Imperative of Cyber Ethics Education to Cyber Crimes Prevention and Cyber Security in Nigeria

K.N. Igwe
Lecturer, Department of Library and Information Science,
Akanu Ibiam Federal Polytechnic Unwana,
Ebonyi State, Nigeria.
knigwe@yahoo.com

Ahiaoma Ibegwam, PhD
University Librarian, The University Library
Michael Okpara University of Agriculture
Umudike, Abia State, Nigeria
anibegwam@yahoo.com

ABSTRACT: ***Arising from digital culture that is fast developing and being used for service delivery in all sectors of the Nigeria's economy such as e-banking, e-businesses, e-education, e-government, and the likes, which led to the emergence of sophisticated cybercrimes threatening the cyber space, this paper advocated for cyber ethics education as a means of preventing cybercrimes. This is in addition to the cybercrimes bill that is being awaited to become law for the punishment of cyber criminals. It examined the growth of digital operations and services in Nigeria, traced the emergence of cybercrimes in the country and described cyber security and protection. The current state of cyber security and protection in Nigeria, the concept of cyber ethics, and the imperative of cyber ethics education for prevention of cybercrimes and security of cyber space in Nigeria were also discussed. The paper concluded that the introduction of cyber ethics education will go a long way in addressing the menace of cybercrimes in Nigeria. Some recommendations, among which is the articulation and integration of cyber ethics education in the programme of all levels of education in Nigeria, were made.***

KEYWORDS: ***Cyber Crimes, Cyber Ethics Education, Cyber Security, Cyber Space, Nigeria.***

I. INTRODUCTION

Developments in information and communication technologies (ICTs) such as computer systems, multimedia tools, telecommunication facilities, electronic gadgets, the Internet and other digital devices are inventions that are shaping the 21st century. Among the ICTs, the Internet acts as a unifying resource that facilitates the information communication and dissemination activities of the other technologies. From its emergence in 1967 till date, the Internet with its sophisticated applications such as the World Wide Web, electronic mail, media platforms, social networking sites, and others have contributed significantly to the advancement of individuals in different fields of endeavors. This significant contribution may appear positive to many, whereas others will see it from the negative perspective. But, suffice it to say that it is rare to see any activity or engagement of man in this globalization era that is not associated with the information and communication systems of the online environment, i.e. the Internet. This include the areas of education, governance, politics, business, agriculture and the likes, the use of the Internet is involved, basically for easy communication and faster delivery of services in Nigeria. This aligns with the position of Ibikunle and Eweniyi [15] who submit that cyber space has transformed the ways we communicate, travel, power our homes, run our economy, and obtain government services.

Meanwhile, the involvement of Internet in various operations and services in the country by both public and private sectors require protection and security, due to emergence of cybercrimes. The rise of technology and online communications has not only produced a dramatic increase in the incidence of criminal activities, but has also resulted in the emergence of what appears to be a new variety of criminal activities [26]. Both the increase in the incidence of criminal activities and the emergence of new varieties of criminal activity pose challenges for legal systems, law enforcement agencies, regulatory agencies and stakeholders [10].

It also has implications for the peaceful co-existence of the Nigerian state. This emphasizes the need for cyber security, not only for protection of digital operations and services in the country but also for the continuity of the system which is driven by efficiency using digital technologies. However, efforts so far at curbing the menace of cybercrimes seem not to be yielding positive results, signifying the urgent need of bringing knowledge of cyber ethics to all and sundry in the Nigerian society. This paper examines the growth of digital operations and services in Nigeria, emergence of cybercrimes in the country, cyber security and prevention, state of cyber security and protection in Nigeria, concept of cyber ethics, and the imperative of cyber ethics education for prevention of cybercrimes and security of cyber space in Nigeria.

II. GROWTH OF DIGITAL OPERATIONS AND SERVICES IN NIGERIA

At present, there is much concentration and heavy reliance on the Internet for operations and services by both public and private sectors of the Nigerian economy. This is more pronounced in businesses, education, government, and other booming sectors of the society. For instance, in business, there are e-banking operations and services, e-commerce, online marketing of products and services, online shopping, and online subscriptions, among other online transactions.

In education, there are issues of online advertisements, sale of admission forms, online admissions, online payment of school fees, online transcripts processing system and e- meetings, e-academic board meetings, online call for papers and chapters, open access scholarly communication and general online publications [7]. There are also online universities, e-learning institutions; online educational programmes at certificate, diploma and degree levels, and learning management systems, automation of library routines and digitization of print materials especially grey literature in libraries and development of institutional repositories, among others.

In the case of the government, the focus is now channeled to e-governance, which is expected to be the best practice for the future of all nations [7]. E-Governance is all about the use of ICTs especially the Internet and its resources to support governance, for the delivery of information and services to the citizens. It involves the use by government agencies of ICTs to improve and transform relations with citizens, businesses, other arms of government, and even the international community, for increased transparency, greater convenience, reduced corruption, revenue growth and reduced cost of running government [3] [13]. E-services, e-management, e-administration, e-democracy and e-commerce are the four dimensions of e-governance [3].

