The Rapid Growth of Cybercrimes Affecting Information Systems in the Global: Is this a Myth or Reality in Tanzania?

Edephonce Ngemera Nfuka*, Camilius Sanga**, Maduhu Mshangi***‡

* Institute of Educational and Management Technologies, Open University of Tanzania, edephonce.nfuka@out.ac.tz

** Department of Informatics, Sokoine University of Agriculture, csanga@gmail.com

***ICT Department, National Examinations Council of Tanzania (NECTA), Tanzania, maduhumshangi@gmail.com

‡Corresponding Author; Address: Tel: +255 754 860 027, Fax: +255-22-2775966,

e-mail: maduhumshangi@gmail.com

Abstract - The main objective of this study was to determine whether the rapid growth of cybercrimes affecting information systems in the global: is a myth or reality in Tanzania. The study was undertaken using a mixed research methods. The research findings reveal that 12.8 % of users are victims of cybercrimes due to visiting unhealthy websites in cyberspace, more than 90.89% of users have been denied access to torrents/p2p applications (with malicious codes); and more than 63.29% of e-mails received by users are spam. It has been noted that Internet users has risen to 5.63 million users in 2012 out of 46.9 million of population in Tanzania; and is increasing at the rate of 416.98% per year thus expectation of 7.34 million users of Internet by December 2015. The increase in the number of Internet users has direct implication to the increase in cybercrimes affecting information systems. The Government of Tanzania has declared that "about 320 people were apprehended between July and December 2011of which over 1bn/- , Euro 8,897 and USD 551,777 reported to have been stolen through cyber". The study concluded that there is a need for a holistic approach in addressing cybercrimes in a developing country like Tanzania.

Key words-. Cybercrime; information systems; cyberspace; cyber security.

1. Introduction

Information system (IS) is an integrated set of components for collecting, storing, and processing data; for delivering information, knowledge, and digital products. IS is not simply about computers, it's about how businesses can make the best use of computer technology to provide the information needed to achieve their goals. Governments deploy ISs to provide services cost-effectively to citizens. ISs generally are classified into five categories: office information systems, transaction processing systems, management information systems, decision support systems, and expert systems [2]. The main components of ISs are computer hardware and software, telecommunications, databases, human resources, and procedures [16], [48]. ISs in cyberspace include all information infrastructures accessible via the Internet, in and beyond territorial boundaries [10], [34].

With this trend of many people depending on ISs in the cyberspace, security issues have moved to the forefront of concerns about global well-being [38]. One of the major problems facing ISs in cyberspace is cybercrime [4]. Cybercrime is a generic term that refers to all criminal activities done using the medium of computers, the Internet, cyberspace and the worldwide web. Although there isn't really a fixed definition for cybercrime [40] but cybercrime encompasses any criminal act dealing with computers and networks (sometimes called hacking). Additionally, cybercrime also includes traditional crimes conducted through the Internet [37], [47]. These include attacks against computer data and systems, identity theft, the distribution of child sexual abuse images, internet auction fraud, the penetration of online financial services, as well as the deployment of viruses, Botnets, and various email scams such as phishing, hoax and spam / junk emails [33], [39]. The unique legal challenge for prosecuting information security offenses deals with jurisdictional issues. For example, an attacker in one country could launch an attack from a computer in another country that targets a computer in another country [41], [52], [56], [68]. Issues of jurisdiction and sovereignty have quickly come to the fore in the era of the Internet. The Internet does not tend to make geographical and jurisdictional boundaries clear, but Internet users remain in physical jurisdictions and are subject to laws independent of their presence on the Internet [40].

1.1. Problem Statement

Fighting against cybercrimes in Tanzania is debatable due to the absence of robust legal regime on cybercrime [13]. The rapid growth of use of Internet based ISs; mobile money industry related value-added service (VAS) such as M-Pesa, Tigo-pesa, and Airtel-Money; lack of cybercrime reporting culture and lack of effective security controls for different ISs endangers Internet users [5], [60]. However many of the cybercrimes happening in Tanzania are not reported [66] but still cybercrimes pose a significant threat to Internet users. Developing countries like Tanzania are uncertain of whether the rapid growth of cybercrimes affecting ISs in the global: is a myth or real?

1.2. Objective of the Study

The general objective of this study was to determine whether the rapid growth of cybercrimes affecting ISs in the global is a myth or reality in Tanzania. In order to address the research problem, the study explores the rapid growth of cybercrimes in the world, in general, and statistical evidence of occurrence of cybercrimes in Tanzania. This paper presents study on the rapid growth of cybercrimes: history and categories of cybercrimes, cybercrime situation in the world and Tanzania in specific; and finally presents the results and discussion, conclusion and recommendations of the best approach to deal with cybercrimes affecting ISs.

2. The Rapid Growth of Cybercrimes

2.1. History of Cybercrime

It is believed that the first recorded cybercrime took place in the year 1820 [39], [40]. This can be true with the fact that, computer did exist since 3500 BC in India, China and Japan though the modern computer began with the analytical engine of Charles Babbage by 1937 [39], [40]. Although the first known virus for a personal computer has been traced to 1980 but the world really did not take notice until the Melissa virus began to infect millions of computers in late March 1999 in which the New Jersey State Police and the Federal Bureau of Investigation (FBI) implicated the perpetrator [23] .

In the earliest times that information security was applied to business computer systems (approximately in 1970s); the focus was on the prevention of fraud [23], [49]. Conventional computer security includes confidentiality, integrity, availability, and theft. For example, protections are required equally to deal with sensitive information

leaks (confidentiality), worms affecting the operation of some critical application (integrity), botnets knocking out an important system (availability), or citizens having their identities compromised (theft). Certainly, the availability threat to national services must be viewed as particularly important, given the nature of the threat and its relation to national assets. One should thus expect particular attention to availability threats to national backbone infrastructure [21].

In Tanzania, the National backbone infrastructure for various ISs is now becoming optic fibre. Optic fibre is mainly used after the landing of submarine cables (EASSy, and SEACOM) and development of the national optic fibre (NICTBB) [42], [45], [54]. The landing of these submarine cables and developed national optic fibre in Tanzania; and similar developments in other countries have complicated how countries need to secure their assets. More cybercrimes have been reported in different countries due to rapid expansion of their Internet infrastructure and web-based ISs. The rapid growth of cybercrime has led to increased challenges in ensuring security of ISs [29], [44], [67].

2.2. Categories of Cybercrime

In this study, the term cybercrime includes cyber war, cyber espionage, cyber hacktivism, and cyber terrorism. Cyber espionage is the act or practice of spying or of using spies to obtain secret information, as about another government or a business competitor; the systematic use of spies to obtain secret information, especially by Governments to discover military or political secrets [17], [23]. The cybercrime can generally be grouped into four categories as follows:

i. Cybercrime against individuals: harassment via e-mails, cyber-stalking, dissemination of obscene material, defamation, unauthorized control/access over computer system (hacking), indecent exposure, email spoofing, spamming, cheating & fraud [15], [31], [40], [56].
ii. Cybercrime against individual property: credit card fraud, computer vandalism, transmitting malicious code (virus/worm/Trojans), unauthorized control/access over computer system (hacking), intellectual property crimes (software piracy: illegal copying of programs, distribution of copies of software, copyright infringement: trademarks violations, theft of computer source code), and internet time thefts [15], [31], [40], [56].
iii. Cybercrime against organization: denial of service, email bombing, salami attack, logic bomb, Trojans horse, data diddling, unauthorized control/access over computer system, possession of unauthorized information, distribution of pirated software and cyber terrorism against the government, organization etc. [15], [31], [40], [56].
iv. Cybercrime against society at large: pornography (basically child pornography), polluting the youth through indecent exposure, trafficking, financial crimes, sale of illegal articles, online gambling, forgery and web jacking [15], [31], [40], [56].

