their usability. Consequently, most computer systems cannot be made secure even after the application of extensive "computer security" measures. Furthermore, if they are made secure, often it is to the detriment of usability.[4]

4.2. ADVANTAGES OF COMPUTER SECURITY

The people of the world have granted control of their existence to computers, networks, and databases. For instance, you own property if a computer says you do. You can buy a house if a computer says you may. You have money in the bank if a computer says so. Your blood type is what the computer says it is. In general, you are who the computer says you are.[5] But however, without securing such important technology first, the result might not be positive. Instead it becomes negative by those who are intentionally causing breaches of the computer system either for financial gain or for the fun of it.

Today, most computer systems, computer software and networks were not designed with security in mind. Even most “secure systems” are challenge with vulnerabilities due to the underlying technology that could enable an attacker to disrupt operations or cause damage.[6] But however, a perfect implemented security procedure has various advantages such as, safeguard and protects the computer systems and data from damage, protect unlawful use, protects hardware, software, and data from natural

[4] “An Introduction to Computer Security” The NIST Handbook Special Publication 800-12, National Institute of Standards and Technology,U.S. Department of Commerce (Page 53)
[5] “How to Own an Identity” (Washington Post 02/20/06)
[6] http://www.security-gurus.com/

disaster like fire, flood, and earthquake. And also, guards against sabotage and espionage, as well as various kinds of theft.[7]

4.3. COMPUTER SECURITY IN COMBATING COMPUTER CRIME AND THE PROSPECT

The Cambridge dictionaries online define the word prospect as the following manner. It is the possibility that something good might happen in the future or the idea of something that will or might happen in the future. Moreover when we see the computer age, it needs concern about criminal laws available to fight the emerging crimes of the computer.

In order to combat computer crime we don't have to invest most of our time and money. But, security is a precaution measures must be implemented in a proper manner. For instance, the costs and benefits of security should be carefully examined in both monetary and no monetary terms to ensure that the cost of controls does not exceed expected benefits. Security should be appropriate and proportionate to the value of and degree of reliance on the computer systems and to the severity, probability and extent of potential harm. Requirements for security vary, depending upon the particular computer system.

In general, security is a smart business practice. By investing in security measures, an organization can reduce the frequency and severity of computer security-related losses. For example, an organization may estimate that it is experiencing significant losses per year in inventory through fraudulent manipulation of its computer system. Security measures, such as an improved access control system, may significantly reduce the loss.[8]

Computers are crucial to the operations of government and business. Computers and networks essentially run the critical infrastructures that are vital to our economic security, public health and safety. Unfortunately, many computer systems and networks were not designed with security in mind. As a result, the core of our critical infrastructure is puzzle with out adequate

[7] Cited at note 1, "S.CHAND'S AND D.P. NAGPAL, "Computer Fundamentals" S.CHAND AND COMPANY LTD" (2004), (Page 466)

[8] "An Introduction to Computer Security" The NIST Handbook Special Publication 800-12, National Institute of Standards and Technology,U.S. Department of Commerce (Page 23)

protection that could enable an attacker to disrupt operations or cause damage to these infrastructures.[9] However, these phenomena can't make us prevent from seeing things in extensive ways. Instead, tasks are going in a well manner to protect computers and computer systems in a secure manner.

4.4 GOVERNMENT POLICY AND THE ROLE OF KEY INSTITUTIONS IN ETHIOPIA

The 'ICT Policy of 2003 provides a framework for defining the direction of the sector and its development objectives. It also sets the stage for institutional arrangements for policy development, and the promotion and regulation of the ICT sector.

As the policy indicates, The Ethiopian Government has made the development of information and communications technology (ICT) one of its strategic priorities. This ICT policy is a demonstration of its commitment to the development of ICT both as an industry and as an enabler of socio-economic transformation.[10] But In general, the application of information technology (IT) in Ethiopia and the overall situation of the present activities and the 10-year perspective plan indicate, as if the situation changes dramatically in the next two to five years.