Nigerian government is making effort towards facilitating digital economy and promoting e-governance in the country. This can be seen through the initiatives and programmes of various ministries, departments and agencies (MDAs) of the government such as Ministry of Communications Technology (MCT), Nigerian Communication Commission (NCC), National Information Technology Development Agency (NITDA), and others. Using the MCT as example, it has engineered the final draft of a comprehensive National ICT policy in 2012, through the harmonization of all existing policies in the ICT sector. The ministry has embarked on initiatives to deploy ICT to drive transparency and efficiency in governance and public service delivery as well as productivity and citizen engagement [4].

The 'Getting Government Online' initiative of the ministry is geared at ensuring that government deploys technology as a mechanism to transform the way government operates and enhance the effectiveness of government service delivery for the benefit of its citizens. This has led to the implementation of two flagship projects, namely the Government Service Portal (GSP) and Government Contact Centre (GCC). The Government Service Portal (GSP) provides a single window technology access by citizens and other stakeholders to government services being provided by various Ministries Departments and Agencies (MDAs) of government. It is multi-featured and includes collaborative channels that deliver core content

management capabilities. The primary objectives of deploying GSP are to create a single point of entry to Federal Government services, enhance accountability and improve the delivery and quality of public services through technology-enabled civic engagements (mobile technology, Facebook, Twitter, Interactive Mapping, Blogs, Wiki, etc.), transform government processes to increase public administration efficiency, increase end-user productivity by integrating many different services or data access paths of MDAs – under a consistent presentation standard as well as mainstream some of the government's non-sensitive datasets on the portal. The phase one of GSP included the automation of government processes in many MDAs and online payment on the Government Service Portal.

The ministry is also setting up Government Contact Centers (GCC), which will facilitate efficient response to citizen requests through a two-tier response approach. The Contact Centre, which will be located in the six geopolitical zones of the country, is planned to house robust databases. It should be noted that before the creation of the MCT in 2011, most MDAs did not have domain names. But in line with its mandate to improve the quality of public service delivery, all websites of ministries across the federation have been migrated to a standard domain name at '.gov.ng' [4].

NITDA is also making significant contributions to e-government in Nigeria. With its establishment in 2001, the agency was designated as Nigeria's institution for the implementation of the then national information technology policy of 2001 as well as flagship for the implementation of e-government in Nigeria. It has established over 400 Rural Information Technology Centers (RITC) in some communities across the country, and the process is still ongoing, to make the Internet and e-government services accessible to the rural dwellers. The establishment of the centers was informed by the need to provide a community-based platform for youth empowerment through e-learning and capacity building in ICT, as well as community-based training in ICT-enabled outsourcing, thereby promoting equitable access to assets [8].

III. EMERGENCE OF CYBER CRIMES IN NIGERIA

The cyberspace has ushered in new opportunities and security challenges, as wars are now fought and won in the cyberspace, which has also become a highway for fraud and other crimes. With heavy dependence on the Internet for operations and services by establishments and institutions in Nigeria, there are several cases of cybercrimes and cyber threats existing in the country *and beyond.* Various terms are used interchangeably to describe what cybercrimes are all about. They include computer crime, computer-related crime, digital crime, information technology crime, Internet crime, virtual crime, e-crime, and net crime. Cybercrimes were categorized into two at the tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders [26], as follows:

- Cybercrime in a narrow sense is any illegal behavior directed by means of electronic operations that targets the security of computers systems and the data processed by them;
- Cybercrime in a broader sense is any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network.

In the Council of Europe's Convention on Cybercrime, cybercrime is used as an umbrella term to refer to an array of criminal activities including offenses against computer data and systems, computer-related offenses, content offenses, and copy-right offenses [26]. The convention covers cybercrime in four main categories:

- Offenses against the confidentiality, integrity, and availability of computer data and systems such as illegal access, illegal interception, data or system interference, and illegal devices;
- Computer related offenses like computer-related forgery and computer-related fraud;

- Content-related offenses (e.g. child pornography);
- Offenses related to infringements of copyright and related rights.

Cybercrime means an aggregate of all illegal activities where the computer, computer systems, information network or data is the target of the crime and those known illegal activities or crime that are actively committed through or with the aid of computer, computer systems, information network or data, in the online environment. Such cybercrimes are explained below [9] [36] [15]:

