A ANALYSIS OF THE LEGAL FRAMEWORK OF CYBER RELATED CRIMES IN UGANDA

BY

DAVID DDUNGU

1153-01024-02714

A RESEARCH REPORT SUBMITTED TO THE SCHOOL OF LAW
IN PARTIAL FULFILLMENT OF THE REQUIREMENT
FOR THE AWARD OF BACHELORS DEGREE IN
LAWS OF UGANDA KAMPALA
INTERNATIONAL
UNIVERSITY

JUNE 2019

Declaration

I do solemnly declare that this dissertation is my own piece of work which has never been submitted for any award of degree in any university or higher institution of learning.

Signed.....Ddungu David..... Date.....29th June 2019.....

DAVID DDUNGU

Approval

This research report has been carried out by the student and submitted for examination with my approval as the candidate's university Supervisor.

Signature.....Date.....29/6/2019.....

SUPERVISOR: MR. JEROME NENGER

Dedication

This research is dedicated to my beloved parents for the love , care and financial support towards my studies.

Acknowledgements

First and foremost my sincere acknowledges go to my supervisor throughout this dissertation session Mr. Jerome Nenger whose intellectual advice has helped me tremendously in structuring and guiding me through the beginning to the completion of this report.

Secondly I would love to acknowledge my family for their tireless contributions to my curricular studies mostly my father and mother and to my entire family for their patience and sincere contributions to my life.

Last but not least I can't finish without acknowledging my friends and classmates for their efforts and hard work they have provided to me through hard and good times.

May the Good Lord Bless You All.

List of acronyms

ICT	Information and Communication Technologies
IT	Information Technology
UPF	Uganda Police Force
ISP	Internet Service Provider
UN	United Nations
WSIS	World Summit on the Information Society
EU	European Union
CFTC	Commonwealth Fund for Technical Co-operation
IP	Internet Protocol
ITU	International Telecommunication Union

List of cases

R V CROPP (1993) QB 94.C.A

Uganda v Garuhanga and Mugerwa CR 17 of 2004

Ssemujju Ibrahim Nganda & Halima Andallah (2005)

List of statutes

The 1995 Constitution of the Republic of Uganda (As Amended)

The Electronic Transaction Act of 2011

The Electronic Signatures Act of 2011

The Computer Misuse Act 2011

Table of contents

Declaration ii

Approval iii

Dedication iv

Acknowledgements v

List of acronyms vi

List of cases vii

List of statutes viii

Table of contents ix

Abstract xii

CHAPTER ONE 1

1.0 Introduction 1

1.1 Background of the study 1

1.2 Statement of the problem 5

1.3 General Objective of the study 5

1.4 Specific Objectives of the study 5

1.5 Research questions 6

1.6 Scope of the study 6

1.7 Significance of the study 6

1.8 Methodology 7

1.9 Literature review 7

1.10 Chapterization 21

CHAPTER TWO 22

LEGAL FRAMEWORK ON CYBER SECURITY IN UGANDA 22

2.0 Introduction 22

2.1 Electronic Transaction Act 22

2.2 The Electronic Signatures Act 23

2.3 The Computer Misuse Act 23

CHAPTER THREE 26

CHALLENGES ASSOCIATED WITH CYBER CRIME 26

3.0 Introduction 26

3.1 Reliance on ICTs 26

3.2 Number of users 27

3.3 Availability of devices and access 28

3.4 Availability of information 29

3.5 Missing mechanisms of control 30

3.6 Independence of location and presence at the crime site 30

3.7 Automation 31

3.8 Resources 32

3.9 Conclusion 32

CHAPTER FOUR 34

STRATEGIES IN THE FIGHT AGAINST CYBERCRIME 34

4.0 Introduction 34

4.1 Implementation of existing strategies 34

4.2 Regional differences 34

4.3 Relevance of cybercrime issues within the pillars of cyber security 35

4.4 A cybercrime policy as starting point 35

4.5 Responsibility within the government 36

4.6 Defining the different components 36

4.7 Determination of stakeholders 37

4.8 Defining key topics for legislation 38

4.9 Legal measures 39

4.10 Conclusion 40

CHAPTER FIVE 42

LEGAL PENALTIES AND CONTRIBUTIONS TO THE ELIMINATION OF CYBER CRIMES 42

5.0 Introduction 42

5.1 United Nations and United Nations Office on Drugs and Crimes 42

5.2 International Telecommunication Union 44

5.3 European Union 45

5.4 The Commonwealth 46

5.5 Conclusion 46

5.6 Recommendations 47

References 49

Abstract

This report provides a comprehensive overview of the most relevant topics linked to the legal aspects of cybercrime and focuses on the demands of developing countries. Due to the transnational dimension of cybercrime, the legal instruments are the same for developing and developed countries. However, the references used were selected for the benefit of the case study (Uganda), in addition to a broad selection of resources provided for a more in-depth study of the different topics. Whenever possible, publicly available sources were used, including many free-of-charge editions of online law journals. The report contains five main chapters. After an introduction (*Chapter 1*), it provides an overview of the phenomena of cybercrime (*Chapter 2*). This includes descriptions of how crimes are committed and explanations of the most widespread cybercrime offences such as hacking, identity theft and denial-of service attacks. An overview of the causes of cybercrimes in Uganda and the world at large, prosecution of cybercrime (*Chapters 3* and *4*). After a summary of some of the activities undertaken by international and regional organizations in the fight against cybercrime and also it continues with an analysis of different legal approaches with regard to substantive criminal law, procedural law, digital evidence, international cooperation and the responsibility of Internet service providers (*Chapter 5*) discusses the conclusions and recommendations to the study.

CHAPTER ONE

1.0 Introduction

This chapter covers the background of the study, the statement problem, purpose, objectives and research questions, the significance, scope, chapterization and literature review of the study.

1.1 Background of the study

The Internet is one of the fastest-growing areas of technical infrastructure development. Today, information and communication technologies (ICTs) are omnipresent and the trend towards digitization is growing. The demand for Internet and computer connectivity has led to the integration of computer technology into products that have usually functioned without it, such as cars and buildings. Electricity supply, transportation infrastructure, military services and logistics virtually all modern services depend on the use of ICTs[1].

Although the development of new technologies is focused mainly on meeting consumer demands in western countries, developing countries can also benefit from new technologies. With the availability of long-distance wireless communication technologies such as WiMAX and computer systems that are now available for less than USD 200, many more people in developing countries should have easier access to the Internet and related products and services. The influence of ICTs on society goes far beyond establishing basic information infrastructure. The availability of ICTs is a foundation for development in the creation, availability and use of network-based services[2].

