

The Impact of Mobile Information and Communication Technology on Cybercrime in Nigeria

Oyenike Mary Olanrewaju¹, Faith Oluwatosin Adebisi²

^{1,2}Department of Mathematical Sciences and Information Technology
Federal University Dutsin-Ma,
Katsina State, Nigeria

Abstract - The advent of mobile Information and Communication Technology (ICT) has recorded a steady growth rate over the past decade but has however given way to something greater and a more alarming increase in the rate of internet insecurity and cybercrime in Nigeria. It is therefore no wonder that crimes like mail scams, phishing, identity theft and privacy intrusion among others are on the increase in the country. Although some efforts have been made in the past to reduce the incidence of these cybercrimes, it is quite obvious that the high demand on mobile ICT and their numerous benefits are being played upon to the detriment of innocent people. This paper discusses the current internet security situation and the direct impact of mobile information and communication technologies on cybercrime in Nigeria and as well proffer solutions.

Keywords: Cybercrime, Security, Mobile Devices, Intelligent, Investigatory

I. INTRODUCTION

Information and Communications Technology (ICT) is often used as an extended synonym for Information Technology (IT). ICT is a term that summarizes the role of unified communications networks and the integration of telecommunications (telephone lines and wireless signals), computers and all its form of networks as well as necessary enterprise software, middleware, storage, and audio-visual systems, which enable users to access, store, transmit, and manipulate information to meet day to day needs of the society.

A mobile device or mobile ICT basically describes a small, handheld computing device, typically having a display screen with a miniature keyboard and portable enough for users to carry with hands or conveniently kept in a pocket. They are also location independent. In other words their functionality is not confined to a specific geographical location. Nokia, LG, Motorola Mobility, BlackBerry, Samsung, and Apple are just a few examples of the many manufacturers producing these types of devices. A handheld computing device has an operating system (OS), and can run various types of application software, mostly called apps. Most handheld devices are also equipped with wireless fidelity (Wi-Fi), Bluetooth, and Geographic Positioning System (GPS) that can allow connections to the Internet and other Bluetooth enabled devices along with a

stable battery power source. Mobile phones, Smartphones and PDAs are popular examples of these mobile devices. (Wikipedia)

Cybercrimes on the other hand can be defined as offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, or deny someone of what belongs to him/her, using modern telecommunication networks such as Internet and mobile phones. Such crimes may threaten a nation's security and financial stability. Cybercrime can simply be explained as crimes carried out with the aid of a computer system against an individual, organization or a nation[9].

The whole African continent is increasingly relying on new information technology and the internet with new media to conduct business, manage industrial activities, and engage in personal communication among other numerous benefits connecting us to the developed world. While these mobile technologies and devices allow for enormous gain in efficiency, productivity and communication, they also create a vulnerability to those who wish to and thrive in taking advantage of new situations.

The exponential growth of the internet and its global acceptance is generating increasing security threats. The cyber space creates unlimited opportunities for commercial, social, and, educational activities as well as a haven for societal miscreants to perpetrate their sinister acts. Technology is developing by leaps and bounds thereby making the internet easily accessible through various mobile devices including smartphones, tablets among others. Even the smallest phone is now internet enabled and thereby susceptible to internet crime or cybercrime.

This article therefore looks into the growth of mobile devices as well as the different cybercrime methods that have threatened the basic benefits of our ICT age. The approach used was to review related literatures on cybercrime in Nigeria, analyze the impact of the tremendous increase in mobile ICT on cybercrime, propose an intelligent cybercrime investigatory system framework and suggest various ways cybercrime can be controlled.

II. LITERATURE REVIEW

Reference [2] carried out investigations into the activities of cyber criminals within Nigeria, where they discovered that cybercriminals' strategies include collaboration with security agents and bank officials, local and international networking, and the use of voodoo that is, traditional supernatural power. It was also revealed that most perpetrators of cybercrime were involved in on-line dating and buying and selling with fake identity among others. The article discussed the need for reorientation of Nigerian youths in higher institutions towards various other means of livelihood.

Reference [9] identify urbanization, unemployment, quest for wealth, weak implementation of cybercrime laws and negative role models among others as major reasons why Nigerian youth commit cyber-crimes. Several youth engage in cybercrime with the aim of emerging as the best hacker, or as a profit making venture since the tools for hacking in our modern world has become affordable by many. The article highlighted reduction of competitive strength, loss of time and resources among others as part of grievous effect of cybercrime in Nigeria.

In the review article by [10], it was stated that 23 percent of people worldwide will fall for spear phishing attacks, while web pages are infected on average every 4.5 seconds. The review also stated that African Countries like Kenya, Nigeria, Tunisia, Tanzania etc. are almost free from the cyber laws and policies. The article highlighted that cybercrime is a sensitive issue for people relying on iPhones for their day today working because some worm can eat all the iPhones and convert the Androids to bricks.

In a survey carried out within Nigeria by [24], the research scope is focused on gathering data on the economic cost of cybercrime on the Nigerian citizen thus simulating a better grasp of this issue and the need to actively promote proper, firm and fair legislation. 2,980 persons participated in the survey from five locations in the country. 41% have been affected by cybercrime in one way or the other.

