International Journal of Business, Human and Social Sciences
ISSN: 2517-9411
Vol:1, No:8, 2007

Cyber Crime in Uganda: Myth or Reality?

Florence Tushabe, and Venansius Baryamureeba

***Abstract*—**There is a general feeling that Internet crime is an advanced type of crime that has not yet infiltrated developing countries like Uganda. The carefree nature of the Internet in which anybody publishes anything at anytime poses a serious security threat for any nation. Unfortunately, there are no formal records about this type of crime for Uganda. Could this mean that it does not exist there? The author conducted an independent research to ascertain whether cyber crimes have affected people in Uganda and if so, to discover where they are reported. This paper highlights the findings.

***Keywords*—**Cyber crime, Internet crime, Uganda crime statistics.

I. Introduction

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 very popular with telecommunications companies configuring email and Internet services on almost all mobile phones. By 2004, the nationwide population of Internet users, according to the World Fact Book [1], 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. It has been defined by Joseph Migga Kizza [2] 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. 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. 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 [3].

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. Section II summarises the international climate regarding cyber crime, Section III discusses the data collection techniques that were employed in this research, Section IV presents the results obtained and Sections V and VI provide some recommendations and concluding remarks respectively.

II. Cyber Crime Internationally

Statistics from the InterGov organisation [4], an international organization committed to ensuring a safe cyberspace environment, show computer crimes are growing at a rate of approximately 92% annually. Furthermore, less than 10% of computer crimes are reported and of all the crimes that are reported, fewer than two percent get convicted. Table 1 shows records from the International Web Police Statistics [4] concerning the reported crimes annually since 1993.

Relatedly, a survey by the anti-virus software manufacturer, Sophos [5] in December 2004 showed that by the end of 2004, there were over 100,000 known viruses; recording a 51.8% increase in the number of new viruses. Interestingly, a German teenager called Sven Jaschan was responsible for more than 50% of all the virus incidents reported in 2004. Furthermore, the 2004 National White Collar Crime Center and Federal Bureau of Investigation report [6] showed how a total dollar loss from all referred cases of internet fraud in the United States alone rose to 68.14 million dollars.

In this era of organised crime and terrorism, the cyberspace is a meeting point for criminal groups like the Tigers-of-Tamil, Russian-Mob and the Mafia-Internet-Securities [7].

Cyber terrorism is one of the recognized cyber crimes. It has been defined as the premeditated use of disruptive activities, or the threat thereof, in cyber space, with the intention to further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance

Manuscript received September 23rd, 2005. This work was supported by the Faculty of Computing and Information Technology and the School of Post Graduate Studies Makerere University.

Florence Tushabe B is currently a PhD student from the University of Groningen and also within the Department of Computer Science, at Makerere University (e-mail: tushabe@cit.mak.ac.ug).

Venansuius Baryamureeba is the Dean of the Faculty of Computing and Information Technology. (e-mail: barya@cit.mak.ac.ug).

of such objectives [8]. Intelligence authorities characterized the first known attack by terrorists against a country's computer systems in Sri Lanka. In 1998, ethnic Tamil guerrillas swamped Sri Lankan embassies with 800 e-mails a day over a two-week period [8]. The messages read," We are the Internet Black Tigers and we are doing this to disrupt your communications". This caused great fear among the diplomats since the rebel group was notorious for killing people.

TABLE I
CRIMINAL AND CIVIL COMPLAINTS FILED [4]

Year	Complaints	Complaint / Day
2002	1,351,897	3,704
2001	701,939	1,923
2000	289,303	793
1999	94,291	258
1998	47,614	130
1997	12,775	35
1996	4,322	11
1995	1,494	4
1994	971	2
1993	640	1.7

Some countries responded to the threat of cyber crimes by modifying and enacting cyber laws. Boda Mash [3] examined the growth and development of the law related to cyber crime in the international community and divided them into nine categories: protection of privacy, protection of intellectual property, illegal and harmful contents, criminal procedural laws, computer related economic crime, unauthorized access, computer forgery, computer fraud and child pornography.

Apart from laws, some countries like China and Saudi Arabia have introduced technical measures like Internet filtering. In 2000, Saudi Arabia set up the Internet Service Unit [9] which was empowered to filter web traffic from ISPs before permitting users access to the contents. If the requested URL was on the 'black list' the user is directed to a page that informs him that access to the requested page has been denied. A survey by Jonathan Zittrain and Benjamin Edelman [10], which requested for 797 sexually explicit websites, recorded a 86.2 % blockage success.