- Hacking: Hackers make use of the weaknesses and loop holes in operating systems to destroy data and steal important information from victim's computer. It is normally done through the use of a backdoor program installed in a computer. A lot of hackers also try to gain access to resources through the use of password hacking software. Hackers can also monitor what one does on his/her computer and can also import files on someone's computer. A hacker could install several programs to one's system without his/her knowledge. Such programs could also be used to steal personal information such as passwords and credit card information. Important data of a company can also be hacked to get the secret information of the future plans of the company.
- Cyber-theft: Cyber-theft is the use of computers and communication systems to steal information in electronic format. Hackers crack into the systems of banks and transfer money into their own bank accounts. This is a major concern, as larger amounts of money can be stolen and illegally transferred. Credit card fraud is also very common. Most of the companies and banks don't reveal that they have been the victims of cyber -theft because of the fear of losing customers and shareholders. Cyber-theft is the most common and the most reported of all cyber-crimes. Cyber-theft is a popular cyber-crime because it can quickly bring experienced cyber-criminal large cash resulting from very little effort.
- Viruses and worms is a very major threat to normal users and companies. Viruses are computer programmess that are designed to damage computers. It is named virus because it spreads from one computer to another like a biological virus. A virus must be attached to some other program or documents through which it enters the computer. A worm usually exploits loop holes in software or the operating system.
- Spamming: This involves mass amounts of email being sent in order to promote and advertise products and websites. Email spam is becoming a serious issue amongst businesses, due to the cost overhead it causes not only in bandwidth consumption but also to the amount of time spent downloading/ eliminating spam mail. Spammers are also devising advanced techniques to avoid spam filters, such as permutation of the emails contents and use of imagery that cannot be detected by spam filters.
- Financial fraud: These are commonly called "Phishing' scams, and involve a level of social engineering as they require the perpetrators to pose as a trustworthy representative of an organization, commonly the victim's bank.
- Identity theft, Credit Card theft, fraudulent e-mails (Phishing): Phishing is an act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in order to scam the user into surrendering private information that will be used for identity theft.
- Cyber harassment: This is electronically and intentionally carried out by threatening acts against individuals. Such acts include cyber-stalking.
- Cyber laundering: Cyber laundering is an electronic transfer of illegally-obtained money with the goal of hiding its source and possibly its destination.
- Website Cloning: One recent trend in cyber-crime is the emergence of fake 'copy-cat'

web sites that take advantage of consumers what are unfamiliar with the Internet or who do not know the exact web address of the legitimate company that they wish to visit. The consumer, believing that they are entering credit details in order to purchase goods from the intended company, is instead unwittingly entering details into a fraudster's personal database. The fraudster is then able to make use of this information at a later stage, either for his own purposes or to sell on to others interested in perpetrating credit card fraud.

In addition, there are also emerging cyber tricks in Nigeria [9] [15]. They include:

- Beneficiary of a Will Scam: The cyber criminals send e-mail to claim that the victim is the named beneficiary in the will of an estranged relative and stands to inherit an estate worth millions.
- Online Charity: Another aspect of e-crime common in Nigeria. This is a situation where fraudulent people host websites of charity organizations soliciting monetary donations and materials to these organizations that do not exist. Unfortunately, many unsuspecting people have been exploited through this means.
- Next of Kin Scam: Collection of money from various banks and transfer fees by tempting the victim to claim an inheritance of millions of dollars in a Nigerian bank belonging to a lost relative.
- The "Winning Ticket in a Lottery one Never Entered" Scam: These scams lately include the United State Department's green card lottery.
- Bogus Cashier's Check: The victim advertises an item for sale on the Internet, and is contacted.
- Internet Service Time Theft: Whiz kids in Nigeria have developed means of connecting Cyber Cafes to Network of some ISPs in a way that will not be detected by the ISPs and thereby allow the Cafes to operate at no cost.
- Lottery scam: allowing users believe they are beneficiaries of an online lottery that is in actual fact a scam.

Cyber Crimes Bill (2013), which is yet to be passed into law, outlines the following offences as cybercrimes in Nigeria:

- offences against critical national information infrastructure;
- unlawful access to a computer;
- unlawful interception of communications;
- unauthorized modification of computer program or data;
- system interference;
- misuse of devices;
- computer related forgery;
- computer related fraud;
- identity theft and impersonation;
- child pornography and related offences;
- cyber stalking;
- cybersquatting;
- cyber terrorism;
- racist and xenophobic offences;
- attempt, conspiracy, aiding and abetting; and
- Corporate liability.

Instances and cases of cybercrimes that are peculiar to Nigeria and committed by Nigerians are described by [9] [15]. *The* instances reported ranges from fake lotteries to internet scams, and include:

- Elekwe: a chubby-faced 28-year-old man made a fortune through the scam after two years of joblessness despite having diploma in computer science. He was lured to Lagos from Umuahia by the chief of a fraud gang in a business centre. He has three sleek cars and two houses from his exploits.
- In July 2001, four Nigerians suspected to be operating a "419" scam on the internet to dupe unsuspecting foreign investors in Ghana were arrested by security agencies. Their activities are believed to have led to the loss of several millions of foreign currencies by prospective investors.
- Two young men were recently arrested after making an online purchase of two laptops advertised by a woman on her website under

false claims. They were arrested at the point of delivery by government officials.

- Mike Amadi. was sentenced to 16 years imprisonment for setting up a website that offered juicy but phony procurement contracts. The man impersonated the EFCC Chairman, but he was caught by an undercover agent posing as an Italian businessman.
- The biggest international scam of all was committed by Amaka Anaejemba who was sentenced to 2½ years in prison. She was equally ordered to return $25.5 million of the $242 million she helped to steal from a Brazilian bank.
- Another Internet scam case was reported on the Sunday PUNCH newspaper of July 16, 2006 involving a 24-year-old Yekini Labaika of Osun State origin in Nigeria and a 42-years-old nurse of American origin, by name Thumbelina Hinshaw, in search of a Muslim lover to marry. The young man deceived the victim by claiming to be an American Muslim by the name, Phillip Williams, working with an oil company in Nigeria and he promised to marry her. He devised dubious means to swindle $16,200 and lots of valuable materials from the victim. The scammer later was sentenced to a total of 19½ years having been found guilty of eight-counts against him. Incidences like these are on the increase. Several young men unabated are still carrying out these illegal acts successfully, ripping off credulous individuals and organizations.
- Recently, a report indicated that Nigeria is losing about $80 million yearly to software piracy. The report was the finding of a study conducted by Institute of Digital Communication, a market research and forecasting firm, based in South Africa, on behalf of Business Software Alliance of South Africa.
- The American National Fraud Information Centre reported Nigerian money offers as the fastest growing online scam, up to 90% in 2001. The Centre also ranked Nigerian cyber-crime impact per capita as being exceptionally high.
- In 2013 alone, Nigerian banks lost a whooping sum of NGN40 billion to online fraud cases, an indication of high rate of cybercrime in Nigeria [34].
- Those involved are between 18-25 years mostly resident in the urban centres. The internet has help in modernizing fraudulent practices among the youths. Online fraud is seen as the popularly accepted means of economic sustenance by the youths involved. The corruption of the political leadership has enhanced the growth of internet crime subculture. The value placed on wealth accumulation has been a major factor in the involvement of youths in online fraud (Adebusuyi, 2008).