Cybercrime has evolved in parallel with the opportunities afforded by the rapid increase in the use of the Internet for e-commerce and its take-up in the developing world. In February 2013, 2.7 billion people, nearly 40% of the world population, had access to the Internet. The rate was higher in the developed world (77%) than in the developing world (31%). While Africa had the lowest Internet penetration rate (16%), between 2009 and 2013, Internet penetration has grown fastest in Africa (annual growth of 27%) followed by Asia-Pacific, the former Soviet Union, and the Arab states (15% annual growth rate). Around one quarter of all Internet users used English (27%) on the web, and another quarter (24%) used Chinese [20].

The exponential growth of the internet and its global acceptance is generating increasing security threats. The cyber space creates unlimited opportunities for commercial, social, and, educational activities as well as a soft spot for haven for those who thrive by perpetrating treacherous acts. Figure 1 below is graphical representation of various cybercrime methods according to internet cybercrime reports. Virus, worms, Trojans and Malware top the list.

These are anomalies that can easily be aided with mobility of devices.

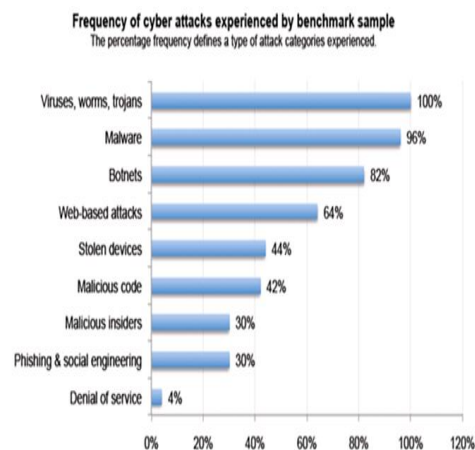


Fig. 1. Distribution of various Cyber-attacks according to Internet Cybercrime Report 2012

III. CYBERCRIME IN NIGERIA

A. TYPES OF CYBERCRIME PERPETRATED THROUGH MOBILE DEVICES

Cybercrimes simply put are crimes that are committed using the Computers and Networks. There are several types of cybercrimes which are aided and given a boost by the advent of mobile devices some of which include:

1) Cyber Terrorism

The Center for Strategic and International Studies (CSIS) has defined it as "the use of computer network tools to shut down critical national infrastructures (e.g., energy, transportation, government operations) or to coerce or intimidate a government or civilian population."

Reference [29] defines cyber terror as "the intimidation of civilian enterprises through the use of high technology to bring about political, religious, or ideological aims and actions that result in disabling or deleting critical infrastructure data or information." On the other hand, [21] defined Cyber terrorism as an act of terrorism committed through the use of cyberspace or computer resources. It means that any act intended to instill fear by accessing and distorting any useful information in organizations or Government bodies using Computer and Internet is generally referred to as Cyber Terrorism.

2) Fraud - Identity Theft

Fraud is a criminal activity in which someone pretends to be somebody and retrieve vital information about someone says [16]; For instance, creating a false bank webpage to retrieve information of someone's account. The concept is about someone gaining access to another person's information and uses it for his own benefit. This could range from a black-hat hacker stealing online banking account login and password to getting access to ATM to commit. In Nigeria people design web links forms requesting users to fill in their basic information including,

unique details like pin numbers and use that to commit crimes.

3) Drug Trafficking Deals

Another type of Cyber Crime is Drug Trafficking; it is a global trade involving cultivation, manufacture, distribution and sale of substances which are subject to drug prohibition law. According to Cyber Advocate, drug traffickers are increasingly taking advantage of the Internet to sell their illegal substances through encrypted e-mail and other Internet Technology. Some drug traffickers arrange deals online, use courier Web sites to track illegal packages of pills, and swap recipes for amphetamines in restricted-access chat rooms. The rise in Internet drug trades could also be attributed to the lack of face-to-face communication. These virtual exchanges allow more intimidated individuals to comfortably purchase illegal drugs.

4) Cyber Stalking

Cyber stalking is essentially using the Internet to repeatedly harass another person. This harassment could be sexual in nature, or it could have other motivations including anger. People leave a lot of information about themselves online. Such information can leave one vulnerable to cyber stalking, a term that essentially refers to using the Internet to stalk (to illegally follow and watch somebody) [12]. Whereas content may be offensive in a non-specific way, harassment directs obscenities and derogatory comments at specific individuals focusing for example on gender, race, religion, nationality, sexual orientation. This often occurs in chat rooms, through newsgroups, and by sending hate e-mail to interested parties.

5) Spam

Spam is the use of electronic messaging systems to send unsolicited bulk messages indiscriminately. While the most widely recognized form of spam is e-mail spam, the term is applied to similar abuses in other media: instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs, wiki spam, online classified ads spam, mobile phone messaging spam, Internet forum spam, junk fax transmissions, social networking spam, television advertising and file sharing network spam [23]. Spamming remains economically viable because advertisers have no operating costs beyond the management of their mailing lists, and it is difficult to hold senders accountable for their mass mailings. Because the barrier to entry is so low, spammers are numerous, and the volume of unsolicited mail has become very high. A person who creates electronic spam is called a spammer.