2.3. Cybercrime Situation in the World

Technology has connected nations; and the world has become a global village. Many socio-economic activities in most nations in the world today are aided by electronic systems via the Internet. Since this Internet is open- to all; it also includes eavesdroppers and criminals. False pretense, finds a fertile ground in this situation [46]. With recent developments in technology, cyber-attacks are increasing their sophistication; hence it is almost next to impossible to trace the attacks to its source [55]. For example, the report published by the Washington Post and Reuters, which came a few days after websites for both Bank of America and JPMorgan Chase experienced unexplained service disruptions; indicated that US officials suspected Iran to be behind similar denial-of-service attacks, which make them completely unavailable by

overwhelming them with garbage traffic in the cyberspace [26], [55].

The availability of cyberspace; the integrity, authenticity and confidentiality of data in cyberspace have become vital questions of the 21st century. Ensuring cyber security has turned into a central challenge for the state, business, organization and society; both at national and international level [18], [55]. Cybercriminals are often external to the victim, but according to the Ponemon Institute, one of the three most costly attacks is associated with malicious insiders [57]. A typical insider cybercrime would be an employee stealing funds via automated clearinghouse (ACH); electronic funds transfer (EFT) or wire transfer. Ultimately, organizations must protect themselves from external and internal threats, and risk [57].

Complaints related to spam e-mails purportedly sent from the FBI continued to be reported with high frequency to the Internet Crime Complaint Center (IC3) (http://www.ic3.gov/default.aspx). In 2012, the IC3 received about 47 complaints per day of this type. With an average adjusted loss of approximately $141 per complaint, victims reported losing more than $6,604 to this scam every day. More than 600,000 FaceBook accounts are compromised every day; 15% of social network users have reported that their profiles have been hacked by pretenders; 1 in 10 social network users said they'd fallen victim to a scam or fake link on social network platforms. Cybercrimes are growing; and by 2017 the global Cyber Security market is expected to skyrocket to $120.1 billion. The estimated annual cost over global cybercrime is 100 billion [25]. The US administration has made a habit of prosecuting Government leakers under the Espionage Act, the 1917 statute used to lock away or execute Soviet-era spies whose work sometimes resulted in the deaths of U.S. informants. The two most famous cases involve Army PFC. Bradley E. Manning, who admittedly turned over some 700,000 pages of documents to the anti-secrecy group WikiLeaks; and former National Security Agency (NSA) contractor Edward Snowden, whose leaks of NSA surveillance programs have roiled the national security and civil liberties communities [1], [27].

2.4. Cybercrime in Tanzania

Globalization and the pervasiveness of the Internet have given rise to new types of needs, rights and vulnerabilities to not only developed countries but also to developing countries like Tanzania. For secure electronic transactions to occur, an environment of trust must be created and sustained through the legal and regulatory apparatus. Cybercriminals around the world are constantly seeking loopholes through which to perform illegal or illicit businesses. Any country that has inadequate cyber-law is essentially offering a safe-haven for cyber-criminals to act with impunity [59]. Cybercrime is a vivid challenge for Information and Communication Technology (ICT) industry in Tanzania. This is from the fact that Information and Communication Technologies (ICTs) especially mobile phones and associated e-services have become pervasive across the country. Statistics report depicts that Tanzania has more than 26,965,476 mobile phone subscribers (Table 1, Table 2). Like many other countries around the globe; Tanzania has embraced ICT as a key enabler for educational, social and economic development in the country. Increasingly, ICTs and ISs in specific are becoming pervasive in all hosts of the daily activities in Tanzania [69]. However, the country faces challenges of cybercrimes.

The trends of ISs being in cyber-space such as Internet and cloud computing has created challenges in maintaining security of information. Cybercrime in Tanzania is increasing; the country has been experiencing massive cyber-attacks on their websites/ISs since January 2010 up to June 2013. Some of websites being hacked over this period are National Bureau of Statistics (NBS), Tanzania Commission for Universities (TCU) and National Council for Technical Education (NACTE), Open University of Tanzania (OUT), Chemi and Cotex

Industries Ltd, and Tanzania Olympic website [61], [62].

Cyber security incidents include theft of intellectual property and Government data, hacktivism, denial-of-service attacks, search engine optimization (SEO) poisoning, social engineering, advanced persistent threat, spear phishing attacks, malware targeting mobile devices and a resurgence of the Zeus Trojan, which targets financial information [50]. Protecting against these attacks is a key challenge for organizations of all sizes for both public and private sectors [8]. Kalunde highlighted that the cybercrimes Tanzania experiencing are computer fraud, hacking, IP crimes, ATM Fraud, denial of service; victims being the government agencies, banks, private business, universities and public in general [32].

Protecting the confidentiality of information manipulated by computing systems is a long-standing yet increasingly important problem [51]. There is lack of confidentiality and integrity in ISs; existing theoretical frameworks for expressing these security properties are inadequate, and practical techniques for enforcing these properties are unsatisfactory. Townsend [9] noted that "from training and operational trips to Uganda and Tanzania, has seen that the threat is widespread, tending to move with the growth of the Internet. It is good to see that governments and corporations are aware of and asking for awareness training, workshops and certification, and are setting up first responder teams" [9].

Policy and law to define and provide a framework for operation and enforcement of legally-accepted cyber activities in Tanzania is the work in progress. This comes after the country has, as all others, experienced increasing cyber-criminal activities. The IT Security experts warn that it is high time for the country to acclimatize the technology era and that includes creating legal frameworks to govern its use.

"While cybercrimes and other related on-line activities in Tanzania pose a significant threat, existing Tanzanian laws do not recognize many cyber space crimes" [63].

Over 500 Tanzanians have been apprehended by the Cybercrime Unit between 2011 and 2012 over cybercrime [11]. The Government reports that after strengthening the Cybercrime Unit in the country, the war against cybercrimes has started to yield fruits. About 320 people were apprehended between July and December 2011. According to Government report in year, 2012, they have arrested 230 over the crime. The Government report also indicate that there were over 1bn/-, Euro 8,897 and USD 551,777 reported to have been stolen through cyber, thus posing a challenge to the Government that if efforts are not made to check the trend, it would shoot up [14].