III. Data Collection

Information from Internet users in Uganda was collected and analyzed using SPSS. The aim was to investigate if they had been perpetuators or victims of cyber crime and if so, where they reported the incidents. The instruments used during the study included a web-based survey, telephone interviews, e-mail statements, face-to-face interviews, case studies and questionnaires.

A. Questionnaires

A set of questionnaires was distributed to a sample of 1000 regular users in the districts of Kampala, Mukono and Mbarara. The questionnaire survey queried incidents like virus attacks, SPAM, Internet fraud, intellectual property infringement, hacking, identity theft, child pornography and child trafficking/ missing children.

Of the 1000 questionnaires that were distributed, 500 responded positively and were analyzed. The participants consisted of students, researchers, the business community, community workers, law enforcement officers and lecturers. The sample space consisted of the following institutions: Makerere University, Uganda Christian University Mukono, Uganda Management Institute, Mbarara University of Science and Technology, Ministry of Health, Busoga University (Kampala branch), Nkumba University, Straight Talk Foundation, Law Development Center, Fraud Uganda, Makerere Hill Internet cafe, Webcity Cafe, Makerere Police Post, Criminal Investigation Directorate (CID), media houses and others.

B. Interviews

Interviews with police officers were conducted in order to shed more light upon the non-existent cyber crime record. The interviews were conducted with Deputy Director of CID, Mr. Ochola Okoth; Crime Intelligence Officers, Mr. Asaba Charles and Mr. Mayende Wilbert; Government Analysts, Mr. Apollo Mutashwerwa and Mr. Olanya Joseph Okwong and the Assistant commissioner of Police (ACP), Mr. Abilu Martin.

C. Web-based Survey

A website was created that would provide an opportunity for a broader distribution of Ugandans to respond to the cybercrime questionnaires.

IV. Results

The study has confirmed that Internet users in Ugandan are both victims and perpetrators of Internet crime and all victims did not report to the police. The major cases involved inter-country situations including within Nigeria, Congo, Kenya and Canada.

A. Specific Cases

In January 2005 [11], a multi-million dollar scam involving a fraudulent intranet bank transfer between Standard Charted Bank, Nairobi and Barclays Bank, Kampala was unveiled. A prominent Ugandan businessman and construction magnet, Andrew Zzimwe Kasagga together with two Congolese nationals were wanted by Interpol (Kenya) over accusations of masterminding the bank fraud that saw Kenyan Standard Chartered Bank staff wiring to them $5 million in three installments to separate bank accounts and recipients 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. Further investigations and trial are being conducted.

Another $3 million being swindled from Kenya was detected before it was sent to forex bureaux via the DFCU bank in Kampala.

In July 2004, one lady, Grace Muwanguzi, lost her passport and 500 dollars (which she had borrowed) to a fake company claiming to arrange visas and free transport and

accommodation in Canada. They used an existing project by the Ministry of Health in which some officials were to travel to Toronto for a Trainer of Trainers (ToT) course in HIV/AIDS management. She thought it was a genuine deal when she saw a website on the Internet containing the details of the conference. On the day the passports (including the visas) were to arrive, the perpetrators of this scheme disappeared. Several others fell victim of this scam and similar ones.

One company confessed about an incident of email spoofing in which a 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 traced the bad email to an employee in a competitors company. The case was settled out of court

In July 2004, the newvision newspaper [12] broke a story about two pornographic sites, www.kimansulo.com and www.hotugandans.com hosted in Canada but selling thousands of pictures and videos of Ugandan women having sex. A follow-up story by a journalist from The Monitor newspaper [13] said, "*But most of the 'models' in the thousands of nude pictures on kimansulo.com are not actors and many did not know that their pictures were taken while having sex. They are neither models nor even prostitutes. They are ordinary office workers and university students who go for a party, get drunk and end up having a fling with someone they thought was a friend. Unknown to them, a concealed video camera is rolling away, recording the minutest details of their actions and facial expressions*". By the end of August 2005, they had closed their websites due to public outcry. No legal case suits have been reported yet.

B. Generalized Results

Over 90% reported to have been a victim of at least one cyber crime incident and twenty five percent confessed that they commit at least one wrongful act while in the cyberspace. The victims are mainly prey of SPAM, virus attacks and pornography, while the perpetrators are mostly SPAM senders, intellectual property infringers and hackers. Most Internet crimes are not reported at all because the country does not have a standing law for computer and internet crimes. The public are therefore not protected against these kinds of crimes and their consequences.

The details that emerged were:

1) Majority of cyber users in Uganda use the Internet for communication and research. E-mail was the leading activity (48%), followed by research (38%). Fig. 1 shows the details of what most cyber citizens in Uganda do while online.