E-mails have displaced traditional letters; online web representation is nowadays more important for businesses than printed publicity materials; and Internet-based communication and phone services are growing faster than landline communications[3]. The availability of ICTs and new network-based services offer a number of advantages for society in general, especially for

---

[1] BBC News of 11, 05, 2005, www.news.bbc.co.uk

[2] Florence Tushabe and Baryamureeba Venansius, (2005). *Cyber Crime in Uganda: Myth or Reality?*, Proceedings of the World Academy of Science, Engineering and Technology, Volume 8.

[3] Ibid

developing countries. ICT applications, such as e-government, e-commerce, e-education, e-health and e-environment, are seen as enablers for development, as they provide an efficient channel to deliver a wide range of basic services in remote and rural areas. ICT applications can facilitate the achievement of millennium development targets, reducing poverty and improving health and environmental conditions in developing countries. Given the right approach, context and implementation processes, investments in ICT applications and tools can result in productivity and quality improvements[4].

In turn, ICT applications may release technical and human capacity and enable greater access to basic services. In this regard, online identity theft and the act of capturing another person's credentials and/or personal information via the Internet with the intent to fraudulently reuse it for criminal purposes is now one of the main threats to further deployment of e-government and e-business services[5]. The costs of Internet services are often also much lower than comparable services outside the network. E-mail services are often available free of charge or cost very little compared to traditional postal services. The online encyclopedia Wikipedia can be used free of charge, as can hundreds of online hosting services.[6]

Lower costs are important, as they enable services to be used by many more users, including people with only limited income. Given the limited financial resources of many people in developing countries, the Internet enables them to use services they may not otherwise have access to outside the network. Cyber crime explains a criminal activity done using the computer over the internet to perform illegal acts. It is associated with offences to do with computers and the internet, inclusive of misuse of computer systems and data[7].

Finding response strategies and solutions to the threat of cybercrime is a major challenge, especially for developing countries. A comprehensive anti-cybercrime strategy generally contains technical protection measures, as well as legal instruments. The development and

---

[4] Geoffrey Wold, (2007). *Computer Crime: The Undetected Disaster*, Disaster Recovery Journal, McGladrey and Pullen Publication.

[5] ITU, ICT Applications and Cyber security www.itu.int/ITU-D/asp/CMS.com

[6] www.wikipedia.com

[7] Tim Simcoe (2005), Open standards and Intellectual Property Rights, Open Innovation: Researching a New Paradigm, Oxford University Press.

implementation of these instruments need time. Technical protection measures are especially cost-intensive. Developing countries need to integrate protection measures into the roll-out of the Internet from the beginning, as although this might initially raise the cost of Internet services, the long-term gains in avoiding the costs and damage inflicted by cybercrime are large and far outweigh any initial outlays on technical protection measures and network safeguards[8].

The risks associated with weak protection measures could in fact affect developing countries more intensely, due to their less strict safeguards and protection. The ability to protect customers, as well as firms, is a fundamental requirement not only for regular businesses, but also for online or Internet-based businesses. In the absence of Internet security, developing countries could encounter significant difficulties promoting e-business and participating in online service industries. The development of technical measures to promote cyber-security and proper cybercrime legislation is vital for both developed countries and developing countries. Compared with the costs of grafting safeguards and protection measures onto computer networks at a later date, it is likely that initial measures taken right from the outset will be less expensive. Developing countries need to bring their anti-cybercrime strategies into line with international standards from the outset[9].

Police records in Uganda do not have any complaint about computer crime and there are no other formal reports about cyber crime rates in Uganda. Does this mean that Internet users in Uganda have not been victims or perpetrators of Internet crimes? Informal and scanty reports about computer crime in Africa and in Uganda particularly result in a misconception that those crimes do not feature there. This deprives decision makers, lawmakers and other stakeholders vital information that could be exploited for better planning and decision-making. Uganda is a small landlocked country in East Africa with a population of 27 million inhabitants, 12% of which live in urban areas. Information and Communications Technology (ICTs) are generally becoming

[8] Mitnick, Kevin and Simon, L. William, (2005). *The Art of Intrusion, The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers*, Hardback ISBO.

[9] Ibid

very popular with telecommunications companies configuring email and Internet services on almost all mobile phones[10].

By 2004, the nationwide population of Internet users, according to the World Fact Book, was 125,000 although it is estimated that the Internet users are as many as 2 million. The cyberspace is the virtual world that Internet users inhabit when they are online[11]. It has been defined by Joseph Migga Kizza as the concept of an environment made up of invisible information. When computer users log onto the Internet, they are able to perform various tasks and services like browsing the World Wide Web, chatting with fellow cyber citizens, transferring files from one computer to another, remote logging to another computer, sending electronic mail, conducting electronic commerce, video conferencing and more. The many functionalities and freedom of use while in the cyberspace brings an equal ease of committing immoral acts and crimes[12].

Cyberspace crimes are the crimes that are committed while in the cyberspace. They include crimes like cyber terrorism, intellectual property infringement, hacking, industrial espionage, on-line child exploitation, Internet usage policy abuses, illegal purchase of goods, sexual assault, internet fraud, software piracy, viruses, impersonation and many more. Laws governing the cyberspace would protect the victims of cyber crime to a certain extent by acting as a deterrent measure and also as a means of possible compensation[13]. Ugandan laws have not yet been modified to expressly define and condemn computer crime. The Computer Misuse Bill, 2003 is still being tabled in the parliament to become an Act. In this paper, we shall use 'crime' as recognized by the international community and as elaborated in. This study aimed at investigating whether Internet users in Uganda have been victims or perpetrators of Internet crimes and if so, what the statistics are and where they are reported[14].

---

[10] Davis Weddi and Steven Candia, (2005). *Porn web site sells Ugandans*", Sunday Vision Newspaper, 24th July.

[11] The Daily Monitor of 2005 5th 05

[12] Ibid

[13] Ibid

[14] Florence Tushabe and Baryamureeba Venansius, (2005). *Cyber Crime in Uganda: Myth or Reality?*, Proceedings of the World Academy of Science, Engineering and Technology, Volume 8.

1.2 Statement of the problem

There is hacking into Internet networks of especially importers of goods from places like Dubai, China and Japan. The unsuspecting business people usually get to discover when either there money has been stolen or the goods they ordered from Europe, China, Japan or Dubai have been diverted to somewhere else. There are also Ugandans who are using the Internet to push through forged travellers' cheques, which they use to purchase goods from unsuspecting business people in Europe, Dubai, China and Japan. What has happened is that manufacturers or traders outside Uganda dispatch goods based on the forged travellers' cheques as confirmation for payment only to discover they cannot cash the cheques among these are Ugandans defrauding foreign business people. Ugandans are also in the habit of forging ministry tender documents claiming they have secured large contracts; and when these unsuspecting foreigners send the goods to Uganda, the culprits receive the goods and cut all communication links. Cases have also been reported where money is way-laid by cyber criminals who hack into people's email accounts; they impersonate the real owners of such email addresses, convince the senders of the money that they have changed bank accounts and in the process, such money gets diverted. People are also defrauded on cell phones but the problem with that is people are reluctant to report to Police. Therefore this research seeks to expose the various cyber related crimes and legal framework on the penalties and implications of cyber crimes in Uganda.