Many of developing countries including Tanzania have no cybercrimes laws [39]. Currently, Tanzania is in the process to enact cybercrimes laws; as the existing e- laws are not sufficient in convicting culprits because of jurisdiction anomalies especially when the investigation transcends international borders. Also obtaining evidence of computer crime that would stand in courts of law is lacking in many such countries since the field of computer forensics is still relatively new and lacks sufficient literature and expertise. Cybercrimes in many of developing countries like Tanzania are not reported, mainly due to the lack of cybercrimes laws, afraid of losing customers and awareness to citizens. Every country should have cybercrimes laws for prosecuting cyber-criminal(s). There should be awareness training for cybercrimes to citizens; and establishing forensic commission/bureau for investigations/collections of cybercrimes evidences [46], [64], [65]. For this to happen, collaborative effort is needed by different ministries (e.g. Ministry of Defence, Ministry of Education and Vocational Training, Ministry of Communication, Science and Technology, Ministry of Home Affairs, Ministry of Foreign Affairs etc.). For this to happen,

collaborative effort is needed by different ministries (e.g. Ministry of Home Affairs, Ministry of Defence, Ministry of Education and Vocational Training, Ministry of Communication, Science and Technology, Ministry of Foreign Affairs etc.).

Table 1. SIMCARD registration: registered as at September 2013

	Vodacom	AirTel	Tigo	ZanTel	TTCL	Benson	Total
Total Mobile Subscriptions	10,023,206	8,772,285	6,217,214	1,798,379	153,864	528	26,965,476
Registered Subscriptions	9,874,481	7,736,993	6,202,910	1,649,670	153,864	528	25,618,446
% Registered	99%	88%	99.8%	92%	100%	100%	95%

Source: [60].

Table 2. Summary of trend of telecom statistics: subscriptions & teledensity

	2005	2006	2007	2008	2009	2010	2011	2012
Fixed	154,420	151,644	163,269	123,809	172,922	174,511	161,063	176,367
Mobile	2,963,737	5,614,922	8,322,857	13,006,793	17,469,486	20,983,853	25,666,455	27,450,789
Total	**3,118,157**	**5,766,566**	**8,486,126**	**13,130,602**	**17,642,408**	**21,158,364**	**25,827,518**	**27,627,156**
Penetration	10%	15%	21%	32%	43%	50%	59%	61%

Source: [60].

3. Materials and Methods

This study employed mixed research (quantitative and qualitative) methods which enabled triangulations to take place. Triangulation refers to the use of different data collection methods within one study in order to ensure that the data are telling you what you think they are telling you. Each method, tool or technique has its unique strengths and weaknesses [58], [30]. By using multi-methods, the weakness of one method was complemented by strength of the other methods [53]. The researchers specifically employed participant observation, semi structured interview and documentary analysis method. Participant observation emphasis is on the discoveries of the meanings that people attach to their actions. Participant observation is where *"the researcher attempts to participate fully in the lives and activities of subjects and thus becomes a member of their group, organization or community. This method enabled the researcher to share the experiences by not merely observing what is happening but also feeling it"* [53].

Another method employed in this study was the semi structured interview to Systems/Network administrators and Systems Security specialists of the selected organizations as case study. The merits of the interview method were: more information and that greater depth of information was obtained; interviewers by their own skills were able to overcome the resistance of the respondents, the interviewers were able to collect supplementary information about the respondent's personal characteristics and environment which were often of great value in interpreting results [35].

Another method employed for data collection was the documentary analysis; this is a way of collecting data by reviewing existing documents. The documents may be internal or external to a program or organization, may be hardcopy or electronic, and may include reports, program logs, performance ratings, funding proposals, meeting minutes, newsletters, and marketing materials [6], [7]. In this study, logs of Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS) and firewalls systems (FS) were analysed. For the purpose of this study, the data were collected from five organizations in education sector which are institutions/agencies under the Ministry of Education and Vocational Training in

Tanzania (Table 3), the ministry itself; and Internet crime data collected by FBI for the year 2012. Information collected from various participants was treated as confidential and their use is only for academic purpose. In this study, the names of the five selected organizations have not been disclosed; there was no reason for mentioning the names of the studied organizations [3], the interest was to explore whether the rapid growth of cybercrimes affecting information systems in the global is a myth or reality in Tanzania. The selected organizations under this study are referred as X, Y, Z, U and V throughout the discussion. In this case, the level of analysis is organizational and their explanations are given in Table 3; the analysis of the data was performed using statistical methods and presented in tables, pie-charts and histograms.

Table 3: Organizations selected for the case study

Organization	**Explanations**
Organization X	The main functions of organization X are to ensure responsibility for examinations within Tanzania and to make provision for places and centers for examinations; to receive from other persons or bodies of persons reports or other material affecting examinations policy and from time to time to consider and review examinations policy as circumstances may require; to co-operate with other persons or bodies of persons in the orderly development of an examinations system in Tanzania; to conduct examinations for, and to grant, diplomas, certificates and other awards of the council; to act as the body which facilitate, administer and supervise foreign examinations in Tanzania.
Organization Y	Organization Y is charged with the responsibility of ensuring the quality of education in Tanzania at the pre-school, primary, secondary and teacher training levels. It is responsible for designing, developing, testing, reviewing and/or revising curricula at pre-primary, primary, secondary, special education and teacher training levels.
Organization Z	Organization Z is mandated for formulation, monitoring and evaluation of the implementation policies, teachers' training, registration of schools, inspection of education services and infrastructure, library services and education press services.
Organisation U	Organisation U is responsible for establishing the regulatory framework for technical education and training, leading to quality assured qualifications; assisting technical institutions to improve and maintain the quality of the education they provide and to ensure that their programmes meet labor market demand, by guiding and monitoring their adherence to the regulatory framework; and advising both Government and technical institutions on the strategic development of technical education and training.
Organization V	Organization V is mandated to recognize, approve, register and accredit Universities operating in Tanzania, and local or foreign University level programs being offered by registered higher education institutions. It also coordinates the proper functioning of all university institutions in Tanzania so as to foster a harmonized higher education system in the country. In order to ensure that such a harmonious higher education system does not compromise institutional peculiarities and autonomy, each University has the legal right to operate under its own charter.

Source: [43].

4. Results and Discussion

The followings are the results and discussions regarding the findings from this study. The analysis of data and discussions start with analysis of users surfing pattern, malicious codes (viruses, worms, Trojans) identified, denied application access for security reasons and finally, presents the analysis of frequently reported Internet crimes in accordance with FBI report of 2012.

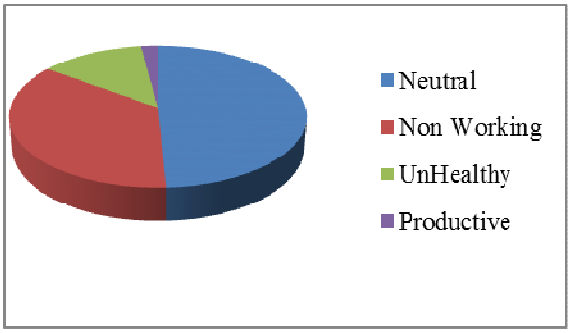
4.1. User Surfing Pattern

The user surfing behaviour was studied and analysed for education sector ISs in Tanzania. The users surfing patterns were grouped into four categories as indicated in Table 4 and Fig.1. The study portrays that 12.86% of users visited unhealthy sites; these are sites with malicious code used by cybercriminals to attack various ISs. This shows that ISs in Tanzania are subject to cyber-attacks due to surfing behaviour of internet users.