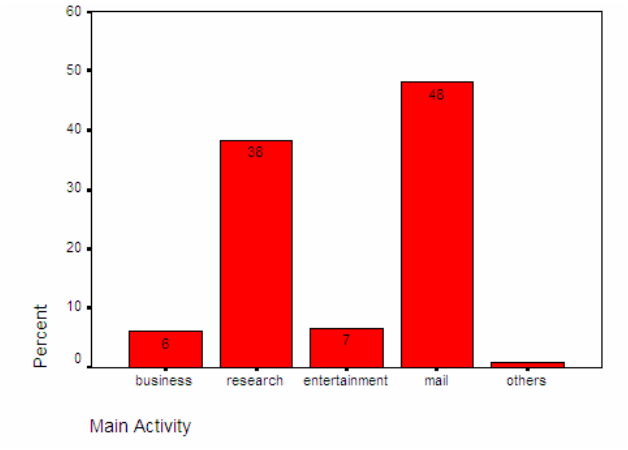

Fig. 1 Internet usage

2) Most Internet users have fallen victim of cyber crime with 92% of respondents having been victim of at least one cyber crime. SPAM and virus attacks are the leading incidents reported by victims. Fig. 2 shows more details.

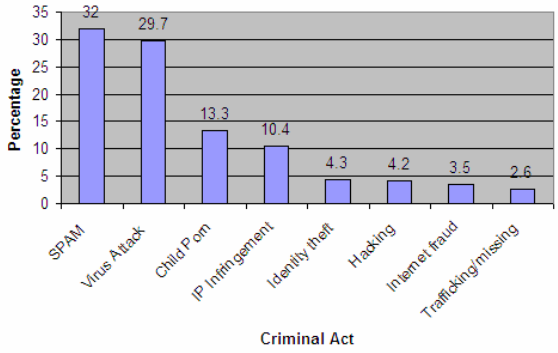

Fig. 2 Experienced cyber crimes

3) 53% of the victims had never told anybody, 34% reported incidences to the System Administrators while 13% told their friends. Most victims prefer to keep quiet because they do not think reporting would help them since preserving evidence is unknown to them. The ones who lost important data are the ones who reported to the system administrators in an attempt to recover it.

4) Internet users in Uganda perform and initiate some wrongful incidents. 25% reported at least one incident they have planned and successfully implemented. SPAM spreaders, intellectual property infringers and hackers are the most rampant. Figure 4 shows details concerning perpetrator trends.

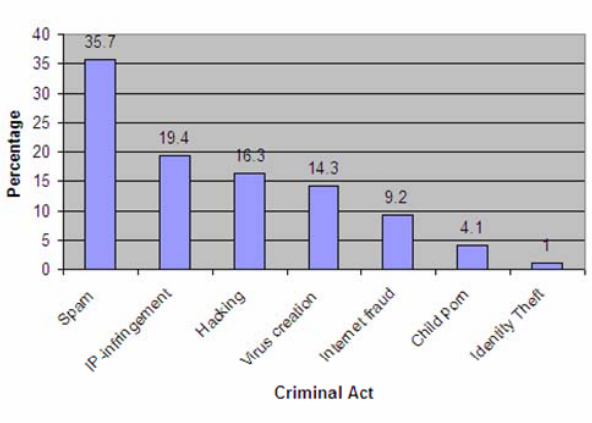

Fig. 3 Performed cyber crimes

5) Internet users are ignorant of ways to detect a computer incident when it occurs. Only 60% are aware of at least one way in which to detect a computer incident and half of these do not have regular system checks.

6) Most perpetuators said that they find it easy to commit these acts because they are protected by a feeling of invisibility while online, the acts are relatively simple to conduct and also for adventure.

These statistics show that Ugandans and internet users in Uganda are initiating and falling victim of cyber crime, although the public are not reporting to the relevant authorities either because of non-existent sensitization programs or hopelessness due to the unavailability of e-laws that would bring them justice.

V. Recommendations

The researcher believes that prevention is best solution to curbing the increasing number security violations on the net. However, it may not be feasible to prevent all incidents, and that is when two major factors come in play. Firstly, forensic knowledge and expertise, followed by the relevant laws that would empower victims to seek justice. This section discusses some few recommendations to that effect.

A. Sensitization

There is need for setting up a public facility (preferably with a presence on the internet) where victims can report incidences. The public need a lot of sensitization and training on what computer crimes are, in which forms they can manifest, how to detect them, what to do after detection and how to prevent and minimize them. The Police should also endeavor to build trust and confidence in the population by using the media and otherwise, so that more such incidents are reported to them for proper and unified record keeping.

