Institution Networks

Shafi'i Muhammad Abdulhamid[*], *Chiroma Haruna*[**]
and Adamu Abubakar[***]

ll crimes performed or resorted to by abuse of computer network or Internet with the purpose influencing the functioning of the computer system and also for financial gains are referred as cybercrime. This paper examines different types of cybercrimes that are frequent in ligeria and also checks the rate at which these crimes are carried out by the use of academic istitution networks as the access point. Data was obtained through questionnaires and analyzed. ome of the findings show that the Yahoo Boys attack is very popular even in the academia nd that students are the most active participants in cybercrime in the Nigerian institution etworks. It is also found that it is possible to create a taxonomy of scams and scammers and evelop tools, measures, campaigns and laws that will hurt their bottom line.

Ceywords: Cybercrime, Yahoo Boys, 419, Hackers, Salami attack, Cyber plagiarism

roduction

nputer interconnectivity and Internet networks have revolutionized the way that governments, academic institutions and much of the world communicate and duct businesses/researches in Nigeria. The benefits have been massive and the reased usage of the world wide web has also enabled a dramatic rise in criminal vity that exploits this interconnectivity for prohibited financial gains. Efforts to lress Internet crime include activities associated with defending networks and a, detecting criminal activities, inquiring into crime and taking legal action inst criminals.

Cyberspace security is crucial for maintaining the continuity of these vital services l for preserving the public's trust in information systems. It requires new levels of nmunication and cooperation, not only among government agencies and departments also between academic institutions and the private sector. It involves protecting tical infrastructures from intrusion or attack as well as using the infrastructure as a l with which law-enforcement institutions, and defense and public-health agencies ı gather, analyze and disseminate information.

Lecturer, Department of Cyber and Security Science, Federal University of Technology, Minna PMB 65, Niger State, Nigeria; and is the corresponding author. E-mail: shafzon@yahoo.com

Lecturer, Department of Computer Science, Federal College of Education (Technical), Gombe PMB 60, Gombe State, Nigeria. E-mail: freedonchi@yahoo.com

* Research Scholar, International Islamic University, Malaysia. E-mail: adamuabubakar9@gmail.com

The use of Information and Communication (ICT) has fundamentally revolut societies. All sectors are affected by the dramatic spread of these technologi bring with them both good and bad effects. On the other hand, there are new t crimes as well as the commission of traditional crimes by means of ICTs, irrespec our national boundaries. Cases of pornography, Internet offences such as ur fund transactions, the offer of unlawful services, hazardous computer worms and v etc., are increasing world wide. Although recently Internet criminality has be spreading in the developing countries, evidence has shown that the countri the technology, legal instruments and manpower to deal with these new c Therefore, there is the need to better understand the evolution of Internet crim on the continent and to support research contributing to generate awareness stakeholders and local capacities in these countries.

So many crimes are committed every day in the cyberspace with Nigeri the forefront of sending fake and deceitful financial proposals all over the Recently, a report by the Internet Crime Complaint Center, which is a partn between the FBI and America's National White Collar Crime Center, re that Nigeria is now ranked third among the list of top ten sources of cybercr the world with 8% behind the US with 65% and the UK with 9.9% (Daily 2010). Criminals that indulge in the advance fee fraud schemes (419) ar popularly called 'Yahoo Boys' in Nigeria (Longe and Chiemeke, 2008). The c has therefore carved a niche for herself as the source of what is now pop called 419-mails, named after Section 419 of the Nigerian Criminal Code 777 of 1990) that forbid advance fee fraud. What the remainder of the wor not know is that a majority of these Internet crimes are committed using aca institution networks in Nigeria.

2. Related Works

Internet crime refers to criminal activities that specifically target a computer or ne for demolition or infiltration. For instance, unauthorized access or distribution of v into systems or networks. Internet crime also includes the use of computers as to conduct criminal activity such as financial fraud, identity theft, phishing, exploitation and copyright violations. The Internet significantly increased the cri power and reach in perpetrating such crimes (Powner, 2007).

Observers are warning that developing countries are fast becoming a major of Internet crimes. For instance, Nigeria is ranked first in the African region target and origin of malicious cyber activities; and this is spreading across the African sub-region (Ribadu, 2007). Egypt is also known to be one of the most pl countries in the world with approximately 2000 phishing incidents, followed by nations in the region such as South Africa (Ojedokun, 2005), and recently Gl

There remains a lack of consensus over the forms of computer misuse that s attract a criminal sanction, as opposed to a civil remedy such as those attach intellectual property and commercial laws. Certainly, some of the cybercrimes listed here do not fall properly within the province of the criminal law (Bronitt and Gani, 2003). Cybercrimes originating in America often implicate national boundaries; plenty of these cases fall under federal laws. National collaboration with local law enforcement and prosecutors to share information and efforts through cooperation has proved efficient in curbing traditional crimes (Hinduja, 2007).