Table 4. Users surfing pattern

Category Type	Hits	Percent
Neutral	14,959,592	49.25%
Non-Working	10,896,686	35.87%
Unhealthy	3,906,681	12.8600%
Productive	613,609	2.02%

Source: [43]



Source: [43]
Fig. 1. Users surfing pattern

4.2. Top Viruses/Worms/Trojans Identified

Table 5 portrays the results of analysis of logs for IDS, IPS and FS in the Local area Network (LAN) or Wide Area Network (WAN) in education sector in Tanzania. The results reveal that cybercriminals are constantly releasing various malicious codes into cyberspace; Tanzania is not in isolation, it is one of the targets. Some of malicious codes identified as trying to penetrate various networks in education sector in Tanzania are: TR/Dropper.Gen, TR/Crypt.XPACK.Gen3, and TR/Crypt.ZPACK.16616. This implies that education sector is at high risk of experiencing cyber-attacks due to malicious codes. It also implies that the ISs in developing country like Tanzania are targeted by various cyber-attacks in cyberspace.

Table 5. Top Viruses/Worms/Trojans identified

S/N	Virus Name	Count
1	HTML/Infected.WebPage.Gen	321
2	TR/Dropper.Gen	92
3	TR/Crypt.XPACK.Gen3	55
4	TR/Injector.128000.6	47
5	TR/Crypt.ZPACK.16616	32
6	TR/Crypt.XPACK.Gen	26
7	TR/Rogue.1429034	25
8	TR/Injector.126464.2	21
9	HTML/Redirector.EU	14
10	TR/Yarwi.B.19	13
11	TR/Crypt.ZPACK.Gen	12

Source: [43]

4.3. Denied Applications for Security Reasons

Table 6 portrays the results of analysis of logs for IPS, IDS and FS for users who accessed various applications in education sector in Tanzania. The results reveal that more than 90.89% of users were denied access for visiting torrent /peer-to-peer (P2P) sites that contain malicious code. This implies that education sector is at high risk of experiencing cyber-attacks due to Internet surfing of users to applications which contains malicious codes.

Table 6. Denied applications access for security reasons

S/N	Application/Proto: Port	Hits	Percent
1	Torrent Clients P2P	2,587,340	82.33%
2	Shareaza P2P	268,887	8.56%
3	TCP:96	176,414	5.61%
4	UDP:53	61,928	1.97%
5	TCP:9100	26,708	0.85%
6	TOR Proxy	6,047	0.19%
7	TCP:441	5,176	0.16%
8	Ultrasurf Proxy	2,106	0.07%

Source: [43]

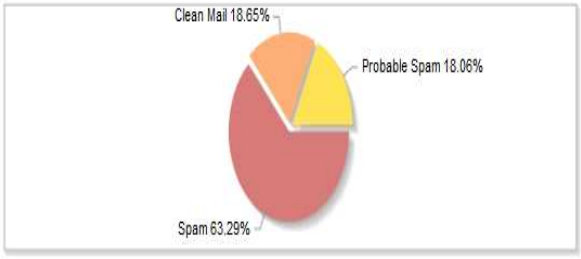
4.4. Mail Traffic Pattern

Table 7 and Fig.2 depict the results of analysis of electronic mail (e-mail) logs in education sector in Tanzania. The results reveal that more than 63.29% of e-mails sent/received are spam. This implies that education sector is at high risk of experiencing cyber-attacks due to spam emails. Spam is unsolicited email sent in massive quantities simultaneously to numerous users, generally trying to advertise or publicize certain products or services. The junk e-mails are also often used as a bridgehead for other types of cyber-crime, such as phishing or e-mail scams. This implies that the ISs in a developing country like Tanzania are target to various cyber-attacks in cyberspace.

Table 7. Mail traffic pattern

Traffic	Hits	Percent
Spam	319	63.29 %
Clean Mail	94	18.65 %
Probable Spam	91	18.06 %

Source: [43]



Source: [43]
Fig. 2. Mail traffic pattern

4.5. Internet Usage Statistics

Table 8 depicts that trends of Internet usage in Tanzania in 2012 has risen to 5.63 million users out of 46,912,768 populations of 2012 [28]; with increase rate of about 416.98 % per year. The trend reveals that by December 2015 the users accessing Internet in Tanzania will rise to 7.34 million users. This implies that more than 7.34 million users in Tanzania will be potential target of cyber-attacks by end of 2015. Table 9 portrays that trends of Internet usage across the global is increasing at a rate of more than 566.40%; approximately more than 2.4 billion out of 7 billion of the world population are accessing Internet. The high rate increase in Internet usage is directly related to the increase in the impact of cybercrimes across the global. This implies that a collaborative approach in fighting against cybercrime is required from various organizations, national wise and in the global.

Table 8. Internet Users, Population and Facebook Statistics for Africa

S/N	AFRICA	Population (2012 Est.)	Internet Users Dec-00	Internet Users 30-Jun-12	Penetration (% Population)	Internet % Africa	Facebook 31-Dec-12
1	Algeria	37,367,226	50,000	**5,230,000**	14.00%	3.10%	4,111,320
52	Tanzania	46,912,768	115,000	**5,629,532**	12.00%	3.40%	705,460
55	Uganda	33,640,833	40,000	**4,376,672**	13.00%	2.60%	562,240
58	Zimbabwe	12,619,600	50,000	**1,981,277**	15.70%	1.20%	n/a
	TOTAL AFRICA	**1,073,380,925**	**4,514,400**	**167,335,676**	**15.60%**	**100.00%**	**51,612,460**

Source:[28]

Table 9. World Internet Usage and Population Statistics

World Regions	Population (2012 Est.)	Internet Users Dec. 31, 2000	Internet Users Latest Data	Penetration (% Population)	Growth 2000-2012	Users % of Table
Africa	1,073,380,925	4,514,400	**167,335,676**	15.60%	3606.70%	7.00%
Asia	3,922,066,987	114,304,000	**1,076,681,059**	27.50%	841.90%	44.80%
Europe	820,918,446	105,096,093	**518,512,109**	63.20%	393.40%	21.50%
Middle East	223,608,203	3,284,800	**90,000,455**	40.20%	2639.90%	3.70%
North America	348,280,154	108,096,800	**273,785,413**	78.60%	153.30%	11.40%
Latin America / Caribbean	593,688,638	18,068,919	**254,915,745**	42.90%	1310.80%	10.60%
Oceania / Australia	35,903,569	7,620,480	**24,287,919**	67.60%	218.70%	1.00%
WORLD TOTAL	**7,017,846,922**	**360,985,492**	**2,405,518,376**	**34.30%**	**566.40%**	**100.00%**

Source: [28]

4.6. Analysis of FBI 2012 Internet Crimes Reported

In 2012, the IC3 received 289,874 consumer complaints with an adjusted dollar loss of $525,441,110, which is an 8.3-percent increase in reported losses since 2011 [19]. In recognition of this increase, the IC3 expanded its efforts to inform the general public about online scams by publishing several public service announcements and providing additional tips for Internet consumers. Table 10 portrays the top fifty countries which are internet crime victim complaints, among of them are: United States: 91.19070%, Canada: 1.4306%, United Kingdom: 0.8766%, Australia: 0.6796% and India: 0.5871%. For Africa in this list, countries listed are South Africa, Egypt and Nigeria. In this statistics Tanzania is not mentioned, this is simply because Internet crimes are not reported; there is no cyber law for prosecuting cybercrime and some people/organization fear to report because they fear for financial loss due to reputation loss to the public.