6) Logic Bombs

A typical logic bomb tells the computer to execute a set of instructions at a certain date and time or under certain specified conditions. The instructions may tell the computer to display "I gotcha" on the screen, or it may tell the entire system to start erasing itself. Logic bombs often work in

tandem with viruses. Whereas a simple virus infects a program and then replicates when the program starts to run, the logic bomb does not replicate – it merely waits for some pre-specified event or time to do its damage. Time is not the only criterion used to set off logic bombs. Some bombs do their damage after a particular program is run a certain number of times. Others are more creative. There are several reported cases that a programmer told the logic bomb to destroy data if the company payroll is run and his name is not on it; this is a sure-fire way to get back at the company if he is fired! The employee is fired, or may leave on his own, but does not remove the logic bomb. The next time the payroll is run and the computer searches for but doesn't find the employee's name, it crashes, destroying not only all of the employee payroll records, but the payroll application program as well. Logic bombs present a major threat to computer systems, not just because of the damage they themselves can do, but because they provide a technique to facilitate more devastating crimes [9].

7) Password Sniffing

Password sniffers are able to monitor all traffic on areas of a network. Crackers have installed them on networks used by systems that they especially want to penetrate, like telephone systems and network providers. Password sniffers are programs that simply collect the first 128 or more bytes of each network connection on the network that's being monitored. When a user types in a user name and a password as required especially when using certain common Internet services like FTP (which is used to transfer files from one machine to another) or Telnet (which lets the user log in remotely to another machine)--the sniffer collects that information. Additional programs sift through the collected information, pull out the important pieces (e.g., the user names and passwords), and cover up the existence of the sniffers in an automated way. Best estimates are that in 1994 as many as 100,000 sites were affected by sniffer attacks [9].

IV. INFLUENCE OF CYBERCRIME

A. ON INDIVIDUALS

The effects of cybercrime are becoming too expensive to bear as many people are falling prey each day and losing huge sums of money from attacks by cybercriminals. Because of this, many people in Nigeria have lost faith in the benefits of the internet and mobile technologies as the negative side seems to prevail. Services aided by mobile technologies such as internet and mobile banking are being termed insecure because loopholes are being found and people duped by the day. People would rather perform their transactions over the counter which could be time and cost ineffective for them.

Fig. 2. is a pictorial representation of items that individual have lost due to cybercrime in Nigeria according to [24].

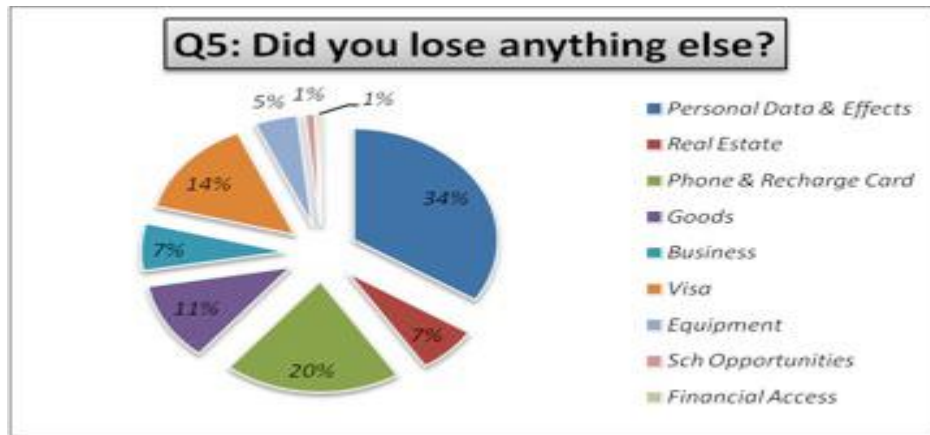


Fig. 2. Individual Loss to Cybercrime Source: Economic Cost of Cyber Crime in Nigeria[24]

B. ON ORGANIZATIONS

In spite of the outcry on cybercrimes, not all organizations and institutions have put in place measures to safeguard their systems and data making them susceptible to logic bombs, data theft among other things. These in the long run cost them a lot of money and efforts to recover from attacks by cyber criminals.

Also, financial institutions that are introducing electronic means of carrying out financial transactions to cut back on operational expenses are finding it hard to gain necessary ground because people do not yet trust the system.

C. ON THE SOCIETY/NATION

Nigeria’s reputation has suffered greatly due to the increase of cybercrime in the country. In the years before full penetration of the internet and mobile technologies, Nigeria had already gained the reputation of one of the most corrupt countries. However, as internet penetration

and technologies gained ground, the situation has grown worse as financial crimes and other forms of crime have escalated with the use of the internet and new mobile technologies. This has caused Nigeria to lose a lot of foreign exchange from business and opportunities from investors. A stigma has been created for Nigeria and almost every Nigerian outside the country is observed suspiciously as a perpetrator of crimes. Reference [24] represented the distribution of cybercrime activities as displayed in Fig. 3 below where Uyo and Abeokuta have the highest value. Nigeria as a whole has been stigmatized as a nation whose citizens are mostly untrustworthy. This has brought about serious embarrassment when Nigerians have to travel to foreign countries; extra searching at airport as well as denial of opportunities because of high rate of cybercrime and other related offences common to Nigerians. Fig. 3 below represents the distribution of cybercrime activities across Nigeria.