The above are few cases reported in the media. There are many others situations involving financial institutions and large corporate establishments that are not reported due to fear of the institutions from losing their customers and supportive stakeholders.

A. CYBER SECURITY AND PROTECTION

Cyber Security and protection is concerned with making cyberspace safe from cyber threats for operations and delivery of services. These threats involve malicious use of ICTs either as a target or as a tool by a wide range of e-criminals. Cyber Security as a term refers only to protection and security of networks and systems – computers, electronics gadgets and ancillary devices. Typical cyber security issues include confidentiality of information, integrity of systems and survivability of information networks. Major objective of cyber security includes protection of system/networks against un-authorized access and data alteration from within, and defense against intrusion from outsiders. Cyber security refers to:

- a set of activities and other measures, technical and non-technical, intended to protect computers, computer networks, related hardware and software devices, and the information they contain and communicate, including software and data,

as well as other elements of cyberspace, from all threats, including threats to national security;
- the degree of protection resulting from the application of these activities and measures; as well as
- The associate field of professional endeavor, including research and analysis, aimed at implementing those activities and improving their quality.

The mission of cyber security is closely related to information security because information security lies at the heart of securing cyber space. Olayiwola describes information security as protecting information and information systems from un-authorized access, use, disclosure, disruption, modification and destruction. Cyber security is in line with protecting data, information, systems, and assets on the cyber space from those who would wish to misuse them; thus with emphasis on three elements - confidentiality, integrity, and availability (CIA) of information. 'Confidentiality' refers to the protection of information from disclosure to unauthenticated parties i.e. ensuring that information is accessible to only those authorized to have access, while 'integrity' refers to the protection of information from unauthorized changes i.e. safeguarding the accuracy and completeness of information and processing methods. 'Availability' means the information should be available to authorized parties when requested i.e. ensuring that authorized users have access to information and associated assets when required [27] [26].

Sometimes, 'accountability', is the requirement that the actions of an entity be uniquely traceable to that entity. That is, accountability underscores the fact that the responsibility or inability of information custodians, information providers, users and other parties concerned with the security of information should be made explicit within the context of the overall organisation's objectives (Kalusopa, 2008; [26]. The key goal of modern information security has, in effect, become to ensure that systems are predictably dependable in the face of all sorts of malice and particularly in the face of denial-of-service attacks, of which cyber security issues are aligned in that direction.

B. STATE OF CYBER SECURITY AND PROTECTION IN NIGERIA

Within and outside the shores of Nigeria, the ugly situation of cybercrimes is causing embarrassment for citizens at both social and business gatherings. These cybercrimes and other internet abuses have been described as hindrance to development in Nigeria [12]. Meanwhile, some efforts are ongoing to tackle the menace of cybercrime in the country. At the first National Cyber Security Forum in Lagos, the National Security Adviser, Col. Sambo Dasuki said the abnormal trend of cybercrime is denting Nigeria's image, and that the cyber terrorists have succeeded in changing the way Nigerians see and relate with one another. According to Dasuki, "Realizing the importance of cyber space, the Federal Government of Nigeria has designated cyber security as a national security priority with the office of the National Security Adviser (ONSA) stepping up efforts towards meeting the challenge by working in close collaboration with all stakeholders to ensure a safer and more secure cyberspace." [6].

On its part, the NCC has been involved in stemming the tide of cybercrimes in the country. Explaining how the commission has been combating cybercrimes in line with global regulatory best practices, the Executive Vice Chairman, Eugene Juwah said the NCC, created a new department "New media and information strategy", about three years ago. The department is responsible for all issues of information security and capacity building in information technology through the accelerated digital awareness program for tertiary institutions (ADAPTI program).

The commission is fully involved in the formulation of the national cyber security bill and other similar initiatives, coordinated by the office of the national security adviser. In addition to capacity building, NCC has improved on its equipment authorization process through which security loopholes in telecoms hardware and software are checkmated. It therefore ensures that security standards are fully implemented by manufacturers in the design and fabrication stage of all telecoms equipment imported into the country. Juwah further noted that there is need for collaborative efforts by relevant government agencies

towards the implementation of domain name system security extension (DNSSEC) on the top level of domain name system in order to address identified vulnerability of the DNS system. "This DNSSEC provides an additional level of security that can strengthen trust on the internet by helping to protect browsers from redirection to fraudulent websites through effective integrity and authenticity checks on DNS protocols." [32] [34].