Cybercrimes are demanding law enforcement departments in general and forensic investigators in particular to channelize an increasing amount of their energy toward successfully detecting, arresting and helping in the successful prosecution of the criminals. Meanwhile, national boundaries effectively disappear for many Internet crimes and the jurisdiction of the crime is another complex problem. Even though a complete study of jurisdictional problems is beyond the scope of this research, it is worthy of notice that nations differ in civil and criminal offense principles, substantive and procedural law, information gathering and storage, and other evidentiary and juridical factors (Lyman, 2002).

The cyberspace currently looks like a safe haven for criminals who have basically moved away from the streets to an electronic platform offered by the world wide web. Different countries have implored different methods to contend with cybercrimes depending on their types and degree. Definitely, a nation with high incidence of crime cannot develop, as crime is the direct reverse of development. It leaves some undesirable social and economic aftermaths (Sylvester, 2001). In Nigeria, so many measures are now being undertaken to curb cyber crimes—the most popular one being the controlling of world wide web access points (Longe and Chiemeke, 2008).

3. Cyber Criminality and National Boundaries

The globalization phenomenon is gradually creating immense opportunities for academia, tourists, and business people, and at the same time increasing economic growth and development. Still, criminals who engage in human trafficking and drug deal, weapon smuggling, fraud, counterfeiting, and other financial crimes are taking advantage of opening up of societies and borders by the cyberspace.

Cybercrime knows no boundaries, yet the criminal law remains deeply protective in nature. This paradoxical pressure connecting the geographically bounded nature of criminal law and the trans-border superiority of cyber criminality is a persistent subject matter in the literature. The customary resolution of this contradiction has been to suggest a thorough reformulation of the set of laws governing jurisdiction. From the onset, we must disclose our doubt towards the globalization of Internet crime and the anxiety to embrace extra-territorial offences as the way out.

Internet, crime techniques have distinctiveness that can greatly improve the reach and impact of unlawful activities, such as the following:

dvancement in technology allows criminal actions to effortlessly cross-ultiply state and countrywide boundaries.

high velocity, and by attacking a huge number of victims at the same int in time, Internet crime can be carried out repeatedly.

ternet criminals can remain unknown more easily.

rcrimes indeed constitute a global concern and no state is free from ility. On the other hand, to appreciate why cybercriminality in Africa differs r parts of the world, one ought to appreciate the state of information security ea which is affected by factors such as the expansion of user base, poor lertness, lack of training for law enforcement authorities, lack of rules and cross-border cooperation.

of Cybercrimes in Nigerian Academic Institutions

rn thief can steal more with a computer than a gun. The following cybercrimes tified to be very popular in Nigerian institutions.

ing

tudents can be seen on a daily basis engaging in brainstorming sessions at s trying to break security codes for e-commerce, funds point cards and g product sites. It is astonishing that even with their low level of training anding of the intricacies of computing techniques, they occasionally get

l of Service Attack

ct by the fraudster who floods the bandwidth of the victim's system or fills nbox with junk mails depriving him of the services he is entitled to access

Dissemination

a computer program that infects files, frequently executable programs, a duplication of itself into the file. These copies are usually executed contaminated file is loaded into memory, giving way to the virus to other files. A virus requires human participation (usually unaware)

e Piracy

es the unlawful reproduction and sharing of applications, games, videos This can be completed in a number of ways. Normally, pirates get an on of an application, film or game from the Internet and unlawfully make

4.5 Pornography

The term 'pornography' covers all types of material such as explicit literature (electronic or print), photography, films and videotapes with varying degrees of sexual content. The Internet has provided a free market for this crime as so many pornographic sites are now all over the net. This is one of the most popular cybercrimes in Nigerian academic institutions (Longe and Longe, 2005).

4.6 Internet Relay Chat (IRC) Crime

IRC servers have chat rooms in which people from anywhere in the world can come together and chat with each other. Criminals use it for meeting co-conspirators. Hackers use it for discussing their exploits and sharing the techniques.