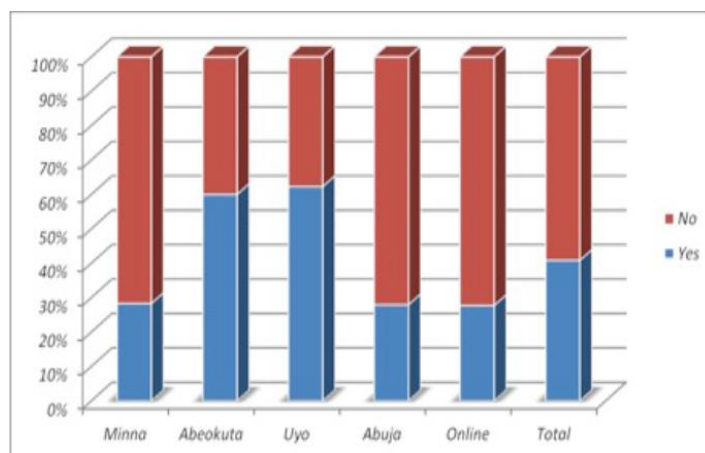


Fig. 3. Distribution of Cybercrime impact by location. Source: Economic Cost of Cyber Crime in Nigeria[24]

Fig. 4 is a representation of impact of cybercrime on the image of Nigerians according to the research carried out by [16]. Research shows that if a country like Nigeria is highly polarized by cybercrime, communication within and outside

such a country would be difficult because everybody will appear as a suspect which would in turn have a negative impression on such a country. A larger population of

respondents strongly agreed that this is possible while few

respondents disagreed with this view.

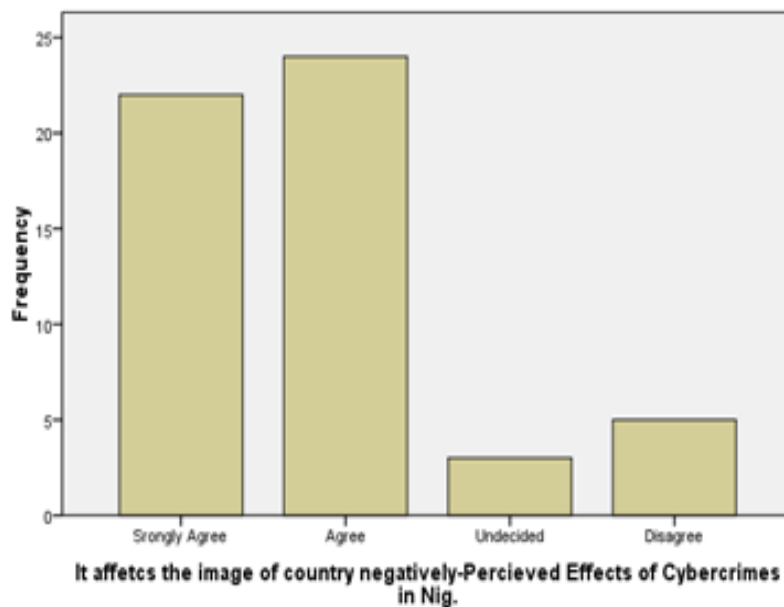


Fig. 4. Fig. 4- Effect of Cybercrime on the image of Nigeria [16]

V. GROWTH OF MOBILE ICT IN NIGERIA




As the world goes mobile, and anxiously desiring more portable and convenient devices, it is obvious from the trend of things that cybercrime will increase. According to current state of cybercrime report (2013), mobile computing levels reached new peaks in 2012. Worldwide smartphone shipments reached 671 million for the year an increase of almost 42% over 2011. As more of our personal and official lives move to the mobile device, cybercriminals continue to develop and refine their schemes to exploit mobile transactions and mobile apps. As the number of mobile users continues to grow globally, mobile transaction volume increases, organizations will continue to add new functionalities to the mobile channel. The report further stresses that global mobile transaction volume and value is expected to have an average 42% annual growth between 2011 and 2016. As users continue to move more of their

daily lives to their mobile devices, it is expected that cybercriminals will do the same and direct more attacks at this growing channel.



The last two years have witnessed the revolution of the information technology world due to massive development and deployment of mobile systems. Unfortunately the development of the sector has not witnessed corresponding increase in the implementation of appropriate security mechanisms to protect these systems. The lack of adequate awareness programs for users to understand the necessity of having to defend a system so valuable is another trouble on its own. Mobile systems have become so valuable and an extension of our personal lives and most of the time the closest companions we have.

Table 1 below is a display of the usage of mobile phones across the nations of the world. Nigeria occupies ninth position which indicates that Nigeria is competitively positioned among other nations[18].

TABLE I. LIST OF COUNTRIES BY NUMBER OF MOBILE PHONES

Rank	Country region	No. of mobile phones	Population	Phones per 100 citizens	Data evaluation date
-	World	6,800,000,000+	7,012,000,000	97	2013
01	 China	1,227,360,000	1,349,585,838	89.2	December 2013
02	 India	1,104,480,000	1,220,800,359	90.47	31 October 2013
03	 United States	327,577,529	350,000,000	93.6	June 2013