Table 10. Complaint statistics by country

Rank	State	Percent	Rank	State	Percent
1	United States	91.19%	26	Portugal	0.08%
2	Canada	1.43%	27	Argentina	0.07%
3	United Kingdom	0.88%	28	Greece	0.07%
4	Australia	0.68%	29	Indonesia	0.07%
5	India	0.59%	30	Afghanistan	0.06%
6	Macedonia	0.37%	31	United Arab Emirates	0.06%
7	Puerto Rico	0.21%	32	Colombia	0.06%
8	Brazil	0.19%	33	Saudi Arabia	0.06%
9	Mexico	0.19%	34	Ireland	0.06%
10	France	0.19%	35	China	0.06%
11	South Africa	0.18%	36	Romania	0.06%
12	Philippines	0.16%	37	Japan	0.06%
13	Germany	0.15%	38	Hong Kong	0.06%
14	Netherlands	0.14%	39	Poland	0.06%
15	Belgium	0.12%	40	Switzerland	0.05%
16	Spain	0.12%	41	Turkey	0.05%
17	Russian Federation	0.12%	42	Thailand	0.05%
18	Italy	0.11%	43	Norway	0.05%
19	Israel	0.10%	44	Ukraine	0.04%
20	New Zealand	0.10%	45	Denmark	0.04%
21	Pakistan	0.10%	46	Egypt	0.04%
22	Malaysia	0.08%	47	Republic of Korea	0.04%
23	Singapore	0.08%	48	Bulgaria	0.03%
24	Sweden	0.08%	49	Hungary	0.03%
25	Nigeria	0.08%	50	Chile	0.03%

Source: [19]

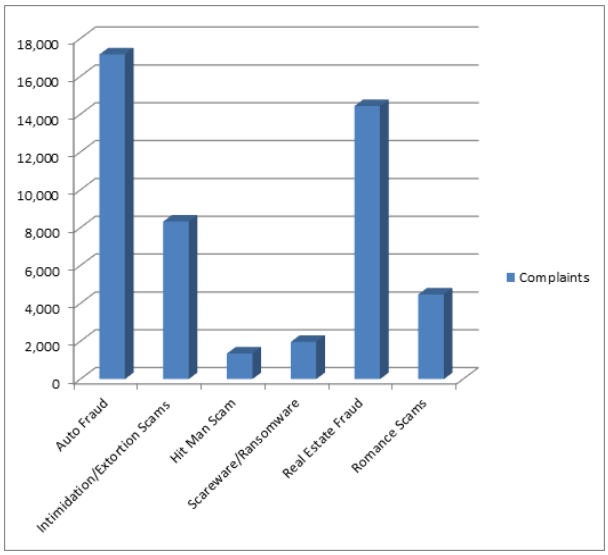
4.7. Frequently Reported Internet Crimes

Table 11 gives the statistics of frequently reported crimes; Fig.3 presents the histogram of complaints reported and Fig. 4 presents the histogram of the losses caused by internet crimes. It is observed that the internet crimes complaints due to "auto fraud (17,159)" are the highest, followed by "Real Estate Fraud (14,432)" (Fig.3). On the other side, the losses caused by internet crime are highest for "auto fraud ($64,572,334.97)", followed by "Romance Scams ($55,991,601.08)" (Fig.4). And the descriptions of the frequently reported Internet crimes are given in Table 12.

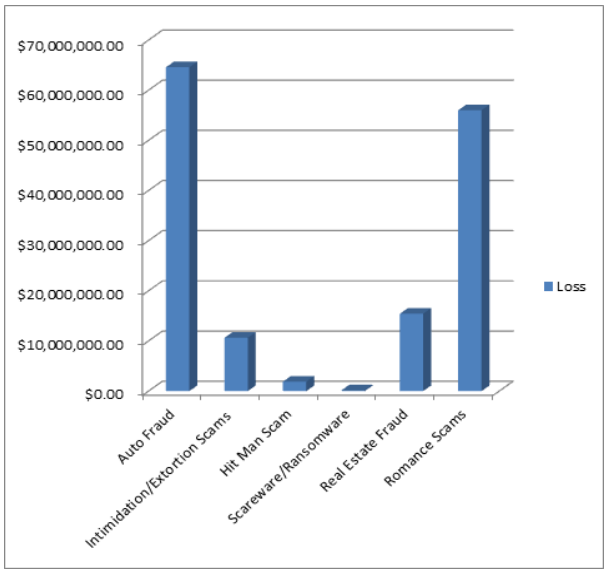
Table 11: Statistics of frequently reported crimes

Internet crime	Complaints	Loss
Auto Fraud	17,159	$64,572,334.97
Intimidation/Extortion Scams	8,324	$10,624,427.14
Hit Man Scam	1,354	$1,884,002.11
Scareware/Ransomware	1,969	$134,899.85
Real Estate Fraud	14,432	$15,418,734.82
Romance Scams	4,476	$55,991,601.08

Source: [19]



Source: [19]
Fig. 3. Complaints of Internet crimes reported



Source: [19]
Fig. 4. Loss caused by Internet crimes

Table 12. Internet crimes reported descriptions

S/N	Internet crimes	Description
1	Auto Fraud	In fraudulent vehicle sales, criminals attempt to sell vehicles they do not own
2	Intimidation/Extortion Scams	Intimidation and extortion scams have evolved over the years to include Telephone Calls, Payday Loan, Process Server and the Grandparent Scam.
2.1	Telephone Calls	In a twist to the pop-up scare ware scheme, victims began. In a twist to the pop-up scare ware scheme, victims began receiving telephone calls from individuals allegedly claiming to be from legitimate well-known software companies.
2.2	Payday Loan	The payday loan scam involves victims receiving harassing telephone calls from individuals claiming they are delinquent in payments.
2.3	Process Server	Person purporting to be a process server for the court appeared at a victim's place of employment and at the home of another victim allegedly to serve papers for a court date.
2.4	The Grandparent Scam	The scam involves fraudsters calling elderly individuals claiming to be a grandson or granddaughter or other young relative in a legal or financial crisis.
3	Hit Man Scam	The scam originated as a person sending an e-mail portraying himself as a hit man hired to kill the victim. The e-mail instructed the recipient to pay an amount of money to ensure the hit man did not carry out the death contract.
4	Scareware/ Ransomware	Extorting money from consumers by intimidating them with false claims pretending to be the federal government watching their Internet use and other intimidation tactics have evolved over the years to include some of the below highlighted scams.
5	Real Estate Fraud	Rental Scams: Criminals search websites that list homes for sale and take information from legitimate ads and post it with their own e-mail addresses on Craigslist® (without Craigslist's consent or knowledge) under the housing rentals category. To sweeten the pot, the houses are almost always listed with below-market rental rates.
6	Romance Scams	Perpetrators use the promise of love and romance to entice and manipulate online victims. A perpetrator scouts the Internet for victims, often finding them in chat rooms, on dating sites and even within social media networks. These individuals seduce victims with small gifts, poetry, claims of common interest or the promise of constant companionship. This crime not only affects the victims financially, there are emotional and mental implications as well.