Legal frameworks for supporting cyber security programmes seem to be a challenge in Nigeria. The Advance Fee Fraud and other Related Offences Act of 2006, the Money Laundering Act of 2004 section 12(1) (c) - (d), the Economic and Financial Crime Commission (EFCC) Establishment Act of 2004, and the Evidence Act of 1948 are the only available provisions in the Nigeria criminal law that may be used to convict perpetrators of cybercrime. Registration of all prospective cyber cafes and public enlightenment are used by law enforcement agencies to check cybercrimes and threats [26].

Investigation revealed that some of the challenges encountered by law enforcement agencies such as EFCC, Nigeria Police Force (NPF), and NITDA in the course of ensuring cyber security include lack of adequate provisions for cybercrime in the criminal code, non-registration of SIM cards and Internet modems, non-cooperation of Internet Service Providers (ISPs) and telecoms service providers, insufficiently trained personnel and inadequate number of trained personnel as well as lack of opportunities for regular training.

Also of relevance are the inadequate knowledge of cybercrime issues and technicalities by Nigerian Judges, and the duplication of duties and responsibilities among law enforcement agencies toward cybercrime activities [26]. Other challenges hindering the performance of law enforcement agencies in combating cybercrime in Nigeria are as follows:

- There is no existing law to adequately address challenges of technology with regards to security breaches and online crime. Thus, absence of laws (legislation) to address online criminality makes it impossible to prosecute offenders;
- the absence of a national Internet gateway for Nigeria has made it difficult to isolate and determine the real criminal activities that could be ascribed to Nigeria on the Internet;
- Lack of national framework and infrastructure for the protection and management of electronic payment fraud and other cybercrimes. Therefore, no single law enforcement agency in Nigeria can bear the cost of system infrastructure;
- there is unavailability of reliable data on the level and extent of cybercrime damages in the country;
- some personnel of the Nigerian law enforcement agencies are not ICT compliant; and lack of computer forensic laboratory at the branches of the NPF and other law enforcement agencies to investigate and analyses cybercrime related issues; and
- Nigeria law enforcement agencies do not have a centralized government body that collects and publish cybercrime statistical reports [26].

At present, there is a bill for an act to provide for the prohibition, prevention, detection, response and prosecution of cybercrimes and other related matters, before the national assembly. The objectives of this proposed Act are to:

- provide an effective and unified legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria;
- ensure the protection of critical national information infrastructure; and
- Promote cyber security and the protection of computer systems and networks, electronic communications; data and computer programs, intellectual property and privacy rights [11].

The Cyber security Bill, if passed into law, will provide a comprehensive framework that will initiate a more strategic conversation on its requirements and what organizations need to do to be compliant. It is also expected to provide more adequate basis for law enforcement agencies to prosecute cyber criminals. The Federal Executive Council (FEC) in August 2013 approved the content of the bill and passed it to the National Assembly for enactment into law. The bill had gone through second reading and was expected to be passed into law in 2014, but experts say the prospect of it being passed into law this year appears gloomy [35].

Meanwhile, as the passage of the bill into law is being awaited, there is still need for an educational programme that will contribute in re-directing the mindset of Nigerians to morality in cyber space, especially children and the youth, thereby preventing the occurrence of cybercrimes and contributing to cyber security. This is where cyber ethics education comes in.

C. CONCEPT OF CYBER ETHICS

Ethics as observed by [28] has no univocal definition. Various scholars from various backgrounds have attempted to define it based on their perspectives, convictions and standpoints. In presenting an etymological definition of ethics Ozumba [29] says the term comes from the Greek word "ethos", which means "customary". This makes ethics equivalent to morals or morality. Iwe [19] defines ethics as "a systematic study of the principles governing human conduct by human reason from the point of view of the right and wrong, the ought and the ought not". He further sees ethics as "the orderly and logical applications of acknowledged moral principles to a given way of life".

Ethics is a branch of philosophy that is concerned with human conduct, more specifically the behavior of individuals in society, deals with what is considered to be right and wrong, studies morals and values, as well as involves systematizing, defending, and recommending concepts of right and wrong behavior [30]. In research process for instance, ethical issues are given due attention, as researchers are expected to be objective, logical and honest, and completed research must be accurately reported and disseminated [5]. Such ethics applied to the internet or cyber space led to the concept of cyber ethics.

Cyber ethics is an aspect of information ethics [25] [20] Mabawonku [21] posits that information ethics refers to the responsible creation and use of information in a variety of formats. It is about the content of data or information and how it is to be used. She noted that ethical considerations pervade the cycle of creation, generation, management, evaluation and dissemination of information by information professionals and indeed, the society at large. That "information professionals have the responsibility in the society, to ensure that in the process of locating, retrieving, using and providing access to information, the moral implications of all activities are understood and considered".

Cyber ethics is really about social responsibility in cyberspace. It involves a system of standards that prescribe morality and immorality in cyberspace, signifying the preservation of freedom of expression, intellectual property, and privacy [30]. Another definition sees cyber-ethics is the discipline of using appropriate and ethical behaviors and acknowledging moral duties and obligations pertaining to online environments and digital media [16].