1.3 General Objective of the study

The general objective of this study is to investigate the legal background and regulation of cyber related criminal activities in Uganda.

1.4 Specific Objectives of the study

I. To establish the legal framework governing cyber related crimes in Uganda.

II. To analyze the impact and challenges associated with cyber crime to the consumers in Uganda.

III. To investigate the various cyber crime strategies that have been put in place to fight cyber crimes in Uganda

IV. To investigate the legal penalties and contributions to the elimination of cyber crimes in Uganda and suggest possible recommendations.

1.5 Research questions

I. What is the legal framework governing cyber related crimes in Uganda?

II. What are the various impacts and challenges associated with cyber crime to the consumers in Uganda?

III. What are the various cyber crime strategies that have been put in place to fight cyber crimes in Uganda?

IV. What are the legal penalties and contributions to the elimination of cyber crimes in Uganda and suggest possible recommendations?

1.6 Scope of the study

The research will be carried out in central Uganda, it will focus on all community members from those that own internet cafes, ministries that utilize computers among other companies, it will also embark on the community members who have been culprits of cyber crimes over the years.

The study contains the meaning, relevance and clear knowledge and understanding of information technology, the impact of cyber crimes to the community or consumers in general, the challenges and legal framework of this problem both to the community and the government of Uganda.

The research covers a period of 8 years since the enactment of the Computer Misuse Act till now, the research assesses the information gathered on the implementation of the act from 2012 to date.

1.7 Significance of the study

This research is of great importance to various entities, first and foremost, the research will be relevant to the researcher in achieving his required objective (graduating in laws), secondly the research is of great importance to the Government of Uganda (GoU) in practicing the process of peace and conflict resolution.

The research will be of great importance to all IT companies and the Ministry of communication on embarking on the elimination of cyber crimes and related challenges. The study will expound on the legal framework and explain on the various cases related to cyber crimes in Uganda in order to help both the community and the concerned parties on how to overcome cyber crimes.

1.8 Methodology

In order to achieve the objectives of the study successfully, the researcher will adopt a Doctrinal research design to help in the compilation of this research, the will basically review secondary information from the university library, and all other publications concerned with cyber security in Uganda. These tools are expected to help in the problem and its scope and gather relevant information concerning the research topic.

1.9 Literature review

The term "cybercrime" is used to cover a wide variety of criminal conduct. As recognized crimes include a broad range of different offences, it is difficult to develop a typology or classification system for cybercrime. One approach can be found in the Convention on Cybercrime, which distinguishes between four different types of offences: Offences against the confidentiality, integrity and availability of computer data and systems; Computer-related offences; Content-related offences; and Copyright-related offences. In Uganda, the Electronic Signature Act, Computer misuse Act and Electronic Transfer Act have recently been implemented to protect against cyber crime while promoting a safe and environmentally healthy electronic transacting environment. However, with the available legal and institutional framework, the country continues to experience increasing cyber crimes.[15] Crimes such as cyber terrorism, intellectual property infringement, internet usage policy abuses, internet fraud, industrial espionage and altering of data, on-line child exploitation and pornography, illegal goods purchasing, piracy, impersonation and hacking, remain a challenge.[16] This is yet to involve more undiscovered crime given the pace of advancing technology and while the future of technology remains rich

[15] Ministry of Information and Communications Technology (2011), National Information Security Strategy (NIIS), 2011

[16] Florence Tushabe (2004), Computer Forensics for Cyberspace Crimes, University of Colombo.

with innovation.[17] In Uganda a significant percentage of transactions and processes are adopting networking technology.[18] Institutions such as the Ministry of Information and Telecommunication and the Uganda Police Force (UPF) have policy frameworks designed to address cyber crime. UPF is legally mandated by the Constitution to prevent and detect crime [19] in order to ensure that the rule of law prevails. However, the institution knows little about computer crimes especially in detecting cyber crimes,[20] are yet these are committed by highly skilled and technical personnel.

In January 2005[21] for example, Andrew Zzimwe Kasagga together with two Congolese were wanted by Interpol (Kenya) for being involved in a multi-million dollar scam. They were accused of masterminding bank when they engaged in fraudulent intranet bank transfer between Standard Charted Bank, Nairobi and Barclays Bank Kampala. The Kenyan Standard Chartered Bank staff wired $5million in three installments to separate bank accounts in Kampala. Suspected conmen got the Nairobi based bank to wire one million dollars to Zzimwe's Barclays Bank account in Kampala and another $2 million from Kenya was intercepted at Crane Bank. It had allegedly been sent to another suspect, Kampala lawyer, Paul Kalemera. While further investigations and trials were being conducted, another $3 million being swindled from Kenya was detected before it was sent to a forex bureau via the DFCU bank in Kampala.

This typology is not wholly consistent, as it is not based on a sole criterion to differentiate between categories. Three categories focus on the object of legal protection: "offences against the confidentiality, integrity and availability of computer data and systems"; content-related offences; and copyright- related offences. The fourth category of "computer-related offences" does not focus on the object of legal protection, but on the method used to commit the crime. This inconsistency leads to some overlap between categories. In addition, some terms that are used to describe criminal acts (such as "cyberterrorism" or "phishing") cover acts that fall within

[17] Mitnick, Kevin and Simon, L. William (2005), The Art of Intrusion, The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers, Hardback ISBO.

[18] Florence Tushabe (2004), Computer Forensics for Cyberspace Crimes, University of Colombo.

[19] The Constitution of the Republic of Uganda 1995, Article 212 (iii)

[20] Florence Tushabe (2004), Computer Forensics for Cyberspace Crimes, University of Colombo.

[21] Ssemujju Ibrahim Nganda & Halima Abdallah (2005),"Interpol pursues Zzimwe fraud case, The Weekly Observer, 13th January 2005.

several categories. Nonetheless, the four categories can serve as a useful basis for discussing the phenomena of cybercrime[22].

The criminal abuse of information technology and the necessary legal response are issues that have been discussed ever since the technology was introduced. Over the last 50 years, various solutions have been implemented at the national and regional levels. One of the reasons why the topic remains challenging is the constant technical development, as well as the changing methods and ways in which the offences are committed. In the 1960s, the introduction of transistor-based computer systems, which were smaller and less expensive than vacuum-tube based machines, led to an increase in the use of computer technology. At this early stage, offences focused on physical damage to computer systems and stored data[23].