Source: [19]

5. Conclusion

The research findings from this study reveals that 12.8 % of users are victims of cybercrimes due to visiting unhealthy websites (sites with malicious codes) in cyberspace, many of users are victims of malicious codes (viruses, worms and Trojans); more than 90.89% of users were denied access to torrents/p2p applications (sites with malicious codes); more than 63.29% of e-mails are spam in education sector in Tanzania. The research also found that Internet users has risen to 5.63 million users in 2012 out of 46.9 million of population in Tanzania; and is increasing at the rate of 416.98% per year thus expectation of 7.34 million users of internet by 2015 in Tanzania. The statistics revealed that there are 2.4 billion users of Internet in world out of 7 billion world population. The increase in the number of Internet users has direct implication to the increase in cybercrimes affecting ISs in the global. This implies that enabling environment for growth of ISs in developing countries like Tanzania due to landing of submarine cables and rapid use of mobile phones has brought a negative effect on cybercrime. There is an exponentially increase of cybercrimes. Thus, the findings from this study support the previous researches which found cybercrimes are growing faster in developing countries compared to the rest of the world [20], [36], [65].

The Government of Tanzania has declared that *"about 320 people were apprehended between July and December 2011".* This also applied to the following year in which 230 were arrested over the crime; and there are over 1bn/- , Euro 8,897 and USD 551,777 reported to have been stolen through cyber, thus posing a challenge to the Government that if efforts won't be made to reduce this trend, it would shoot up. Currently, Tanzania is in

processes of enacting cybercrimes laws; as the existing e-laws are not sufficient in convicting culprits because of jurisdiction anomalies especially when the investigation transcends international borders. Also obtaining evidence of computer crime that would stand in courts of law is lacking in many developing countries like Tanzania since the field of computer forensics is still relatively in infancy stage and lacks sufficient literature and experts. The study revealed that the rapid growth of cybercrimes affecting ISs in the global is indeed a reality in Tanzania. It concluded that there is a need for holistic and collaborative approaches in addressing cybercrimes in a developing country like Tanzania. A holistic approach to cybercrime is paramount. Also collaborative approach consisting of integrated initiatives at inter-national (global), national, sub-national and local levels are needed [65]. Holistic and collaborative approaches must accommodate efforts from different experts from a wide range of disciplines.

6. Recommendations

The findings from this study have led the authors to recommend a holistic approach to deal with cybercrime. The proposed holistic and collaborative approaches comprise of three categories namely: legal, strategic and technical perspectives in predicting, preventing, identifying, and responding against cybercrimes.

A. Legal perspective

i. The Government of Tanzania should have cybercrime laws for dealing with cybercrime and there should be collaborations of different stakeholders (i.e. within organization, national wide and worldwide).
ii. There should be forensic bureau (competent in IT security) for investigations/collection of digital cybercrimes evidences.
iii. High penalties should be enforced for cybercrime committed and for those who do not report the incident of cybercrime.
iv. Training and awareness to citizens, organizations, the Government and public in general regarding the collection of digital forensics evidences; and how to report cybercrime.

B. Strategic perspective

i. The Government should revise the National ICT policy of 2003 to accommodate new ICT developments in the industry.
ii. The organizations/Government should have Internet usage and security policies in specific
iii. Standards and procedures should be enacted with regard to usage of information systems in cyberspace
iv. Use multi-factor authentications (something you know: personal identification number (PIN) or password; something you have: such as Auto Teller Machine (ATM) card or smart card; something you're: biometric characteristic such as a fingerprint) for accessing information systems.
v. Perform Information systems audits.
vi. Perform penetration test (ethical hacking) for information systems (simulating malicious attacks from an organization's internal and external users).
vii. Training and certifications in cyber security, information systems assurance, information systems security and other related risks management certifications or professional. The education system curricula should be reviewed to incorporate training in the field of information systems security and cyber security.
viii. Carry out researches in the field of cyber security, information systems security, and information systems assurance.

C. Technical perspective

i. Use of firewalls, IDS, IPS, updated antivirus and anti-spyware.
ii. Enforce a password policy. Complex passwords make it difficult to crack password files on compromised computers. This helps to prevent or limit damage when a computer is compromised.
iii. Ensure that programs and users of the computer use the lowest level of privileges necessary to complete a task. When prompted for a root or User Account Control (UAC) password, ensure that the program asking for administration-level access is a legitimate application.
iv. Disable AutoPlay to prevent the automatic launching of executable files on network and removable drives, and disconnect the drives when not required. If write access is not required, enable read-only mode if the option is available.
v. Turn off file sharing if not needed. If file sharing is required, use Access Control List and password protection to limit access. Disable anonymous access to shared folders. Grant access only to user accounts with strong passwords to folders that must be shared.
vi. Turn off and remove unnecessary services. By default, many operating systems install auxiliary services that are not critical. These services are avenues of attack. If they are removed, threats have less avenues of attack.
vii. If a threat exploits one or more network services, disable, or block access to, those services until a patch is applied.
viii. Always keep your patch levels up-to-date, especially on computers that host public services and are accessible through the firewall, such as Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), mail, and DNS Domain Name System (DNS) services.
ix. Configure your email server to block or remove email that contains file attachments that are commonly used to spread threats, such as .vbs, .bat, .exe, .pif and .scr files.
x. Isolate compromised computers quickly to prevent threats from spreading further. Perform a forensic analysis and restore the computers using trusted media.
xi. Train employees not to open attachments unless they are expecting them. Also, do not execute software that is downloaded from the Internet unless it has been scanned for viruses. Simply visiting a compromised Web site can cause infection if certain browser vulnerabilities are not patched.
xii. If Bluetooth is not required for mobile devices, it should be turned off. If you require its use, ensure that the device's visibility is set to "Hidden" so that it cannot be scanned by other Bluetooth devices.
xiii. If device pairing must be used, ensure that all devices are set to "Unauthorized", requiring authorization for each connection request. Do not accept applications that are unsigned or sent from unknown sources.
xiv. Encryption of data on transit, processing and storage.
xv. Maintain the disaster recovery room containing all important information management resources.

References

[1]. Africa-Review. Africa Review: http://www.africareview.com/News/WikiLeaks-spotlights-Tanzania-on-corruption/-/979180/1075764/-/iyjkcfz/-/index.html website on “WikiLeaks spotlights Tanzania on corruption” , Latest Access Time for the website is 05 March 2014.

[2]. M. Awais, T.Samin, and M.Bilal. "Effective Business Value of Bal Information System”. IJCSI International Journal of Computer Science, Vol.8, pp.366-370, 2011.