4.7 Credit Card Fraud

If electronic transactions are not protected, the credit card numbers can be stolen by hackers when users type the credit card number into the Internet page of the seller for online transaction. The hackers can abuse this card by impersonating the credit card holder.

4.8 Cyber Extortion

Hacking into and controlling various industry databases (or the threat of), promising t release control back to the company if funds are received or some other demand satisfiec

4.9 Phishing

This is a technologically advanced scam that often uses spontaneous mails to tric people into disclosing their financial and/or personal data. This is used by students Nigerian campuses. Phishing refers to cloning product and e-commerce web pages order to dupe unsuspecting users. Criminals clone product websites to trick innoce world wide web users into ordering products that are actually unreal.

4.10 Spoofing

To have one computer on a network to act like another computer, usually one w exceptional access rights, so as to gain access to the other systems on the network

4.11 Cyber Stalking

The fraudster follows the victim by distributing mails and entering the chat roc frequently.

4.12 Cyber Defamation

The fraudster sends e-mails containing defamatory content to people related to victim or posts it on a website. A displeased member of staff may use this against manager; ex-boys against the girl; divorced husband against spouse, etc.

one displeased may do this against a boss, friend or official.

Salami Attack

ni assaults are flamboyant economic scams or exploits against confidentiality omprehensive data gathering. Their nature and intricacy baffle the most tive process accountants, should they ever be known. Occasionally the most nificant things, handled in a smart way, can multiply beyond expectation rucci, 2002).

Cyber Plagiarism

is the act of stealing peoples' ideas through the world wide web. With increase in vide spread campus networks in Nigeria, students and lecturers alike use it to other people's ideas and publish them as their own original work.

Yahoo Boys Attack

Yahoo Boys assault, also called 419, is characterized by a slow turnaround from est of e-mail addresses to the first message (typically at least one month), sive number of messages being sent to each harvested spam-trapped addresses, ypical product-based spam (i.e., spam selling an actual product to be shipped wnloaded even if the product itself is fraudulent). E-mail addresses are obtained world wide web access points using e-mail address harvesting applications spiders) such as E-Mail Extractor Lite1. These tools can automatically retrieve il addresses from web pages. Nigerian fraud letters join the warning of rsonation scam with a variation of an advance fee technique in which an l from Nigeria offers the recipient the 'chance' to share a percentage of a huge nt of money that the author, a self-proclaimed government official, is trying to n out of the country.

lethodology

al of ten academic institution networks satisfied the stratification for availability mputer network facilities, speed, patronage and consistency for the objective. urvey method employed was the use of questionnaire, which solicits information respondents selected for the research. The questionnaire titled "Cybercrimes gerian academic institutions" was administered to respondents in ten locations geria—two institutions in the north western region, five in the north-central n and three in the western region. Confidentiality of personal information was nteed as respondents were asked to specify their age, gender and occupation. respondents were encouraged to provide honest answers, and items in the ionnaire involving some Internet technicalities were explained to assist the ndents in understanding each question.

for age, gender and occupation. The data captured ... presented and analyzed below.

5.1 Data Presentation and Analysis

Table 1 presents the data obtained from the questionnaires as categorized accordir to occupation of respondents in the institutions.

Table 2 presents the total frequency of data obtained from th questionnaires, the percentage and the mean of each cybercrime as supplie by the respondents.