Rank	Country region	No. of mobile phones	Population	Phones per 100 citizens	Data evaluation date
04	 Brazil	271,100,000	201,032,714	136.45	December 2013
05	 Russia	256,116,000	142,905,200	155.5	July 2013
06	 Indonesia	236,800,000	237,556,363	99.68	September 2013
07	 Pakistan	130,583,076	188,854,781	69.18	December 2013
08	 Japan	121,246,700	127,628,095	95.1	June 2013
09	 Nigeria	114,000,000	165,200,000	69	May 2013
10	 Bangladesh	114,808,000	165,039,000	69.5	January 2014
11	 Germany	107,000,000	81,882,342	130.1	2013
12	 Philippines	106,987,098	94,013,200	113.8	October 2013
13	 Iran	96,165,000	73,973,000	130	February 2013
14	 Mexico	92,900,000	112,322,757	82.7	Dec. 2011
15	 Italy	88,580,000	60,090,400	147.4	Dec. 2013
16	 United Kingdom	75,750,000	61,612,300	122.9	Dec. 2013
17	 Vietnam	72,300,000	90,549,390	79	October 2013
18	 France	72,180,000	63,573,842	114.2	Dec. 2013
19	 Egypt	92,640,000	82,120,000	112.81	Egypt Ministry of Communications & IT, August 2013
20	 Thailand	69,000,000	65,001,021	105	2013
21	 Turkey	68,000,000	75,627,384	89.9	2013
22	 Ukraine	57,505,555	45,579,904	126.0	Dec. 2013
23	 Spain	55,740,000	47,265,321	118.0	Feb. 2013
25	 South Korea	52,510,000	48,580,000	108.1	2013
25	 Argentina	56,725,200	40,134,425	141.34	2013
26	 Poland	47,153,200	38,186,860	123.48	2013
27	 Colombia	49,066,359	47,000,000	104.4	2013
28	 South Africa	59,474,500	50,586,757	117.6	2013 GSM African Mobile Observatory report

Ran k	Country region	No. of mobile phones	Population	Phones per 100 citizens	Data evaluation date
29	 Algeria	33,000,000	35,000,000	94.2	2013
30	 Taiwan	28,610,000	23,197,947	123.33	September 2013

A. THE CONTRIBUTION OF MOBILE DEVICES TO CYBER INSECURITY

According to the 2012 Norton Cybercrime report, Cybercrime has gone mobile with the increase of mobile technologies and devices. In the report, it is stated that 2/3 of adults use a mobile device to access the internet which has increased mobile vulnerabilities by double the previous occurrences. Mobile vulnerabilities doubled in 2011 from 2010. Also, 31% of mobile users received a text message from someone they didn't know requesting that they click on an embedded link or dial an unknown number to retrieve a voicemail. In short, as consumers go mobile, so do cybercriminals. According to internet report, [11] the top 10 perpetrators of cybercrime are:

1. United States 65.4%
2. United Kingdom 9.9%
3. Nigeria 8.0%
4. Canada 2.6%
5. Malaysia 0.7%
6. Ghana 0.7%
7. South Africa 0.7%
8. Spain 0.7%
9. Cameroon 0.6%
10. Australia 0.5%

Nigeria occupies 9th position on mobile phone users and correspondingly occupies 3rd position on cybercrime table. The location independent operations of mobile devices alongside with the low cost of these devices make cyber security more difficult to implement. According to a survey carried out by [6] in 2013, one of the respondents claimed *"My view on the perpetrated point of crime is the home. This is due to the fact that even ordinary Nokia C3 can browse and with the reduction in the price of MB (data bundles), anybody who is interested in criminality can afford it."* It is therefore very clear that as Nigeria is celebrating progress in the technological world, cyber criminals are also celebrating an increase of their territory and impact.

B. CHALLENGES OF CYBER SECURITY PROVISIONING IN NIGERIA

Based on an interview with a Governmental Cyber security Agency, The National Information Technology Development Agency (NITDA) suggests that the major problem towards identifying cybercrime activities is Section

14 of the Nigerian Constitution, which states that *"no person shall be punished for a crime unless such crime is prohibited by written law and specific penalties are provided for the violation"*. As such; there is no cybercrime in Nigeria because there is no written law prohibiting any activities on the Internet. The agency reports that, the law enforcement agencies get evidences to ensure conviction through any other means apart from electronic evidence because there are no legal provisions or instruments available in the Nigerian Criminal Law that address cybercrime directly.

The agency contributes to efforts towards cyber security through capacity building workshops on cybercrime, public enlightenment programs, and interactive sessions with the Bankers' Committee and law enforcement agencies. They also sponsored the cybercrime bill, worked with the Law Reform Commission in updating the evidence act, and partners with the private sector in setting network security rules. In spite of all their efforts, they still face some challenges owing to the fact that they are not a law enforcement agency. Another great challenge is the alarmingly low awareness of the general populace as well as law enforcement agencies and policy makers on cybercrime. For instance, banks in Nigeria will hardly provide information to law enforcement agencies on cyber security threats they receive. Furthermore, the Agency is plagued with inadequate funding which makes it difficult for them to set up a forensic laboratory, equip and train personnel.

C. SUGGESTED SOLUTION TO CYBERCRIME BY STAKEHOLDERS

1) INDIVIDUAL NIGERIANS

It may be almost impossible to completely eliminate the incidence of cybercrime in Nigeria as criminals will always try to find a loophole to perpetrate their crimes either for financial gain, reputation or revenge. However, individual Nigerians will have to be more alert about the situation and put in place measures to secure themselves. Some of these include having strong passwords for their emails, systems and mobile devices. A good password should never consist of things people would easily guess including your name. It is advisable for a password to contain a mixture of lower and upper case characters, numbers and special characters. Also, debit (ATM) card PINS should not be written or stored in places people have access to and should be changed periodically. Since mobile devices and smartphones are being used for financial transactions, they should be guarded jealously and protected with a good antivirus and passwords to forestall intruders.

Individuals are also advised to avoid downloading supposedly free software from untrusted sites online as they tend to carry baggage along with them that are harmful in the long run.