[3]. J. K. Bakari . A Holistic Approach for Managing ICT Security in Non-Commercial organisations A Case Study in a Developing Country. *PhD Thesis.* Stockholm, Sweeden: Stockholm University/ Royal Institute of Technology Department of Computer and Systems Science, 2007.

[4]. C. M. Blanc. "The evolving challenge of identity-related crime:addressing fraud and the criminal misuse and falsification of identity", ISPAC 2007, Itally, pp.284-290, 30 November − 2 December 2007.

[5]. G. Bougaardt and M. Kyobe. "Investigating the Factors Inhibiting SMEs From Recognizing and Measuring Losses From Cyber Crime in South Africa". *Electronic Journal Information Systems Evaluation*, Vol.14.No.2, pp.167-178, 2011.

[6]. G. A. Bowen. "Document Analysis as a Qualitative Research Method". *Qualitative Research Journal*, Vol.9.No.2, pp.27 – 40, 2009.

[7]. CDC.GOV. Data Collection Methods for Evaluation: Document Review. *Technical Report*. Department of Health and Human Services Centers for Disease Control and Prevention http://www.cdc.gov/healthyyouth/evaluation/pdf/brief18.pdf, 2009.

[8]. M.S. I. Center. "Monthly Security Tips NEWSLETTER: Cyber Security Emerging Trends and Threats", *Multi-State Information Sharing and Analysis Center*, Vol.7.No.1, pp.1-2, January 2012.

[9]. C. Cilli. "Global Perspectives". *ISACA Journal*, Vo.1.No.1, pp.1-2, 2006.

[10]. D.Clemente. Cyber Security and Global Interdependence: What Is Critical?. *Technical Report*. The Royal Institute http://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/0213pr_cyber.pdf, 2013.

[11]. Daily News. "Tanzania: 500 Held Over Cyber Crimes". *News Paper*. AllAfrica http://allafrica.com/stories/201206270137.html, 26 June, 2012.

[12]. Daily News. "Tanzania: Law on Cyber Crime in Offing". *News Paper*. AllAfrica: http://allafrica.com/stories/201207161123.html, 14 July, 2012.

[13]. Daily News. "Tanzania Government finalizing Cyber crime act". *News Paper*. PcTech Magazine http://pctechmag.com/2013/05/tanzania-government-finalizing-cyber-crime-act/, 10 May, 2013.

[14]. Daily News. "Tanzania: Cybercrime Law in the Pipeline". News Paper. AllAfrica http://allafrica.com/stories/201309110118.html, 11 September, 2013.

[15]. E.H. Dalla, and M. Geeta. "Cyber Crime A Threat to Persons, Property,Government and Societies". *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol.3. No.5, pp.997-1002, 2013.

[16]. Encyclopadia. Encyclopadia Britannica http://www.britannica.com/EBchecked/topic/287895/information-system website on "Information Systems" Latest Access Time for the website is 05 January 2014.

[17]. Encyclopedia. Encyclopedia: http://www.pcmag.com/encyclopedia/term/64376/cyber-espionage website on "cyber espionage ", Latest Access Time for the website is 05 January 2014.

[18]. ENISA. European Union Agency for Network and Information Security http://www.enisa.europa.eu/media/news-items/german-cyber-security-strategy-2011-1 website on "Cyber Security Strategy for Germany" , Latest Access Time for the website is 05 January 2014.

[19]. FBI. FBI-IC3 2012 Internet Crime Report Released. *Technical report*. Federal Bureau of Investigation (FBI) http://www.ic3.gov/media/annualreport/2012_ic3report.pdf , 2012.

[20]. F. S. Gady . Africa's Cyber http://www.foreignpolicy.com/articles/2010/03/24/africas_cyber_wmd?page=0 website on "Think that Russia and China pose the biggest hacking threats of our time? The virus-plagued computers in Africa could take the entire world economy offline", Latest Access Time for the website is 24 March 2014.

[21]. P. D. Gallagher. Managing Information Security Risk. *Technical report*. National Institute of Standards (NIST) and Technology. U.S.

Department of Cormmerce. http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf, March 2011.

[22]. M.Gercke. Understanding cybercrime: a guide for developing countries. *Technical report*. ICT Applications and Cybersecurity Division (CYB) Policies and Strategies Department Bureau for Telecommunication Development International Telecommunication Union, Geneva, Switzerland, March 2011.

[23]. S.Ghosh, and E. *Turrini. A Multidisciplinary Analysis*. Springer-Verlag Berlin Heidelberg, 2010.

[24]. S.Ghosh, and E.Turrini. *CyberCrimes: A Multidisciplinary Analysis*. Springer-Verlag Berlin Heidelberg, 2011.

[25]. GO-GULF.COM. www.go-gulf.ae/blog/cyber-crime website on "Cyber Crime Statistics and Trends [Infographic]", Latest Access Time for the website is 24 March 2014.

[26]. D.Goodin. http://arstechnica.com/security/2012/09/web-attacks-us-banks-originated-in-iran/ website on "Web attacks on big US banks originated in Iran", Latest Access Time for the website is 05 January 2014.

[27]. IBT. INTERNATIONAL BUSINESS TIMES http://www.ibtimes.com/manning-wikileaks-verdict-edward-snowden-manning-charged-under-espionage-act-1363799 website on "Manning WikiLeaks Verdict: Like Edward Snowden, Manning Charged Under The Espionage Act", Latest Access Time for the website is 31 January 2014.

[28]. INTERNETWORLDSTATS.COM. Internet Users, Population and Facebook Statistics for Africa. *Startics report.* Internet World Stats http://www.internetworldstats.com/stats1.htm#africa, 2012.

[29]. ITU. TRENDS IN TELECOMMUNICATION REFORM. *Technical report*. International Telecommunication Union place des Nations (ITU), CH-1211, Geneva, Switzerland http://www.itu.int/dms_pub/itu-d/opb/reg/D-REG-TTR.14-2013-SUM-PDF-E.pdf, 2013.

[30]. T. D. Jick. "Mixing Qualitative and Quantitative Methods: Triangulation in Action". *Administrative Science Quarterly*, Vol.24. No.4, pp.602-611, 1979.

[31]. Y. Joshi, and A. Singh. "A Study on Cyber Crime and Security Scenario in India". *International Journal of Engineering and Management Research*, Vol.3. No.3, pp.13-18, June 2013.

[32]. S. M. Kalunde. The status of Cybercrime in Tanzania :Strasbourg, France. *Technical report*. Council of Europe http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/Octopus2011/Update_session_Tanzania.pdf, 2011.

[33]. E. Kamanda. "Spetrum Times: Cyber Crime at Spectrum Network". *Quarterly Journal on risk Management*, Vol.1. No.1, pp.1-8, November 2013.

[34]. A.T. Kingsmith. "Virtual Roadblocks: The Securitisation of the Information Superhighway". *Bridges: Conversations in Global Politics and Public Policy*. Vol.2. No.1, pp.1-14, October 2013.

[35]. C. Kothari. *Research Methodology: Methods & Techniques* .2nd ed. New Delhi, New Age International (P) Limited, Publishers, 2004.