6. Results and Discussion

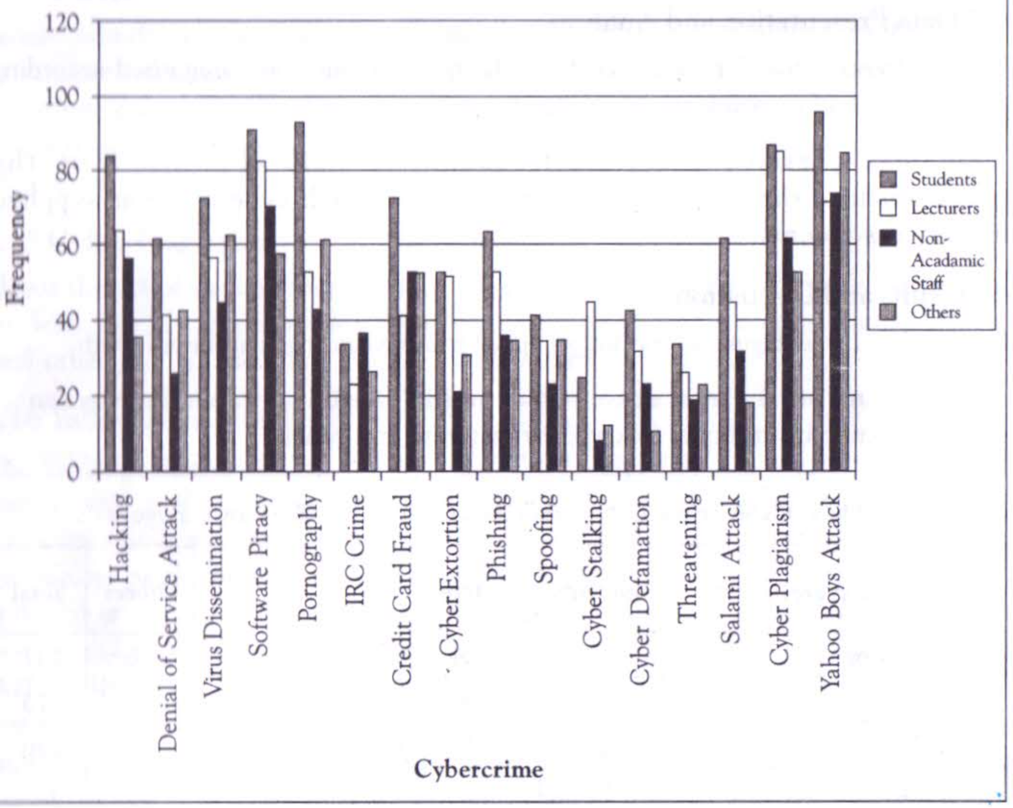
From Table 1 and Figure 1, the following interesting findings can be inferred:

- Students are the most active participants in cybercrime within the Nigerian academic institutions, followed by lecturers and others.

Table 1: Cybercrime in Nigerian Academic Institutions by Category

S. No.	Cybercrime	Students	Lecturers	Non-Acadamic Staff	Others	Tot
1.	Hacking	84	64	57	36	24
2.	Denial of Service Attack	62	42	26	43	17
3.	Virus Dissemination	73	57	45	63	23
4.	Software Piracy	91	83	71	58	30
5.	Pornography	93	53	43	62	25
6.	IRC Crime	34	23	37	27	12
7.	Credit Card Fraud	73	42	53	53	22
8.	Cyber Extortion	53	52	21	31	15
9.	Phishing	64	53	36	35	18
10.	Spoofing	42	35	23	35	1
11.	Cyber Stalking	25	45	8	12	
12.	Cyber Defamation	43	32	23	11	1
13.	Threatening	34	26	19	23	1
14.	Salami Attack	62	45	32	18	1
15.	Cyber Plagiarism	87	85	62	53	2
16.	Yahoo Boys Attack	96	72	74	85	3

by Occupation



- The 'Yahoo Boys' syndrome cut across all ages and all occupations. That is, there is no category of cyber users that does not participate in this type of crime.
- The 'Yahoo Boys attack' is more popular in students, non-academic staff and others, while cyber stalking and defamation are the least popular amongst them.
- Cyber plagiarism is more popular amongst lecturers and IRC crime is the least popular amongst them.
- It also shows that cyber pornography has a high rate of patronage in Nigerian campuses.

From Table 2, the following interesting findings can also be inferred:

- The Yahoo Boys attack has the highest number of respondents claiming that people use the campus networks to carry out such attacks, with a frequency

- Software piracy, plagiarism and pornography are also at a very high rate Nigerian academic institutions networks.
- Respondents conceded to the fact that most cybercrimes are perpetrat using mobile and private systems like laptops within academic institution
- A good number of the perpetrators are not members of the academ institutions; they are private individuals, who come from outside, use t network and leave. They constitute the category called 'Others' in Table

Table 2: Cybercrime in Nigerian Academic Institutions by Percentage and Aver

S. No.	Cybercrime	Frequency	Percentage of Response	Ave
1.	Hacking	241	7.77	60
2.	Denial of Service Attack	173	5.58	43
3.	Virus Dissemination	238	7.68	59
4.	Software Piracy	303	9.77	75
5.	Pornography	251	8.10	62
6.	IRC Crime	121	3.90	30
7.	Credit Card Fraud	221	7.13	55
8.	Cyber Extortion	157	5.06	39
9.	Phishing	188	6.06	47
10.	Spoofing	135	4.35	3
11.	Cyber Stalking	90	2.90	2
12.	Cyber Defamation	109	3.52	2
13.	Threatening	102	3.29	2
14.	Salami Attack	157	5.06	3
15.	Cyber Plagiarism	287	9.26	7
16.	Yahoo Boys Attack	327	10.55	8