Such incidents were reported, for example, in Canada, where in 1969 a student riot caused a fire that destroyed computer data hosted at the university. In the mid 1960s, the United States started a debate on the creation of a central data-storage authority for all ministries. As in each preceding decade, new trends in computer crime and cybercrime continued to be discovered in the 21st century. The first decade of the new millennium was dominated by new, highly sophisticated methods of committing crimes, such as "phishing", and "botnet attacks", and the emerging use of technology that is more difficult for law enforcement to handle and investigate, such as "voice-over-IP (VoIP) communication" and "cloud computing". It is not only the methods that changed, but also the impact. As offenders became able to automate attacks, the number of offences increased. Countries and regional and international organizations have responded to the growing challenges and given response to cybercrime high priority. Crime statistics can be used by academia and policy-makers as a basis for discussion and for the ensuing decision-making process. Furthermore, access to precise information on the true extent of cybercrime would enable law-enforcement agencies to improve anti-cybercrime strategies, deter potential attacks and enact more appropriate and effective legislation. However, it is difficult to quantify the impact of cybercrime on society on the basis of the number of offences

[22] Florence Tushabe, (2004). *Computer Forensics for Cyberspace Crimes*, University of Colombo.

[23] Ibid

carried out in a given time-frame. Such data can in general be taken from crime statistics and surveys, but both these sources come with challenges when it comes to using them for formulating policy recommendations[24].

To make matters worse, organizations that make use of cyberspace services also lack sufficient information on security controls. This complicates the process of prevention and detection of crime to duly seek police assistance.[25] This portrays that much as UPF is mandated to combat crime, it requires informational support which is not available because the level of risk identification and evaluation is poor. For example in July 2004, Grace Muwanguzi lost a passport and 500 dollars to a fake company arranging visas, free transport and accommodation in Canada. The company camouflaged under an HIV/AIDS project of Trainer of Trainers course (ToT) by the Ministry of Health where officials were to travel to Toronto. Grace viewed their website over the internet with details of the conference, and met the requirements. On the expected day of returning passports and visas the perpetrators disappeared affecting many others like Grace.[26]

The offence described as "hacking" refers to unlawful access to a computer system, one of oldest computer-related crimes. Following the development of computer networks (especially the Internet), this crime has become a mass phenomenon. Famous targets of hacking attacks include the US National Aeronautics and Space Administration (NASA), the US Air Force, the Pentagon, Yahoo, Google, eBay and the German Government. Examples of hacking offences include breaking the password of password-protected websites and circumventing password protection on a computer system. But acts related to the term "hacking" also include preparatory acts such as the use of faulty hardware or software implementation to illegally obtain a password to enter a computer system, setting up "spoofing" websites to make users disclose their passwords and installing hardware and software-based keylogging methods (e.g. "keyloggers")

[24] Geoffrey Wold, (2007). *Computer Crime: The Undetected Disaster*, Disaster Recovery Journal, McGladrey and Pullen Publication.

[25] Florence Tushabe (2004), Computer Forensics for Cyberspace Crimes, University of Colombo.

[26] Joseph Migga Kizza, "Ethical and Social Issues in the Information Age," Second Edition, Springer, 2003.

that record every keystroke – and consequently any passwords used on the computer and/or device[27].

The legal framework is also still limited in scope with changing technology. The Electronic Transaction Act[28] provides for the use, security, facilitation and regulation of electronic communications and transactions in addition to encouraging the use of e-government services and providing for matters connected therewith to broadly remove existing legal impediments that can prevent a person from transacting electronically because of the omissions of the traditional laws; making provisions for functional equivalency making paper transactions and electronic transactions to be treated similarly; establishing rules that validate and recognize contracts formed through electronic means and setting out default rules for contract formation and governance of electronic contract performance; providing the characteristics of a valid electronic writing and an original document; in addition to supporting the admission of computer evidence in courts and arbitration proceedings. However, this will affect the position of judges as prosecutions for Cyber crime will requires judges to possess enough technical knowledge to be able properly to adjudicate on Cyber crime cases or else inappropriate acquittals will be exercised as seen in ***R V CROPP***[29] where the jury was misled by trial judge in the application of the Computer Misuse Act 1990 (UK).

The motivation of offenders varies. Some offenders limit their activities to circumventing security measures only in order to prove their abilities. Others act through political motivation (known as "hacktivism") – one example is a recent incident involving the main United Nations website. In most cases, though, the motivation of the offender is not limited to illicit access to a computer system. Offenders use this access to commit further crimes, such as data espionage, data manipulation or denial- of-service (DoS) attacks. In most cases, illegal access to the computer system is only a vital first step.

Many analysts recognize a rising number of attempts to illegally access computer systems, with over 250 million incidents recorded worldwide during the month of August 2007 alone. Three

---

[27] *Gercke*, The Slow Wake of a Global Approach against Cybercrime, Computer Law Review International 2006, 141.

[28] Electronic Transaction Act 2011

[29] (1993) QB 94.C.A

main factors have supported the increasing number of hacking attacks: inadequate and incomplete protection of computer systems, development of software tools that automate the attacks, and the growing role of private computers as a target of hacking attacks[30].

The Electronic Signatures Act[31] regulates the use of electronic signatures and ensures that transactions are carried out in a secure environment; enhances authenticity and security of documents by establishing a public key infrastructure; recognizes different signature creating technologies; and provides effective administrative structures for certification of authorities.

Hundreds of millions of computers are connected to the Internet, and many computer systems are without adequate protection in place to prevent illegal access. Analysis carried out by the University of Maryland suggests that an unprotected computer system that is connected to the Internet is likely to experience attack within less than a minute. The installation of protective measures can lower the risk, but successful attacks against well-protected computer systems prove that technical protection measures can never completely stop attacks. There has been development of software tools that automate the attacks; recently, software tools are being used to automate attacks. With the help of software and pre- installed attacks, a single offender can attack thousands of computer systems in a single day using one computer. If the offender has access to more computers e.g. through a botnet he/she can increase the scale still further. Since most of these software tools use preset methods of attacks, not all attacks prove successful. Users that update their operating systems and software applications on a regular basis reduce their risk of falling victim to these broad-based attacks, as the companies developing protection software analyse attack tools and prepare for the standardized hacking attacks.

The Computer Misuse Act[32] regulates cyber crime to promote safety and security of electronic transactions and information systems; prevents unlawful access, abuse and misuse of electronic devices like mobile phones including computers and secures the conduct of electronic transactions in a trustworthy electronic environment in addition to providing for other related matters. The cyber laws provide tough penalties for offenders where companies and individuals involved may be de-licensed and if charged in court risk serving up to three years in prison.

---

[30] *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, Computer und Recht International, 2006, page 95.