B. Internet Filtering

Countries implementing Internet filtering at client, Internet Service Provider (ISP) and government levels would prevent access to illegal websites like those promoting concepts like drug use, gambling, immorality, pornography, bomb making recipes, terrorism and the like. Legislative organs can mandate a body to filter all incoming web traffic before it is accessed by Internet users in that country and block away websites that pose security threats to the users. Internet Service Providers are also in position to protect their clients against most cyber attacks like distributed denial of service attacks, email spoofing, SPAM and the like if they were only allowed to do it.

C. Regulation of Cyber Cafes

A crime committed in a public facility like an internet café will be very hard to detect and identification of the culprit impossible. Setting up policies like supervision of children or always logging onto system resources using the unique identifiers (like smart cards, passports or national identity cards) as usernames will simplify process of tracking the culprits.

D. Amendment of Laws

Enacting global cyber laws that deal with harmonization and standardization of computer crime would bring us closer to attaining total justice to cybercrime victims. Although a number of countries have enacted cyber laws and have punished criminals within their jurisdiction, they are dominated by the developed countries.

Most developing countries have not yet enacted e-laws and we recommend that they urgently incorporate them into the Laws of the land. Harsh punishments should be given to defaulters so that people fear to commit these acts and victims motivated to report them. This would prevent escalation of cases and further loss of money, time, data and equipment.

E. International Co-operation and Further Research

Countries should actively work together and strengthen research activities that will explore new techniques and procedures that will combat the rate at which cyber crime spreads and the ease at which they can be conducted.

VI. Conclusion

Our study has revealed that cyber crime is silent but common even in the developing countries like Uganda. Cyber crime instances are mainly discussed socially and the victims suffer in silence, while the perpetrators continually hide under the invisibility of the cyber world. As much as 90% of Internet users in Uganda have suffered losses caused by Internet crimes. Furthermore, 25% have confessed to having initiated cyber crimes. It is hard to convict cyber criminals because of two major reasons. Firstly, few countries have enacted e-laws and the existing ones are not sufficient in convicting culprits because of jurisdiction anomalies especially when the investigation transcends international borders. Secondly, obtaining evidence of computer crime that would stand in courts of law is lacking in many countries since the field of computer forensics is still relatively new and lacks sufficient literature and expertise. Cyber crime is a serious threat to the security of cybercitizens and all countries should take it seriously.

REFERENCES

[1] The World Fact Book (2005) Available: http://www.cia.gov/cia/publications/factbook/geos/ug.html, May 2005.
[2] Joseph Migga Kizza, "Ethical and Social Issues in the Information Age," Second Edition, Springer, 2003.
[3] Boda Mash, "International Law and Cyber crime" Paper presented at a seminar on Cyber Liability, 25 - 26th November 2002, Pune, India.
[4] InterGOV International, "International Web statistics report 2002", Available: http://www.intergov.org/public information/general information/latest web stats.html. Accessed in January 2005.
[5] Sophos Anti Virus Company, "War of the worms: Netsky-P tops list of year's worst virus outbreaks", 2004 Press Release Available: http://www.sophos.com/pressoffice/pressrel/uk/20041208yeartopten.html
[6] "IC3 2004 Internet Fraud - Crime Report", National White Collar Crime Center (NW3C), 2005. Available: http://www.ifccfbi.gov/strategy/2004_IC3Report.pdf
[7] All net Available: http://www.all.net/CID/Threat/Threat22.html, February 2004
[8] Asian School of Cyber Laws Available at: http://www.asianlaws.org, May 2004
[9] The Internet Service Unit Available at http://www.isu.net.sa/index.htm, March 2004
[10] Jonathan Zittrain and Benjamin Edelman, Berkman, " Documentation of Internet Filtering in Saudi Arabia" Berkman Center for Internet at Harvard Law School, Available: http://cyber.law.harvard.edu/filtering/saudiarabia/
[11] Ssemujju Ibrahim Nganda & Halima Abdallah, "Interpol pursues Zzimwe fraud case", The Weekly Observer, 13th January 2005.
[12] Davis Weddi and Steven Candia "Porn web site sells Ugandans", Sunday Vision Newspaper, 24th July, 2005.
[13] The Valencian Newspaper "Internet Kimansulo targets Ugandans", 23rd July 2005. Available: http://www.thevincentian.com/forum/forum_posts.asp?TID=43&PN=0&TPN=29