7. Proposed Solutions

Internet crimes know no borders, and perpetrators continue to exploit leg gaps and jurisdictional issues to their advantage. Furthermore, it is often as to whose responsibility it is to tackle a particular crime or lead an invest or how best to cooperate with each other through extradition and assistance policies. This is so not only on a global stage but also within where several law enforcement departments are implicated. The follow

- Content fitter should be employed in all Nigerian institution networks to reduce the use of pornographic websites.
- The Nigerian National Assembly should enact legislative laws that will specify punishments for all types of cybercrimes. But in the interim, academic institutions will have to devise their own ways of dealing with the perpetrators.
- Access to Nigerian institution networks should be restricted to the members of the academia only.
- The institutions should device ways of monitoring the activities of all Internet users within their networks.
- The Nigerian Economics and Financial Crime Commission (EFCC) is the body saddled with the responsibility of curbing financial crimes within the country. They have been doing a great job in this regard but it still needs legal backing to be able to trial the perpetrators.
- Forensic science should be encouraged or introduced in Nigerian institutions of higher learning to be able to catch up with the rising cases of Internet crimes within and outside the country.

onclusion

ber security issues are a global happening and can be tackled by global solutions. do this, we must work hand in hand, put a global security plan and the intellectual omos, and also put together a worldwide and bilateral corporation against cybercrime enace. Knowing fully well that the fraudsters are in business, we can deduce that ey are reasonably flourishing. In fact, we see increasing Nigerian scams every day on e Internet. This is not about people lacking scientific skills; it is about them not inking critically. User alertness and education campaigns could transform this. gerian fraudsters are not restricted to Yahoo Boys, nor to frauds in which they try to tain people's cameras free of charge. This research gives us optimism that it is likely create a taxonomy of scams and scammers, and build up apparatus and campaigns at will hurt the base line of the fraudsters.

Nigerian academic institutions should direct the line of attack in war against bercrime in the state by instituting legal and technical frameworks to protect systems d networks, and secure vital data infrastructure for the academic circles and the ate as a whole. Establishment of a podium for public-private stakeholder's partnership set guide principles and standards for cyber security in Nigeria. enable Nigeria deal with the menace of cybercrime, it is important to build global w enforcement collaboration with other worldwide agencies.

papers/Salami.html

2. Bronitt Simon and Gani Miriam (2003), "Shifting Boundaries of Cybercrime: Fro Computer Hacking to Cyber-Terrorism", *Crim. L. J.*, Vol. 27, pp. 303-321.
3. Daily Trust (2010), "EFCC—Country on Cyber Crime Top Ten List", available http://allafrica.com/201012010182.html, Accessed on December 1, 2010.
4. Hinduja Sameer (2007), "Computer Crime Investigations in the United Stat Leveraging Knowledge from the Past to Address the Future", *International Journ of Cyber Criminology*, Vol. 1, No. 1.
5. Longe O B and Chiemeke S C (2008), "Cyber Crime and Criminality in Niger What Roles are Internet Access Points Playing?", *European Journal of Social Scienc* Vol. 6, No. 4, pp. 132-139.
6. Longe O B and Longe A Folake (2005), "The Nigerian Web Content: Combat Pornography Using Content Filters", *Journal of Information Technology Impa* Vol. 5, No. 2, pp. 59-64.
7. Lyman M D (2002), *Criminal Investigation: The Art and the Science*, 3rd Editi Prentice Hall, Upper Saddle River, New Jersey.
8. Ojedokun A A (2005), "The Evolving Sophistication of Internet Abuses in Afri *The International Information and Library Review*, Vol. 37, No. 11, pp. 11-17.
9. Powner Dave (2007), "Cybercrime: Public and Private Entities Face Challen in Addressing Cyber Threats", pp. 1-10, Report to Congressional Request GAO-07-705.
10. Ribadu N (2007), "Cyber-Crime and Commercial Fraud: A Nigerian Perspecti Presented at the Congress Celebrating the 40th Annual Session of the Un Nations Commission on International Trade Law, July 9-12, Vienna, Austria.
11. Sylvester L (2001), "The Importance of Victimology in Criminal Profiling", avail at http://isuisse.ifrance.com/emmaf/base/impvic.html

Reference # 35J-2011-03-0