Therefore, all ethical issues, which applies in computer ethics and information ethics are also applicable to cyber ethics, but only focused on its application to the Internet. Some cyber ethical issues include plagiarism, copyright, hacking, fair use; file sharing, online etiquette protocols, posting incorrect/inaccurate information, cyber-bullying, stealing or pirating software, music, and videos, online gambling, gaming, and internet addiction. Others are privacy, security, electronic monitoring of employees, collection and use of personal information on consumers, and identity theft.

In sum, the basic rule in the cyber world is that individuals should not do something in cyber space that would be considered wrong or illegal in everyday life. When determining online responsible behaviors, individuals should consider the following:

Do not use rude or offensive language.

- Do not be a bully on the Internet. This means that people should not be called names, lied about, sent embarrassing pictures of them, or do anything else to try to hurt them.
- Do not copy information from the Internet and claim it as yours.
- Adhere to copyright restrictions when downloading material, including software, games, movies, or music from the Internet.
- Do not break into someone else's computer.
- Do not use someone else's password.
- Do not attempt to infect or in any way try to make someone else's computer unusable.

Knowledge of cyber ethics and its practice is required by individuals in different sectors of the economy. In scholarly communication which is associated with tertiary institutions and research institutes, it is a necessity for scholars especially those that have bias for open access publishing. Information synthesis, citation and referencing, issue of plagiarism, copyright infringement implications, and the likes as applicable to the online environment are cyber ethical issues which open access scholars should be conversant with. In e-banking and other e-businesses cyber ethics knowledge is also required for online transactions. What of e-governance that involve e-service, e- management, e-democracy and e-commerce? application of cyber ethics is also required, among others. These are justifications for cyber ethics education in Nigeria.

D. CYBER ETHICS EDUCATION FOR PREVENTION OF CYBER CRIMES AND SECURITY OF CYBER SPACE IN NIGERIA

Education is all about inculcating the right knowledge and attitudes in people for successful living. It involves teaching, learning and development of individuals that will be useful to the society. Cyber ethics education will be aimed at inculcating knowledge of responsible behavior in man when using the online environment. Cyber ethics education can be described as instructional programme that is aimed at inculcating in individuals knowledge of ethical standards and issues required while using the cyber space in order to avoid acts that constitute cybercrimes, which are punishable by law. Such educational programme is also expected to familiarize the beneficiaries (i.e. students or other participants) with various forms of cybercrimes, threats and tricks employed by cyber criminals for their illegal activities as well as how to respond accordingly to avoid being victims of cybercrime.
Cyber ethics education is very important in Nigeria as it will go a long way in integrating moral and responsible values in children, the youth and even the adults while using the Internet and navigating on the cyber space. In fact, cyber ethics education is a must according to Mintz [23]. Take for instance, the various e-government initiatives, cashless policy of the Central Bank of Nigeria, e-banking and e-businesses as well other online-based transaction programmes of public and private organizations in the country which require the knowledge of cyber. All kinds of cybercrimes that are punishable by law should be part of our educational system in Nigeria.

Eze pointed out that “as the country integrates electronic payment system into its financial institutions [15]; a step that is expected to accelerate the nation’s e-commerce growth, the negative impact of cybercrime on businesses, and the absence of appropriate laws to guarantee the legality of online transactions, continue to create fear in the mind of users and potential online users”. With the continuous rise and dangers of cyber-crime and breaches in cyber security, there is need to focus on a way to reduce or completely eradicate its incidence in Nigeria, through education and sensitization programmes.

Thus, according to Eugene Juwah, the Executive Vice Chairman of NCC, one of the fundamental challenges of cyber security, is to effectively educate the end users to be aware of, and understand the potential dangers inherent in the cyberspace, noting that cyber threats such as malware, spoofing, phishing, spam, worms, viruses, hacks, Trojans, pharming, amongst others, are becoming extremely sophisticated [34]. As Nigeria meet technical, legal, and operational challenges associated with cybercrimes and threats, she should not forget to educate her youth and others in society that computer hacking and virus dissemination is not only illegal,

but ethically wrong [33]. An average individual knows that it is wrong to break into our neighbors' houses and steal things or damage their property. Yet, it doesn't seem that our youth today are being taught that the same principles apply to their behavior on computers and the Internet. Unfortunately, in certain instances, unethical online behaviors are been glorified [33].

Just as protecting youth from dangers on the Internet is important, so is protecting the Internet from young people who might abuse it. Parents, caregivers, teachers, and adults, should work to teach youth Internet safety by telling them to keep their personal information safe and avoid predators, i.e. it is very important to teach youth cyber ethics.

Teaching teens about the ethical treatment of others on the web and of websites and intellectual property (such as music, videos, and written materials) in cyberspace can help prevent cybercrime. While youth who commit cybercrimes may realize that their actions are wrong, they may not know that their Internet mis behaviors are illegal. The United States Department of Justice Attorney's Office (www.usdoj.gov/usao/paw/task_force) categorizes cybercrime in three ways: the computer as a target (using a computer to attack other computers); the computer as a weapon (using a computer to commit a crime); and the computer as an accessory (using a computer to store illegal files or information). These categories include crimes such as launching viruses, storing illegal files (such as child pornography), committing fraud, infringing copyrights, and pirating software, among others.