[31] The Electronic Signatures Act 2011

[32] The Computer Misuse Act

High-profile attacks are often based on individually-designed attacks. The success of those attacks is often not the result of highly sophisticated methods, but the number of attacked computer systems. Tools enabling these standardized attacks are widely available over the Internet – some for free, but efficient tools can easily cost several thousands of US dollars. One example is a hacking tool that allows the offender to define a range of IP-addresses (e.g. from 111.2.0.0 to 111.9.253.253). The software allows for the scanning for unprotected ports of all computers using one of the defined IP-addresses. Access to a computer system is often not the primary motivation of an attack. Since business computers are generally better protected than private computers, attacks on business computers are more difficult, challenges and legal response to carry out using pre-configured software tools.

Over the past few years, offenders have focused their attacks increasingly on private computers, since many private computers are inadequately protected. Further, private computers often contain sensitive information (e.g. credit card and bank account details). Offenders are also targeting private computers because, after a successful attack, offenders can include the computer in their botnet and use the computer for further criminal activities. Illegal access to a computer system may be viewed as analogous to illegal access to a building and is recognized as a criminal offence in many countries. Analysis of different approaches to the criminalization of computer access shows that enacted provisions in some cases confuse illegal access with subsequent offences or attempt to limit criminalization of illegal access to grave violations only. Some provisions criminalize the initial access, while other approaches limit the criminal offence only to those cases where the accessed system is protected by security measures or the perpetrator has harmful intentions or data was obtained, modified or damaged. Other legal systems do not criminalize mere access, but focus on subsequent offences.

However, with supportive laws in place to address cyber crime, police records in the country reflect few complaints about computer crime with no formal reports about cyber crime.[33] But this does not imply that internet users in Uganda have not fallen victims or perpetrators of major internet crimes. According to Tumushabe, the crimes have been on the increase since the early

[33] Florence Tushabe and Baryamureeba Venansius (2005), Cyber Crime in Uganda: Myth or Reality?, Proceedings of the World Academy of Science, Engineering and Technology, Volume 8.

2000 but with informal and scanty reports, thus public gets to know less of it.[34] This reflects a challenge to the law making and enforcement institutions, decision makers and stakeholders in advancing better protective mechanisms.

Sensitive information is often stored in computer systems. If the computer system is connected to the Internet, offenders can try to access this information via the Internet from almost any place in the world. The Internet is increasingly used to obtain trade secrets. The value of sensitive information and the ability to access it remotely makes data espionage highly interesting. In the 1980s, a number of German hackers succeeded in entering US government and military computer systems, obtaining secret information and selling this information to agents from a different country. Offenders use various techniques to access victims' computers, including software to scan for unprotected ports or circumvent protection measures, as well as "social engineering".

The Ministry of Information and Communication Technology has also shown a level of interest in developing and protecting against the abuse of technology. The ministry proposed strategies to establish a national computer incident response team with a 24/7 call center, constituency computer incident response teams, a watch and alert center, and reporting mechanisms. Its framework is to develop a strategy within the government to ensure access and full time availability of organized information and its integrity; keeping abreast with modern, safe and better technologies of information security by considering the trend of globalization; recognizing the contribution of the businesses and organizations in enhancing information security in addition to promoting information protection schemes and mechanisms for assurance. [35]

The last approach especially, which refers to a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people into breaking normal security procedures, is interesting as it not based on technical means. In the context of illegal access it describes the manipulation of human beings with the intention of gaining access to computer systems. Social engineering is usually very successful, because the weakest link in computer security is often the users operating the computer system. One example is "phishing", which has

[34] Ibid

[35] The Ministry of Information and Communications Technology (2011), National Information Security Strategy (NIIS) Final Draft, 2011.

recently become a key crime committed in cyberspace and describes attempts to fraudulently acquire sensitive information (such as passwords) by masquerading as a trustworthy person or business (e.g. financial institution) in a seemingly official electronic communication.

Although the human vulnerability of users opens the door to the risk of scams, it also offers solutions. Well-educated computer users are not easy victims for offenders using social engineering. As a consequence, user education should be an essential part of any anti-cybercrime strategy. In addition, technical measures can be taken to prevent illegal access.

OECD highlights the importance of cryptography for users, as cryptography can help improve data protection. If the person or organization storing information uses proper protection measures, cryptographic protection can be more efficient than any physical protection. The success of offenders in obtaining sensitive information is often due to the absence of protection measures. Since important information is increasingly being stored in computer systems, it is essential to evaluate whether the technical protection measures taken by the users are adequate, or if law-makers need to establish additional protection by criminalizing data espionage.

Despite, this interest, the ministry has little knowledge about the actual issues involved in securing networks and electronic assets. For example much as internet users are experiencing malicious spread of viruses through emails and these have proved much more than a release of e-mail attachment with greater consequences, support to secure systems is still difficult. Malicious spread of internet virus is leading to potential losses in productivity by corrupting intellectual assets.[36] Worse still individuals with technical knowledge of networks and networking devices continue to steal sensitive information and money through online access to bank accounts or credit card numbers used by online retailers or conduct a host of juvenile pranks like erasing backup files, raising the temperature in buildings, turning off phone and traffic systems.[37]

[36] Georges P. Racine, (London), *A Review Of Key Issues Related To The Re-Licensing Of Telecom Networks And Services In Developing Countries*, One-Day Course on Re-Licensing (GICTD – World Bank), 30 March 2005, Washington DC.

[37] The Ministry of Information and Communications Technology (2011), National Information Security Strategy (NIIS) Final Draft, 2011.

For instance In ***Uganda v Garuhanga and Mugerwa***[38] computer data was manipulated resulting into 3.8 Billion Shillings loss for Shell Uganda Ltd. The accused were charged with embezzlement and false accounting as there was no enabling law by then, for charges of computer forgery and computer fraud.

Although offenders usually target business secrets, data stored on private computers are also increasingly targeted. Private users often store bank-account and credit-card information on their computer. Offenders can use this information for their own purposes (e.g. bank-account details to make money transfers) or sell it to a third party. Credit-card records are for example sold for up to USD 60. Hackers' focus on private computers is interesting, as the profits from business secrets are generally higher than the profits to be made from obtaining or selling single credit-card information. However, since private computers are generally less well protected, data espionage based on private computers is likely to become even more profitable.

There are two approaches to obtaining information. Offenders can access a computer system or data storage device and extract information; or try to manipulate the user to make them disclose the information or access codes that enable offenders to access information ("phishing"). Offenders often use computer tools installed on victims' computers or malicious software called spyware to transmit data to them. Various types of spyware have been discovered over recent years, such as keyloggers. Keyloggers are software tools that record every keystroke typed on an infected computer's keyboard. Some keyloggers send all recorded information to the offender, as soon as the computer is connected to the Internet. Others perform an initial sort and analysis of the data recorded (e.g. focusing on potential credit-card information) to transmit only major data discovered. Similar devices are also available as hardware devices that are plugged in between the keyboard and the computer system to record keystrokes on the keyboard. Hardware-based keyloggers are more difficult to install and detect, as they require physical access to the computer system. However, classical anti-spyware and anti-virus software is largely unable to identify them.