To achieve the desire goal of the government, there are governmental bodies that are responsible to accomplish such objective of the policy. For instance, The National Computer Committee and The National Computer Centers are organs that are established by the government in order to promote the development of computer knowledge and services in Ethiopia. Besides, they also provide training courses, Assist government organizations in designing projects, preparing terms of reference for consultants when required, and monitoring project implementation and to perform other related tasks. And this makes the sector develop mostly in the application of computers and promote the technology innovation in Ethiopia.

When we see the institutional role in the development of the technology in Ethiopia, we must not forget computer security. Such security measures makes an organization keep it's in information in a good manner.

[9] . http. www.jmu.educomputingsecurityinfohowthe.html (Accessed on Jul, 27, 08)

[10]. The Information Technology policy of Ethiopia (2003)

For instance, the guideline presented by The Ethiopian Science and Technology Commission regarding data security crises shows, the government needs to develop a strategy to keep alert and able to respond to unexpected crisis on computerized data processing and control systems. Besides, the guideline states more about computer security of an organization at the time of disaster[11]. In addition the guideline also shows the objective, the scope and the beneficiary of such guidelines that are used for. For instance, the objective of the guidelines shows that the guidelines uses to create awareness in all public and private sectors, and introduce new approach of data disaster prevention and recovery management towards adopting complete risk analysis technique to determine the level of protection required for application, systems, facilities in ICT development and recover from any disaster without serious business discontinuity and major damages and loss to the system and data.[12]

Moreover, when we see the same guidelines regarding information security standards, No. 8.3 and 8.16 it reads as follows.

8.3 Control of computers and Information Resources

- *Sensitive information in any media shall be accessible only to personnel who are authorized by an institution on the basis of need, and performance of their duties. Data containing any sensitive information shall be readily identifiable and treated as sensitive in its entirety by respective organs of an institution.*

- *External users shall have defined access to public domain information.*

8.16 Personnel Security

- *Every employee shall be held responsible for information resource security to the degree that his or her job requires the use of information resources. Fulfillment of security responsibilities shall be mandatory.*

- *Awareness in security shall be done through on-going briefings and continual reinforcement of the value of security consciousness.*

- *Care shall be taken on friendly and unfriendly termination*

[11] Disaster Prevention and Recovery Management Guidelines (Ethiopian Science and Technology Commission) (2001)

[12] Ibid

To sum up the points, such security methods and guidelines are not meant to protect computer criminals at large. Instead, indirectly contributes its own share to the prevention computer crime in Ethiopia. But in general, Computer security is a complex and pervasive problem that often stumps many organization, which struggle to balance proper security against the cost and inconvenience of providing it. It cannot be achieved through computerization or sophisticated equipment alone. It also requires the active participation of employees with common sense, good judgment, and high moral values. Because security is ultimately the responsibility of the individual using the computer, Therefore, it is not surprising that organization that promote creativity, innovation, trust and high ethical standards appear to be more successful in enforcing computer security than organizations with stuff in cultures.[13]

And also, it has to be know that the effectiveness of security controls depends on such factors as system management, legal issues, quality assurance, and internal and management controls. In order to get a sound result on the protection of computer crime and get a bright vision of prospect, Computer security needs to work with traditional security disciplines including physical and personnel security. Many other important interdependencies exist that are often unique to the organization or system environment. Besides, all concerned body should recognize how computer security relates to other areas of systems and their right and duty in order to keep the computer secure and combat computer crime at large.

13. S.CHAND'S AND D.P. NAGPAL, "Computer Fundamentals" S.CHAND AND COMPANY LTD. (Page 466)

BIBLIOGRAPHY

A. BOOKS AND JOURNALS

1. D.P. NAGPAL, (2004), “Computer Fundamentals” ” S. Chand and Company Ltd

2. R. Sarvana Kumar, R. Parames Waran, T. Jayalakshmi (2005), “A Text Book of Information Technology” S. Chand and Company Ltd

3. Alexis Leon and Mathews Leon,(1999) “ Fundamentals of Information Technology” Leon Press,Chennal and vikas publishing House Pvt. Ltd. New Delhi

4. Efraim Turban, R. Kelly Rainer, jr, Richard E. Potter, “Introduction to information technology (2ndedition)” (2003), John Wiley and sons. Inc.