Many youth commit cybercrime by downloading and sharing copyrighted information assets, video and music files; harassing others via chat blogs (computer programs designed to imitate human conversation); as well as hacking into computer networks to deface websites, enter sites that the school forbids, or change grades. The best way to prevent youth from committing cybercrimes is to educate them about ethical and legal rules of the Internet, and the emotional and financial costs of cybercrimes to victims. Moreover, cybercrimes carry real consequences. Youth should be taught that their actions in cyberspace are not anonymous, and that real people are affected by their crimes (National Crime Prevention Council, 2006).

In many cases, teens still consider computer and online mischief harmless. Majority do it as fun, because they have easy and unhindered access to the online environment. A recent survey found that 48 percent of students in elementary and middle school don't consider hacking illegal (Hopper, 2013). As there are many cases of cybercrimes involving teens. Sharing the cases with them during cyber ethics education will help them realize the seriousness of cybercrimes, and will therefore take precautionary measures (National Crime Prevention Council, 2006).

Meanwhile, as noted by Hope [22], positive behavior is developed at primary level so that it will be able to support the students' development to higher levels of education. This is why cyber ethics education is imperative here, not only at the primary level of education, but also at secondary and higher levels in order to set responsible and moral mindsets in pupils and students so that they will grow with them to maturity as responsible citizens.

At the tertiary level of education, Mabawonku [21] found out that there are limited research efforts on information ethics, of which cyber ethics is a key component, by Nigerian scholars and lecturers, decrying that exposure to the subject is limited. She further noted that in teaching the subject, issues that deserve special focus are internet research ethics, free and open source, ethics of information on the Internet, email spam and intellectual property rights. These afore-mentioned issues fall under cyber ethics. Thus, cyber ethics education is essential for all in the Nigerian society.

IV. CONCLUSION AND RECOMMENDATIONS

There is no doubt that prevention of cybercrimes and enforcement of cyber security is a necessity in Nigeria requiring holistic attention of all stakeholders. Cyber ethics education will go a long way in addressing the menace in the country. It is required that the cybercrimes bill be passed into law.

It should be complemented with cyber ethics education for prevention of cybercrimes. In addition,

the following recommendations should be given consideration by educational planners and other stakeholders in the Nigeria project:

- Cyber ethics education and its content should be properly articulated and integrated in computer education or social studies subject in primary and secondary schools in the country by the National Educational Research and Development Council of Nigeria.
- Cyber ethics education should form a key component of citizenship education offered in tertiary institutions across the country, or better still it can be made a separate compulsory general studies course.
- More universities and other tertiary institutions should establish cyber security science departments like the case in Federal University of Technology Minna, so as to develop more high level manpower that will address cyber threats and crimes in the country. Although many higher institutions offer computer science as a course, however specialization in cyber security will contribute significantly in fighting cybercrimes.
- Organizations, establishments, corporate bodies, agencies of government and tertiary institutions should organize seminars and workshops on cybercrime and cyber ethics for their staff and students (in the case of tertiary institutions).
- In addition to the existing ones, more Rural Information Technology Centres should be established by NITDA, and be used in conjunction with public libraries as centres for inculcating cyber ethics education in youths and adults in the society. Even as the NITDA Director General, Peter Jack, plans to digitize and rename RITC to Community Digital Opportunity Centres, with a triangular business model that features the tele-centre, the corner shop and an eatery, it should be given attention as centres for inculcation of cyber ethics in the Nigerian society.
- There should be the establishment of Non-Governmental Organisations (NGOs), with focus of sensitization and contributing in fighting the menace of cybercrimes and cyber threats. Nigerians that are passionate about the ugly situation should rise up to the challenge.

V. REFERENCES

[1] Adebusuyi, A. (2008) The Internet and emergence of yahoo boys sub-culture in Nigeria.

[2] *International Journal of Cyber-Criminology*, 2(2), 368 – 381.

[3] Adejuwon, K.D. (2012) From e-government to e-governance: whither African public administration. *Advances in Arts, Social Sciences and Education Research,* 2 (1), 63 – 75. http://www.ejournal.sedinst.com

[4] Aginam, E. (2014) UN ranks Nigeria high in e-government development index. Accessed July 9, 2014 from at http://www.vanguardngr.com/2014/07/un-ranks-nigeria-high-e-government-devt-index.

[5] Aina, L.O. (Ed.) (2002) *Research in information science: an African perspective*. Ibadan: Stirling Horden Publishers.