The Ministry of Communication faces challenges in its institutional framework due to non uniform uptake of ICT by different government ministries, agencies, departments as well as

[38] CR 17 of 2004

local governments. The level of IT remains different. This being the case different entities have advanced technology differently and their systems therefore vary. While some have information security strategies and policies others do not and while others have higher levels of ICT development and implementation, others do not and require hiring IT services to install, implement and update systems. This leads to infringements of information security. In addition, the lack of top management support and too little financial support in implementing information security measures is also prevalent among agencies and organization making institutional policy difficult. [39]

Apart from accessing computer systems, offenders can also obtain data by manipulating the user. Recently, offenders have developed effective scams to obtain secret information (e.g. bank-account information and credit-card data) by manipulating users using social engineering techniques. "Phishing" has recently become one of the most important crimes related to cyberspace. The term "phishing" is used to describe a type of crime that is characterized by attempts to fraudulently acquire sensitive information, such as passwords, by masquerading as a trustworthy person or business (e.g. financial institution) in an apparently official electronic communication.

Much as the country is experiencing various losses and damages caused by fraud, theft, willful neglect, gross negligence, vandalism, sabotage, extortion there is still a general failure to secure adequate funding for information security; a failure to comply with the national laws, contracts, standards in which business operations should be conducted. This has destroyed plans, management and monitoring of performance of technology-related projects, products, services, processes, staff and delivery channels and instead fueled negative effects of public opinion, customer opinion and market reputation. Under such circumstances there is unauthorized disclosure and modification of information due to loss of employee integrity and making inappropriate use of information. For example the money scam faced by MTN.[40] The Ministry therefore finds difficulties in managing cohesive issues that arise, more so when support funds remain limited.

[39] The Ministry of Information and Communications Technology (2011), National Information Security Strategy (NIIS) Final Draft, 2011.

[40] Computer Misuse Act 2011

Offenders can intercept communications between users (such as e-mails) or other forms of data transfers (when users upload data onto webservers or access web-based external storage media) in order to record the information exchanged. In this context, offenders can in general target any communication infrastructure (e.g. fixed lines or wireless) and any Internet service (e.g. e-mail, chat or VoIP communications). Most data-transfer processes among Internet infrastructure providers or Internet service providers are well protected and difficult to intercept. However, offenders search for weak points in the system. Wireless technologies are enjoying greater popularity and have in the past proved vulnerable. Nowadays, hotels, restaurants and bars offer customers Internet access through wireless access points. However, the signals in the data exchanges between the computer and the access point can be received within a radius of up to 100 metres. Offenders who wish to intercept a data-exchange process can do so from any location within this radius. Even where wireless communications are encrypted, offenders may be able to decrypt the recorded data.

To gain access to sensitive information, some offenders set up access points close to locations where there is a high demand for wireless access (e.g. near bars and hotels). The station location is often named in such a way that users searching for an Internet access point are more likely to choose the fraudulent access point. If users rely on the access provider to ensure the security of their communication without implementing their own security measures, offenders can easily intercept communications. The use of fixed lines does not prevent offenders from intercepting communications. Data transmissions passing along a wire emit electromagnetic energy. If offenders use the right equipment, they can detect and record these emissions and may be able to record data transfers between users' computers and the connected system, and also within the computer system. Most countries have moved to protect the use of telecommunication services by criminalizing the illegal interception of phone conversations. However, given the growing popularity of IP-based services, law- makers may need to evaluate to what extent similar protection is offered to IP-based services.

Computer data are vital for private users, businesses and administrations, all of which depend on the integrity and availability of data. Lack of access to data can result in considerable (financial) damage. Offenders can violate the integrity of data and interfere with them by deleting, suppressing or altering computer data. One common example of the deletion of data is the computer virus. Ever since computer technology was first developed, computer viruses have

threatened users who failed to install proper protection. Since then, the number of computer viruses has risen significantly. Not only has the number of virus attacks increased, but also the techniques and functions of viruses (payload) have changed.

Previously, computer viruses were distributed through storage devices such as floppy disks, whilst today most viruses are distributed via the Internet as attachments either to e-mails or to files that users download. These efficient new methods of distribution have massively accelerated virus infection and vastly increased the number of infected computer systems. The computer worm SQL Slammer was estimated to have infected 90 per cent of vulnerable computer systems within the first 10 minutes of its distribution. The financial damage caused by virus attacks in 2000 alone was estimated to amount to some USD 17 billion. In 2003, it was still more than USD 12 billion. Most first-generation computer viruses either deleted information or displayed messages. Recently, payloads have diversified. Modern viruses are able to install back-doors enabling offenders to take remote control of the victim's computer or encrypt files so that victims are denied access to their own files, until they pay money to receive the key[41].

The same concerns over attacks against computer data apply to attacks against computer systems. More businesses are incorporating Internet services into their production processes, with benefits of 24-hour availability and worldwide accessibility. If offenders succeed in preventing computer systems from operating smoothly, this can result in great financial losses for victims. Attacks can be carried out by physical attacks on the computer system. If offenders are able to access the computer system, they can destroy hardware. For most criminal legal systems, remote physical cases do not pose major problems, as they are similar to classic cases of damage or destruction of property. However, for highly profitable e-commerce businesses, the financial damages caused by attacks on the computer system are often far greater than the mere cost of computer hardware.

More challenging for legal systems are web-based scams. Examples of these remote attacks against computer systems include computer worms and denial-of-service (DoS) attacks. Computer worms are a subgroup of malware (like computer viruses). They are self-replicating computer programs that harm the network by initiating multiple data-transfer processes. They

[41] Williams, M. (2006) *Virtually Criminal: Crime, Deviance and Regulation Online,* Routledge, London.

can influence computer systems by hindering the smooth running of the computer system, using system resources to replicate themselves over the Internet or generating network traffic that can close down availability of certain services (such as websites).

While computer worms generally influence the whole network without targeting specific computer systems, DoS attacks target specific computer systems. A DoS attack makes computer resources unavailable to their intended users. By targeting a computer system with more requests than the computer system can handle, offenders can prevent users from accessing the computer system, checking e-mails, reading the news, booking a flight or downloading files. In 2000, within a short time, several DoS attacks were launched against well-known companies such as CNN, eBay and Amazon. Similar attacks were reported in 2009 on government and commercial websites in the US and South Korea. As a result, some of the services were not available for several hours and even days. The prosecution of DoS and computer-worm attacks poses serious challenges to most criminal law systems, as these attacks may not involve any physical impact on computer systems. Apart from the basic need to criminalize web-based attacks, the question of whether the prevention and prosecution of attacks against critical infrastructure needs a separate legislative approach is under discussion.