[36]. N. Kshetri. *Cybercrime and cybersecurity in the Global South.* Palgrave Macmillan, 2013.

[37]. M.Levi, and M.Williams. eCrime Reduction Partnership Mapping Study. *Technical report*.Cardiff for crime, Law and Justice Card School of Social Science, Cardiff University http://www.cardiff.ac.uk/socsi/resources/Levi%20Williams%20eCrime%20Reduction%20Partnership%20Mapping%20Study.pdf, 2012.

[38]. O.Longe, O.Ngwa, F.Wada, V.Mbarika, and L.Kvasny. "Criminal Uses of Information & Communication Technologies in Sub-Saharan Africa: Trends, Concerns and Perspectives". *Journal of Information Technology Impact*. Vol.9.No.3, pp.155-172, 2009.

[39]. B.Magalla. The New Era of Cyberspace: Their Protection, Prevention and Detection. Tumaini University Iringa University College https://www.academia.edu/5287646/THE_NEW_ERA_OF_CYBERSPACE_THEIR_PROTECTION_PREVENTION_AND_DETECTION, 2013.

[40]. P.Mali. *Cyber Crimes and Penalties*. Cy b e r L aw Co ns u l t i n g, 2008.

[41]. A. J. Mambi. *ICT Law Book: A Source Book For Information & Communication Technologies and Cyber Law*. Dar es Salaam: Mkuki na Nyota Publishers Ltd, 2010.

[42]. M.M.Behitsa, and B.D. Diyamett. Tanzania ICT Sector Performance Review:Towards Evidence-based ICT Policy and Regulation Volume Two , Policy Paper II. *Policy review report*. Tanzania Government Portal http://www.tanzania.go.tz/egov_uploads/documents/Vol_2_Paper_11_-_Tanzania_ICT_Sector_Performance_Review_2010_sw.pdf, 2010.

[43]. MoEVT. Ministry of Education and Vocational Training (MoEVT): http://www.moe.go.tz/ website on "Institutions and Agencies", Latest Access Time for the website is 26 April 2014.

[44]. MST.GO.TZ. Ministry of Communication, Science and Technology: http://www.mst.go.tz/index.php/login website on "Programmes/Projects:National Communications Infrastructure Backbone Network", Latest Access Time for the website is March 06, 2014.

[45]. NICTBB.CO.TZ. http://www.nictbb.co.tz/news.php website on "Status of the National ICT Broadband Backbone (NICTBB) and Prospects for Local Contents Development in Tanzania", Latest Access Time for the website is March 06, 2014.

[46]. R. E. Okonigene, and B. Adekanle. "Cybercrime in Nigeria". *Business Intelligence Journal*. Vol.3.No.1, pp.93-98, 2010.

[47]. V.Olena. "Problem of Cybercrime in Ukraine: Spread of, Specific Nature, and Methods of Fighting". *Internal Security*. Vol.4.No.1, pp.153-163, 2012.

[48]. J.Paul, V.Belle, M.Eccles, and J.Nash. Discovering Information Ssytems. Berne Conversion, 2003.

[49]. S. J. Ross, and R.Masters. "Creating a Culture of Security". *ISACA journal*, Vo.1.No.1, pp.1-140, 2011.

[50]. K.Rowley. "Cyber Security Emerging Trends and Threats". *Multi-State Information Sharing and Analysis Center*, Vo.7.No.1, pp.1-3, 2012.

[51]. A.Sabelfeld, and C.Myers. "Language-Based Information-Flow Security". *IEEE Journal on Selected Areas in Communications*, Vol.21.No.1, pp.1-15, January 2003.

[52]. C.Sanga. "Digital age dillemma: (DAD) are we secure?". *A Newsletter of Sokoine University of Agriculture*, SUACONE, ISBN 9987 640 02 8, pp.12-14, 2009.

[53]. M. N. Saunders, P.Lewis, A.Thornbill, and M.Jenkins. Research Methods for Business Students. England: Pearson Education Limited, 2003.

[54]. SEACOM. seacom.mu: http://seacom.mu/wp-content/uploads/SEACOM-IP-MPLS_12-November-2013.pdf website on "SEACOM IP and MPLS Services", Latest Access Time for the website is 19 March, 2014.

[55]. H. Çil, C. Z. Şentürk, and Ş.Sağıroğlu. "Cyber Security Analysis of Turkey", *International Journal of Information Security Science*, Vol.1.No.4, pp.112-125, 2012.

[56]. D. L. Shinder. *Scene of the Cybercrime: Computer Forensics Handbook*. Syngress Publishing, Inc, 2002.

[57]. T.Singleton. "Understanding the Cybercrime Wave". *ISACA JOURNAL*, Vol.1.No.1, pp.1-5, 2014.

[58]. H. W. Smith. *Strategies of Social Research*:The Methodological Imaglnation. Prentice-Hall, 1975.

[59]. TANZANIA ICT POLICY. TANZANIA ICT POLICY. Tanzania Governent Portal

http://www.tzonline.org/pdf/ictpolicy2003.pdf, 2003.

[60]. TCRA. Quarterly Telecom Statistics Quarter1. *Technical report.* The Tanzania Communications Regulatory Authority (TCRA) http://www.tcra.go.tz/images/documents/telecommunication/telecomStatsSept13.pdf, 2013.

[61]. Tech360Magazine. http://www.tech360magazine.com/2012/07/tanzania-lost-89218-billions-on.html website on "Tanzania lost 892.18 Billions on Cybercrimes last financial year ", Latest Access Time for the website is 27 October, 2013.

[62]. TechMtaa. http://www.techmtaa.com/2010/01/31/tanzanian-government-websites-suffer-from-massive-hacking-attacks/ website on "Tanzanian Government websites suffer from massive hacking attacks ", Latest Access Time for the website is 27 October, 2013.

[63]. THE GUARDIAN. IPPMEDIA: http://www.ippmedia.com/frontend/?l=57518 website on "Lack of laws hinder cyber crime probes", Latest Access Time for the website is 20 February, 2014.

[64]. F.Tushabe. Computer Forensics for Cyberspace Crimes. *Master Dissertation.* Master of Science in Computer Science of Makerere University, 2004.

[65]. F.Tushabe, and V.Baryamureeba. "Cyber Crime in Uganda: Myth or Reality?". *Proceedings of World Academy of Science, Engineering and Technology*, Vol.8, pp.66-70. October 2005.

[66]. UNCTAD. Mobile Maney for Business Development in the East African Community: A Comperative Study of Existing Pltaforms & Regulations. *Technical report*.United Nations, 2012.

[67]. USAID. Emerging Technology & Practice for Conservation Communication in Africa: A Report on the State of the Art and Trends with Recommendation For USAID. *Technical Report*. International Resources Group (IRG), 2012.

[68]. M.Watkins, and K. Wallace. *CCNA Security Official Exam Certification Guide*. (G. Johnson, Ed.) New Delhi, India: Pearson Education, Inc. and Dorling Kindersley Publishing, Inc., 2009.

[69]. J. J..Yonazi. "Cyber Security in Tanzania". The Cyber-Security Mini-Conference. Dar ES Salaam, 2012.