2) ORGANIZATIONS AND PROFESSIONAL BODIES

Organizations, companies, firms and institutions that work with the internet and technological devices should take measures to protect themselves from attacks. Usually, cyber criminals are on the lookout for loopholes and the best thing would be to find them out internally and plug them before they are found out and damage is caused. Also, security policies and strategies should be put in place for all staff and guests as regards access to organization data and resources.

Different professional bodies like Nigerian Computer Society (NCS) and Computer Professionals of Nigeria (CPN) could partner with government agencies like Nigeria Communications Commission (NCC), National Information Technology Development Agency (NITDA) among others to create awareness and sensitize the Nigerian people on the menace of cybercrime and ways to avoid them.

3) NIGERIAN GOVERNMENT

Different nations have adopted different strategies to contend with crimes depending on their nature and extent. Certainly, a nation with high incidence of crime cannot grow or develop. This is because crime is the direct opposite of development. It leaves a negative social and economic consequence[32]. For Nigeria, a nation in the process of saving her face regarding cybercrimes, efforts should be directed at the sources and channels through which cybercrimes can be perpetrated - the most popular one being internet access points. The bill on cybercrime should be passed into law by the National Assembly. This will at least restrain the criminals to some extent[31].

Nigerian law enforcement agencies are basically technology illiterate; they lack computer forensics training and often result to conducting police raids on internet service sites with little information and imperfect strategies.

This becomes imperative because there is the need to do more in the area of legal framework. The traditional provisions on impersonation and criminal fraud as contained in Nigerian Criminal Code, Penal Code and AFF Act 2006 should be updated adequately take care of complex cases of phishing, identity theft and other electronic related economic crimes.

At the moment, some of the legislative frameworks we have in the country have not been enacted, including the EFCC Act of 2010, sponsored by Hon. Abubakar. Even before the EFCC Amendment Act of 2010, there were some other bills that were also drafted and have been sent to the National Assembly, part of which has not yet been enacted as well. In 2005, there was the Computer Security and Critical Infrastructure protection bill sponsored by another law maker, that bill has never being enacted. In 2008, the Cyber Security Agency bill was sponsored by Hon. Basse Etim, and has not been enacted and others like that which have not been enacted. There is therefore serious need for the law-makers to amend the EFCC Act for them to be able to arrest and prosecute cyber criminals in the most effective way [5].

Urgent Forensic training is therefore necessary for our law enforcement agencies and law makers. Cybercrime policy should be evidence-based and subject to rigorous evaluation to ensure efficiency and effectiveness. Therefore, concerted and coordinated efforts at the international level should be made to establish funding mechanisms to facilitate practical research and curb many types of newly emerging cybercrimes. It is, however, equally important to ensure that research be internationally coordinated and that research results be made widely available.

4) NETWORK OPERATORS

As technology is increasing rapidly and network operators are trying to gain customers in the country, the cost of internet services has come crashing down. As much as this is of immense benefits to the general populace, the network operators like MTN, Glo, Etisalat and Airtel should help to sensitize people and put in place policies to safeguard their clientele from attacks. Also, it is paramount they readily cooperate with law enforcement agencies when such crimes are reported and being investigated.

To prevent cybercrime committed through calls placed from mobile phones and smart devices, Network operators could develop a system that would request for user authorization before a call is allowed. This system would enable each registered user to create and change a Personal Identification Number (PIN) that would be required before a call connects and the account balance subsequently debited. This means that an unauthorized call cannot be placed from one's mobile number to perpetrate any crimes to implicate other individuals.

VI. PROPOSED CYBERCRIME INVESTIGATORY SYSTEM ARCHITECTURE

Fig. 5 below is a representation of the system architecture for the proposed Intelligent Cybercrime Investigatory System (ICIS). The ICIS will be a user friendly system that would allow various stakeholders in the Nigerian community to lodge their complaints related to suspected cybercrime activities or actual crimes. Once complaints are received, they will be forwarded to the appropriate bodies for investigation after which, reports will be given to complainant and other relevant bodies.