Underreporting affects the performance of police in combating cyber crimes. The public does not report to authorities because its hope for justice is low having to deal with an invisible criminal. Moreover the perpetrators also feel protected by a feeling of their invisibility.[42] Indeed cyber bullying is becoming critical in cyber crime yet its impact is overlooked because its hard to monitor.[43] For example one company confessed about an incident of email spoofing in which one supposed employee sent an email to their clients threatening that the aircraft they were using for business was in poor condition and passengers should use it at their own risk. Many passengers began canceling their flights for no apparent good reason. The company sought an IT specialist and together with their system Administrator, carried out the investigation which

[42] Joseph Migga Kizza, "Ethical and Social Issues in the Information Age," Second Edition, Springer, 2003.

[43] Will Gardner (2010), Protecting and Empowering Children and Individuals on-line: Cyber Security Forum, Childnet, London.

traced the bad email to an employee in a competitors company. The case was settled out of court.[44]

1.10 Chapterization

This research contains five chapters; chapter one discusses the introduction and overview of the research and related literature to the study, chapter two looks at the causes of cybercrimes in the country whereas chapter three focuses on the various measures undertaken to control cybercrimes. Chapter four covers the international systems and legal analysis of the international bodies on cybercrimes in the world whereas chapter five concludes the study and provides recommendations to the concerned bodies.

[44] Joseph Migga Kizza, "Ethical and Social Issues in the Information Age," Second Edition, Springer, 2003.

CHAPTER TWO

LEGAL FRAMEWORK ON CYBER SECURITY IN UGANDA

2.0 Introduction

Cyber crime explains a criminal activity done using the computer over the internet to perform illegal acts. It is associated with offences to do with computers and the internet, inclusive of misuse of computer systems and data.

2.1 Electronic Transaction Act

The legal framework is also still limited in scope with changing technology. The **Electronic Transaction Act**[45] provides for the use, security, facilitation and regulation of electronic communications and transactions in addition to encouraging the use of e-government services and providing for matters connected therewith to broadly remove existing legal impediments that can prevent a person from transacting electronically because of the omissions of the traditional laws; making provisions for functional equivalency making paper transactions and electronic transactions to be treated similarly; establishing rules that validate and recognize contracts formed through electronic means and setting out default rules for contract formation and governance of electronic contract performance; providing the characteristics of a valid electronic writing and an original document; in addition to supporting the admission of computer evidence in courts and arbitration proceedings.

However, this will affect the position of judges as prosecutions for Cyber crime will requires judges to possess enough technical knowledge to be able properly to adjudicate on Cyber crime cases or else inappropriate acquittals will be exercised as seen in ***R V CROPP***[46] where the jury was misled by trial judge in the application of the Computer Misuse Act 1990 (UK).

---

[45] Electronic Transaction Act 2011

[1646] (1993) QB 94.C.A

2.2 The Electronic Signatures Act

The **Electronic Signatures Act**[47] regulates the use of electronic signatures and ensures that transactions are carried out in a secure environment; enhances authenticity and security of documents by establishing a public key infrastructure; recognizes different signature creating technologies; and provides effective administrative structures for certification of authorities.

2.3 The Computer Misuse Act

The Computer Misuse Act[48] regulates cyber crime to promote safety and security of electronic transactions and information systems; prevents unlawful access, abuse and misuse of electronic devices like mobile phones including computers and secures the conduct of electronic transactions in a trustworthy electronic environment in addition to providing for other related matters. The cyber laws provide tough penalties for offenders where companies and individuals involved may be de-licensed and if charged in court risk serving up to three years in prison.

However, with supportive laws in place to address cyber crime, police records in the country reflect few complaints about computer crime with no formal reports about cyber crime.[49] But this does not imply that internet users in Uganda have not fallen victims or perpetrators of major internet crimes. According to Tumushabe, the crimes have been on the increase since the early 2000 but with informal and scanty reports, thus public gets to know less of it.[50] This reflects a challenge to the law making and enforcement institutions, decision makers and stakeholders in advancing better protective mechanisms.

The Ministry of Information and Communication Technology has also shown a level of interest in developing and protecting abuse of technology. The ministry proposed strategies to establish a national computer incident response team with a 24/7 call center, constituency computer incident response teams, a watch and alert center, and reporting mechanisms. In its framework is to

---

[47] The Electronic Signatures Act 2011

[20] The Computer Misuse Act

[49] Florence Tushabe and Baryamureeba Venansius (2005), Cyber Crime in Uganda: Myth or Reality?, Proceedings of the World Academy of Science, Engineering and Technology, Volume 8.

[50] Ibid

develop a strategy within the government to ensure access and full time availability of organized information and its integrity; keeping abreast with modern, safe and better technologies of information security by considering the trend of globalization; recognizing the contribution of the businesses and organizations in enhancing information security in addition to promoting information protection schemes and mechanisms for assurance.[51]

Despite, this interest, the ministry has little known about the actual issues involved in securing networks and electronic assets. For example much as internet users are experiencing malicious spread of viruses through emails and these have proved much more than a release of e-mail attachment with greater consequences. Support to secure systems is still difficult. Malicious spread of internet virus is leading to potential losses in productivity by corrupting intellectual assets.[52] Worse still individuals with technical knowledge of networks and networking devices continue to steal sensitive information and money through online access to bank accounts or credit card numbers used by online retailers or conduct a host of juvenile pranks like erasing backup files, raising the temperature in buildings, turning off phone and traffic systems.[53] For instance In ***Uganda v Garuhanga and Mugerwa***[54] computer data was manipulated resulting into 3.8 Billion Shillings loss for Shell Uganda Ltd. The accused were charged with embezzlement and false accounting as there was no enabling law by then, for charges of computer forgery and computer fraud.

The Ministry also faces challenges in its institutional framework due to non uniform uptake of ICT by different government ministries, agencies, departments as well as local governments. The level of IT remains different. This being the case different entities have advanced technology differently and their systems therefore vary. While some have information security strategies and policies others do not and while others have higher levels of ICT development and implementation, others do not and require hiring IT services to install, implement and update

---

[51] The Ministry of Information and Communications Technology (2011), National Information Security Strategy (NIIS) Final Draft, 2011

[52] Georges P. Racine, (London), *A Review Of Key Issues Related To The Re-Licensing Of Telecom Networks And Services In Developing Countries*, One-Day Course on Re-Licensing (GICTD – World Bank), 30 March 2005, Washington DC.

[53] The Ministry of Information and Communications Technology (2011), National Information Security Strategy (NIIS) Final Draft, 2011.

[54] CR 17 of 2004

systems. This leads to infringements of information security. In addition, the lack of top management support and too little financial support in implementing information security measures is also prevalent among agencies and organization making institutional policy difficult.