5. “Introduction to Computers”, A Workshop for San Diego State University Faculty and Staff, 2000.San Diego State University

6. Scott Charney and Kent Alexander, “COMPUTER CRIME”, Computer Crime Research Center, 2001-2002

7. Dr. Cecil Greek, computer crime New Media course by, school of criminology and criminal justice of Florida state university (1996)

8. Michael Kunz & Patrick Wilson, Computer Crime and Computer Fraud, University of Maryland, Department of Criminology and Criminal Justice Fall, 2004

9. Kang Shuhua (1991). “Criminology” Beijing: Peking University Press.

10. Cornwall, Hugo (1987). Data theft: computer fraud, industrial espionage and information crime.pp.46, London: Heinemann Professional Press.

11.Lishan Adam, “Information and Communication Potential for Social and Economic Development” Association Workshop, (2 March 1999)

12. Teferi Kebede, Information technology in Ethiopia, 1994

13. Security in Cyberspace (Comm. Print 1996), Staff of Senate on Gov't Affairs, Permanent Subcommand on Investigations, 104th Cong.

14. Michael Noblett, Computer Analysis and Response Team (CART): The Microcomputer as Evidence, Crime Laboratory Dig. 11 (1992).

15. David J. Audlin, (1992) Crime, Culture and Law Enforcement” Florida State University School of Law.

16. Warren B. Chik* (2006) “Challenges to Criminal Law Making in the New Global Information Society”

17. Cf. John Stuart Mill, on Liberty, 1859; Popper, the Open Society and Its Enemies, 2 volumes, 1945.

18. Department of Trade & Industry, Information Security Breaches Survey: Technical Report, April 2006 06/803

19. Mansell, Robin and Utawhen. (1998). Knowledge Societies: Information technology for sustainable development. Oxford: Oxford University Press.

20. Castells, Manuel. (1996). The Rise of Network Society. The Information Age: Economy, Society and Culture. London: Blackwell

21. Parliamentry office of science and Technology, Post note, October 2006 Number 271

22. "An Introduction to Computer Security" The NIST Handbook Special Publication 800-12, National Institute of Standards and Technology, U.S. Department of Commerce

23. "How to Own an Identity" (Washington Post 02/20/06)

B. WEB PAGES

1. http://en.wikipedia.org/wiki/Data (Accessed on 01, Apr, 2008 G.C)

2. http://library.thinkquest.org/C007091/uses.htm (Accessed on 07, Mar 2008 G.C)

3..http://en.wikipedia.org/wiki/Extortion (Accessed on 17, Apr, 2008 G.C)

4. http://www.ed.uiuc.edu/wp/crime/hacking.htm (Accessed on 17, Apr, 2008 G.C)

5. http://www.cnn.com/SPECIALS/cold.war/spies/melton.essay/ (Accessed on 17, Apr, 2008G.C)

6. http://www.microsoft.com/piracy/ (Accessed on 07, Apr 2008 G.C)

7. http://www.clickz.com/ (Accessed on 05, Apr, 2008 G.C)

8. http://www.uplink.com. Accessed on 01, Apr 2008 G.C)

9. http://www.sh.sd. Org/acceptable_use_of _computer.htm (Accessed on 01, Apr 2008 G.C)

10. http://www.ists.dartmouth.edu (Accessed on 01, Apr 2008 G.C)

11. http://en.wikipedia.org/wiki/Crime Accessed, on 19, May 2008 G.C)

12. http://www.uplink.com.au/lawlibrary/Doc122.html Accessed on 01, Apr, 2008 G.C)

13. http://en.wikipedia.org/wiki/Law_enforcement_agency (Accessed on Jul, 27, 08)

14. http://www.ethiopianembassy.org/judiciary.shtml, (Accessed on Jul, 27, 08)

15. www.law.ed.ac.uk/ahrc/complaw/docs/chik.doc, (Accessed on Jul, 27, 08)

16. http://www.security-gurus.com/ (Accessed on Jul, 27, 08)

17. http:// www.jmu.educomputingsecurityinfohowthe.shtml (Accessed on Jul, 27, 08)