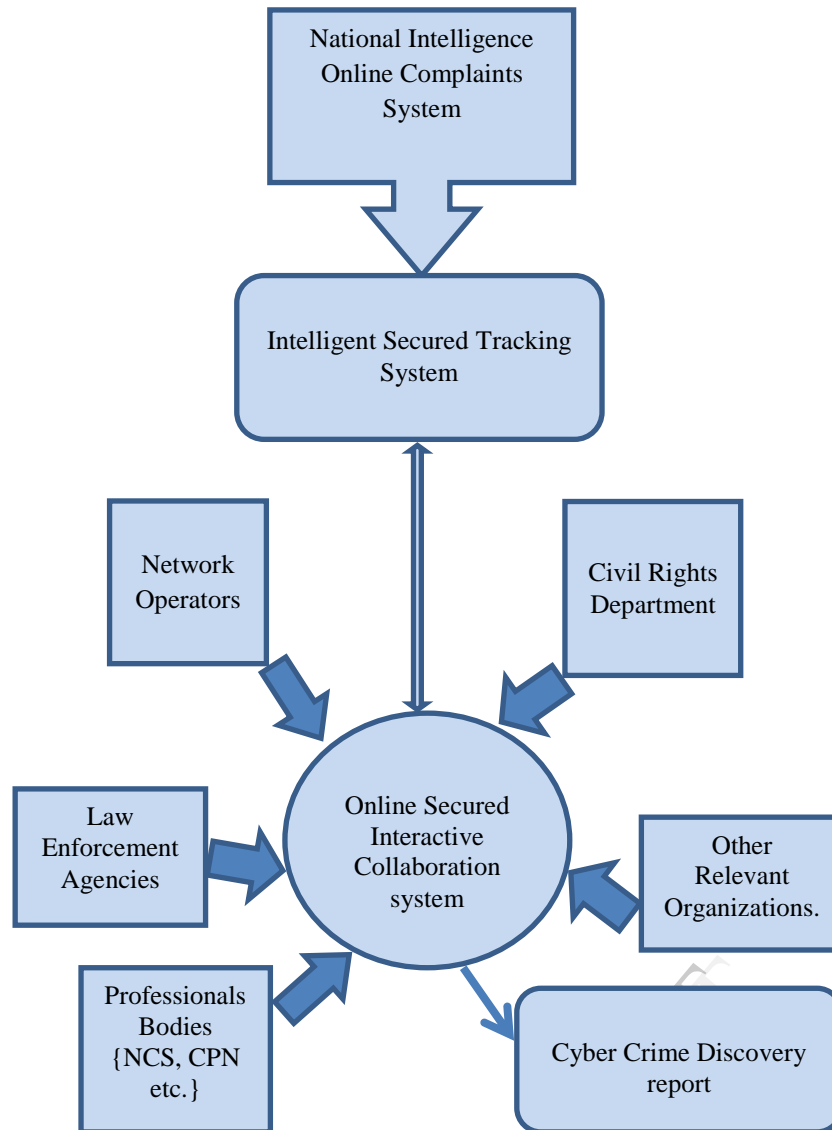


Fig. 5. Proposed Intelligent Cybercrime Investigatory System

1) National intelligent Complaint system

This is a system any user can immediately log on to from any internet enabled device to report cybercrime cases. This system is expected to have interfaces that will enable concerned individuals or organizations to supply information that is crucial to the crime in focus. This system captures the complaint and forwards it to the intelligent tracking System.

2) Intelligent Tracking System

This system is saddled with the responsibility of securing the information received from the complainant, dissemination of the details to the collaboration system.

3) Online Secured Collaboration System

The contributors/participatory units comprises of Network Operator/Internet Service Providers, Security agencies, Professional bodies. Relevant organizations and Civil right commission. The respective unit is expected to play their part in the investigatory process to discover the cybercrime perpetrators. The civil right commission is to make the right of individual concern is not be tampered with unjustifiably.

The report from this collaboration system will be a detail report that can be used to prosecute the offender.

VII. CONCLUSION

It is glaring that the advent and increase of mobile information and communication technologies has paved a smooth path for cybercrime being perpetrated in Nigeria. It is also clear that our current strategies, laws and efforts are inadequate to curb the situation on ground. However, the fight against cybercrime is not on any individual, law enforcement agency or government; rather, it has to be a collective and united effort of all. Though we might not be able to completely eradicate cybercrime, hand in hand we will be able to frustrate their work and ensure a fairly safe technological Nigeria. The government should immediately work on laws concerning cybercrime and provide the appropriate law enforcement agencies with required instruments to investigate and prosecute cybercrimes.