CHAPTER THREE

CHALLENGES ASSOCIATED WITH CYBER CRIME

3.0 Introduction

This chapter focuses on the various causes of cybercrimes, how they have managed to spread in the country, and how the government has embarked on previous measures of how to control these problems.

3.1 Reliance on ICTs

Many everyday communications depend on ICTs and Internet-based services, including VoIP calls or e- mail communications. ICTs are now responsible for the control and management functions in buildings, cars and aviation services.[55] The supply of energy, water and communication services depend on ICTs. The further integration of ICTs into everyday life is likely to continue. Growing reliance on ICTs makes systems and services more vulnerable to attacks against critical infrastructures[56]. Even short interruptions to services could cause huge financial damages to e-commerce businesses. It is not only civil communications that could be interrupted by attacks; the dependence on ICTs is a major risk for military communications.

Existing technical infrastructure has a number of weaknesses, such as the monoculture or homogeneity of operating systems. Many private users and SMEs use Microsoft's operating system, so offenders can design effective attacks by concentrating on this single target. The dependence of society on ICTs is not limited to the western countries. Developing countries also face challenges in preventing attacks against their infrastructure and users. The development of cheaper infrastructure technologies such as WiMAX698 has enabled developing countries to offer Internet services to more people.

Developing countries can avoid the mistakes of some western countries, which have concentrated mainly on maximizing accessibility, without investing significantly in protection. US experts have explained that successful attacks against the official website of governmental

---

[55] Goodman, The Civil Aviation Analogy – International Cooperation to Protect Civil Aviation Against Cyber Crime and Terrorism in Sofaer/Goodman, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 69

[56] Ibid

organizations in Estonia699 could only take place due to inadequate protection measures. Developing countries have a unique opportunity to integrate security measures early on. This may require greater upfront investments, but the integration of security measures at a later point may prove more expensive in the long run. Strategies must be formulated to prevent such attacks and develop countermeasures, including the development and promotion of technical means of protection, as well as adequate and sufficient laws enabling law-enforcement agencies to fight cybercrime effectively.

3.2 Number of users

The popularity of the Internet and its services is growing fast, with over 2 billion Internet users worldwide by 2010. Computer companies and ISPs are focusing on developing countries with the greatest potential for further growth. In 2005, the number of Internet users in developing countries surpassed the number in industrial nations, while the development of cheap hardware and wireless access will enable even more people to access the Internet. With the growing number of people connected to the Internet, the number of targets and offenders increases. It is difficult to estimate how many people use the Internet for illegal activities. Even if only 0.1 per cent of users committed crimes, the total number of offenders would be more than one million[57]. Although Internet usage rates are lower in developing countries, promoting cybersecurity is not easier, as offenders can commit offences from around the world.

The increasing number of Internet users causes difficulties for the law-enforcement agencies because it is relatively difficult to automate investigation processes. While a keyword-based search for illegal content can be carried out rather easily, the identification of illegal pictures is more problematic. Hash-value based approaches are for example only successful if the pictures were rated previously, the hash value was stored in a data base, and the picture that was analysed has not been modified.

[57] Ibid

3.3 Availability of devices and access

Only basic equipment is needed to commit computer crimes. Committing an offence requires hardware, software and Internet access. With regard to hardware, the power of computers is growing continuously. There are a number of initiatives to enable people in developing countries to use ICTs more widely.[58] Criminals can commit serious computer crimes with only cheap or second-hand computer technology – knowledge counts for far more than equipment. The date of the computer technology available has little influence on the use of that equipment to commit cybercrimes.

Committing cybercrime can be made easier through specialist software tools. Offenders can download software tools designed to locate open ports or break password protection[59]. Due to mirroring techniques and peer-to-peer exchange, it is difficult to limit the widespread availability of such devices. The last vital element is Internet access. Although the cost of Internet access is higher in most developing countries than in industrialized countries, the number of Internet users in developing countries is growing rapidly[60]. Offenders will generally not subscribe to an Internet service to limit their chances of being identified, but prefer services they can use without (verified) registration. A typical way of getting access to networks is the so-called "wardriving". The term describes the act of driving around searching for accessible wireless networks. The most common methods criminals can use to access the network fairly anonymously are public Internet terminals, open (wireless) networks, hacked networks and prepaid services without registration requirements.

Law-enforcement agencies are taking action to restrict uncontrolled access to Internet services to avoid criminal abuse of these services. In Italy and China, for example, the use of public Internet terminals requires the identification of users. However, there are arguments against such identification requirements. Although the restriction of access could prevent crimes and facilitate the investigations of law-enforcement agencies, such legislation could hinder the growth of the information society and the development of e-commerce. It has been suggested that this

---

[58] World Information Society Report 2007", ITU, Geneva, available at: www.itu.int/wisr

[59] Ealy, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, page 9 et seq., available at: www.212cafe.com/download/e-book

[60] Development Gateway's Special Report, Information Society – Next Steps?, 2005

limitation on access to the Internet could violate human rights. For example, the European Court has ruled in a number of cases on broadcasting that the right to freedom of expression applies not only to the content of information, but also to the means of transmission or reception. In the case Autronic v. Switzerland, the court held that extensive interpretation is necessary since any restriction imposed on the means necessarily interferes with the right to receive and impart information. If these principles are applied to potential limitations on Internet access, it is possible that such legislative approaches could entail violation of human rights.

3.4 Availability of information

The Internet has millions of WebPages of up-to-date information. Anyone who publishes or maintains a webpage can participate. One example of the success of user-generated platforms is Wikipedia, an online encyclopaedia where anybody can publish.

The success of the Internet also depends on powerful search engines that enable users to search millions of webpages in seconds. This technology can be used for both legitimate and criminal purposes. "Googlehacking" or "Googledorks" describes the use of complex search-engine queries to filter many search results for information on computer security issues. For example, offenders might aim to search for insecure password protection systems. Reports have highlighted the risk of the use of search engines for illegal purposes. An offender who plans an attack can find detailed information on the Internet that explains how to build a bomb using only chemicals available in regular supermarkets. Although information like this was available even before the Internet was developed, it was however, much more difficult to get access to that information. Today, any Internet user can get access to those instructions. Criminals can also use search engines to analyse targets[61]. A training manual was found during investigations against members of a terrorist group highlighting how useful the Internet is for gathering information on possible targets.[62] Using search engines, offenders can collect publicly available information (e.g. construction plans from public buildings) that help in their preparations. It has been reported that insurgents attacking British troops in Afghanistan used satellite images from Google Earth.

---

[61] Thomas, Al Qaeda and the Internet: The Danger of 'Cyberplanning' Parameters 2003, page 112 et seq

[62] Brown/Carlyle/Salmerón/Wood, "Defending Critical Infrastructure", Interfaces, Vol. 36, No. 6, page 530