REFERENCES

- [1] 2012 Norton Cybercrime report, <http://www.norton.com/2012cybercrimereport> March 19, 2014
- [2] Aransiola J. O. and Asindemade S. O (2011), Understanding Cybercrime Perpetrators and the Strategies They Employ in Nigeria; *Cyberpsychology, Behavior, And Social Networking Volume 14, Number 12*, 2011 Mary Ann Liebert, Inc.DOI: 10.1089/cyber.2010.0307
- [3] Barry Collin (1997) The Future of Cyberterrorism, *Crime & Justice International Journal (March 1997): Vol#13 Issue #2*, <http://www.cjimagazine.com/archives/cji4c18.html?id=415> retrieved May 7, 2014
- [4] Cyber Advocate; Computer Crime <http://www.cyberadvocate.com/ComputerCrime.html> retrieved May 7, 2014
- [5] Emmanuel Ebeleke (2011) Why cybercrime thrives in Nigeria, by Ewelukwa; Vanguard News, <http://www.vanguardngr.com/2011/04/why-cyber-crime-thrives-in-nigeria-by-ewelukwa/> retrieved May 5, 2014
- [6] Folashade B. Okeshola & Abimbola K. Adeta (2013), The Nature, Causes and Consequences of Cyber Crime in Tertiary Institutions in Zaria-Kaduna State, Nigeria, *American International Journal of Contemporary Research Vol. 3 No. 9; September 2013*
- [7] General Introduction to Cybercrime (2013) <http://martinslibrary.blogspot.com/2013/08/general-introduction-to-cyber-crime.html>, 2013
- [8] Gyongyi (2005) Web Spam Taxonomy; *Proceedings of the First International Workshop on Adversarial Information Retrieval on the Web AIRWeb 2005* airweb.cse.lehigh.edu/2005/proceedings.pdf; retrieved May 7, 2014
- [9] Hassan A. B., Lass F. D. and Makinde J (2012) Cybercrime in Nigeria: Causes, Effects and the Way Out; *ARN Journal of Science and Technology ©2011-2012.VOL. 2, NO. 7, August 2012 ISSN 2225-7217* <http://www.ejournalofscience.org> 626.
- [10] Hemraj Saini, Yerra Shankar Rao, T.C.Panda (2012) Cyber-Crimes and their Impacts: A Review. *International Journal of Engineering Research and Applications (IJERA)* ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 2, Mar-Apr 2012, pp.202-209 202
- [11] Internet Crime Report, (2009), *Internet Crime Complaint Centre*; http://www.ic3.gov/media/annualreport/2009_ic3report.pdf retrieved April 25, 2014
- [12] Justin Plot (2010) Top Five Computer Crimes & How to Protect Yourself From Them <http://www.makeuseof.com/tag/top-five-computer-crimes-protect/> retrieved May 7, 2014
- [13] K. Jaishankar(2008); Identity Related Crime In The Cyberspace: Examining Phishing And Its Impact, *International Journal of Cyber Criminology (IJCC) ISSN: 0974 – 2891 January-June 2008, Vol 2 (1): 10–15*
- [14] Knowledge@Wharton (2013), Mobile Devices and Cybercrime: Is Your Phone the Weakest Link?; *Wharton University of Pennsylvania*, <http://knowledge.wharton.upenn.edu/article/mobile-devices-and-cybercrime-is-your-phone-the-weakest-link/> retrieved April 24, 2014
- [15] Maitanmi Olusola, Ogunlere Samson, Ayinde Semiu and Adekunle Yinka(2013). Impact of Cyber Crimes on Nigerian Economy *The International Journal Of Engineering And Science (IJES)* Volume| 2 Issue 4 Pages 45-51 ISSN(e): 2319 – 1813 ISSN(p): 2319 – 1805 www.theijes.com
- [16] Maitanmi Olusola, Ogunlere Samson, Ayinde Semiu, & Adekunle Yinka (2013); Cyber Crimes and Cyber Laws in Nigeria *The International Journal Of Engineering And Science (IJES) ||Volume||2 ||Issue|| 4 ||Pages|| 19-25||2013|| ISSN(e): 2319 – 1813 ISSN(p): 2319 – 1805*
- [17] Mbaskei Martin Obono (2008); Cybercrimes: Effect on Youth Development; <http://www.genius.org/member/profile.php/id/1138/post/1007> retrieved May 7, 2014
- [18] Mohit Kumar(2011) 3G technology will increase cybercrime Wednesday, February 16, 2011 by http://en.wikipedia.org/wiki/List_of_countries_by_number_of_mobile_phones_in_use
- [19] Oladeji, Matthew Olaniyi(2011), New Media and Revolutionary Changes: Challenges of Cybercrimes In Nigeria; *POLYCOM Journal (FBCS)* Vol. 15 No. 2 2011
- [20] Overview of Cyber security, Recommendation International Telecommunications Union, Telecommunications Standardization Sector, ITU -T X.1205 (04/2008), <http://www.itu.int/ITU-T/recommendations/rec.aspx?id=9136>
- [21] Parker, D (1983): Fighting Computer Crime, Charles Scribner's Sons, United States,
- [22] Roderic Broadhurst, Peter Grabosky, Mamoun Alazab, Brigitte Bouhours, and Steve Chon (2013) Organizations and Cybercrime; ANU Cybercrime Observatory; *International Journal of Cyber Criminology* https://www.academia.edu/5196452/Organizations_and_Cybercrime
- [23] Saul Hansell (2007); Social network launches worldwide spam campaign New York Times retrieved May 7, 2014
- [24] Sesan O., Soremi B. and Oluwafemi B Economics Cost of Cybercrime in Nigeria, Cyber Stewards Network Project, Munk School of global affairs, University of Toronto
- [25] The Cost of Cybercrime(2011), A Detica Report in Partnership with the Office of Cyber Security and Information Assurance in the Cabinet Office, http://www.baesystemsdetica.com/uploads/press_releases/THE_COST_OF_CYBER_CRIME_SUMMARY_FINAL_14_February_2011.pdf
- [26] United Nations (2004). A More Secure World, Our Shared Responsibility: Report of the High-Level Panel on Threats, Challenges, and Change (Online Report). http://www.un.org/en/events/pastevents/pdfs/secure_world_exec_summary.pdf Retrieved May 7, 2014
- [27] United Nations (2005). UN recommendations on fighting cybercrime. <http://www.crime-research.org/news/13.05.2005/1225/> Retrieved May 6, 2014.
- [28] What is Cyber Security (2013) <http://www.itgovernance.co.uk/what-is-cybersecurity.aspx>, February 10, 2014
- [29] William L. Tafoya, Ph.D. (2011) Cyber Terror; *FBI Law Enforcement Bulletin* <http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/november-2011/cyber-terror>; retrieved May 7, 2014
- [30] Yip, M. (2011); An investigation into Chinese cybercrime and the applicability of social network analysis. *University of Southampton EPrint, 1-4*. http://eprints.soton.ac.uk/272351/1/139_paper.pdf Retrieved May 7, 2014
- [31] F. Wada, G.O. Odulaja(2012); Assessing Cybercrime and its Impact on E-Banking in Nigeria Using Social Theories. *African Journal of Computing & ICT Vol4. No 3. Issue 2*
- [32] Sylvester Linn (2001); The Importance of Victimology in Criminal Profiling. <http://isuisse.ifsrance.com/emmaf/base/impvic.html>