[6] Akingbolu, R. (2014) Nigeria: combating cybercrime through constructive engagement. Accessed July 9, 2014 from *http://allafrica.com/stories/201407101214.html.*

[7] *Asiabaka, C.C. (2014) Imperatives of e-government and the future of Nigeria. Owerri: FUTO. Accessed July 4, 2014 from www.softwareclubnigeria.org/.../FUTO%20VC%20E- Gov%20Imperatives%20*

[8] Azeez, K. (2013) NITDA establishes 400 rural IT centres. Accessed July 13, 2014 from nationalmirroronline.net/new/nitda-establishes-400-rural-it-centres/

[9] Balogun, V.F. & Obe, O.O. (2010) E-crime in Nigeria: trends, tricks and treatment. *The Pacific Journal of Science and Technology*,

11 (1), 343 – 355. Accessed July 12, 2014 from www.akamaiuniversity.us/PJST.htm

[10] Brenner, S (2007) *Law in an era of smart technology*. Oxford: Oxford University Press

[11] *Cybercrime Bill (2013) Nigeria cybercrime bill of 2013. Accessed July 10, 2014 from http://pinigeria.org/download/cybercrimebill2013.pdf*

[12] *Ekeke, E.C. (2012) Internet abuses as hindrance to development in Nigeria: a Christian ethical approach. International Journal of Asian Social Science, 2 (7), 1123 – 1131.*

[13] Godse, V. & Garg, A. (2009) *From e-government to e-governance.* New Delhi, India:

[14] Computer Society of India

[15] Ibikunle, F. & Eweniyi, O. (2013) Approach to cyber security issues in Nigeria: challenges and solution. *International Journal of Cognitive Research in Science, Engineering and Education*. 1 (1), Accessed July 6, 2014 from http://ijcrsee.com/index.php/ijcrsee/article/view/11/114

[16] IKeepSafe (2014) *Cyber ethics*. Accessed July 12, 2014 from http://www.ikeepsafe.org/educators_old/more/c3-matrix/cyber-ethics/

[17] Iwe, N. S. S. (1987) *Socio-ethical issues in Nigeria.* New York: Peter Lang.

[18] Jack, P. (2014) NITDA to digitalise 200,000 rural information technology centres. Accessed July 12, 2014 from http://www.mydailynewswatchng.com/nitda-digitalise-200000-rural-information-technology-centres/

[19] *Kalusopa, T. (2008) Information security management: challenges and prospects in Africa. In: L.O. Aina, S.M. Mutula & M.A. Tiamiyu (Eds.) Information and knowledge management in the digital age: concepts, technologies and African perspectives (pp. 403 – 425). Ibadan, Nigeria: Third World Information Services*

[20] *Kemoni, H.N. (2012) Status of information ethics teaching at the school of information sciences, Moi University Kenya. In: A. Tella & A.O. Issa (Eds.). Library and Information Science in developing countries: contemporary issues (pp. 141 – 147). Philadelphia, USA: IGI Global*

[21] *Mabawonku, I (2010) Teaching information ethics in Nigerian library schools and some tertiary institutions: overview, challenges and prospects*. Accessed March 27, 2013 from *www.africainfoethics.org/pdf/2010/.../Mabawonku%20%20paper.pdf*

[22] Masroom, M., Mahmood, N.H.N & Zainon, O. (2013) Cyber ethics and internet behaviour of Malaysian primary education students. *Journal of Emerging Trends in Educational Research and Policy Studies*, 4 (1), 105 – 111.

[23] Mintz, S. (2012) Cyber ethics education: teaching young people about cybercrime. Accessed July 12, 2014 from http://www.ethicssage.com/2012/09/cyber-ethics-education.html

[24] National Crime Prevention Council (2006) Teaching youth cyber ethics. Accessed July 9, 2014 from http://www.ncpc.org/programs/teens-crime-and-the-community/monthly-article/teaching-youth-cyberethics

[25] Ocholla, D.N. (2009) Information ethics and education in Africa: where do we stand? *International Information and Library Review*, 41, 79 – 88. Doi: 10.1016/j.iilr.2009.04.001.

[26] Odumesi, J.O. (2014) A socio-technological analysis of cybercrime and cyber security in Nigeria. *International Journal of Sociology and Anthropology*, 6 (3), 116 – 125.

[27] Olayiwola, P.O. (2012) Information security framework and national cyber security. *Paper presented at the Conference on Regulatory Imperatives for Cybercrimes and Cyber Security in Nigeria, organized by Nigerian Communications Commission, held at International Conference Centre, Abuja, and March 5, 2012. Accessed July 8, 2014 from* www.ncc.gov.ng/index.php

African Journal of Computer & ICTs, 5 (1), 69 – 82.

[28] Omoregbe, J. I. (1993) Ethics: a *systematic and historical study*. Lagos: Joja Educational Research.

[29] Ozumba, G. O. (2001) *A course text on ethics.* Lagos: Obaroh & Ogbinaka.

[30] Ramadhan, A., Sensuse, D.I. & Arymurthy, A.M. (2011) E-government ethics: a synergy of computer ethics, information ethics, and cyber ethics. *International Journal of Advanced Computer Science and Applications,* 2(8), 82 – 86. Accessed July 10, 2014 from www.ijacsa.thesai.org

[31] Tyendezwa, T.G.G. (2012) Legislation on cybercrime in Nigeria: imperatives and challenges. *Paper presented at the Conference on Regulatory Imperatives for Cybercrimes and Cyber Security in Nigeria, organized by Nigerian Communications Commission, held at International Conference Centre, Abuja, and March 5, 2012. Accessed July 8, 2014 from* www.ncc.gov.ng/index.php.

[32] Udofia, R. (2014) Nigeria must clean cyber space – juwah. Accessed July 12, 2014 from http://www.vanguardngr.com/2014/07/nigeria-must-clean-cyberspace-juwah/

[33] Uwaje, C. (2009) Techtrends: Nigeria and the challenges of cybercrime. Accessed July 12, 2014 from http://techtrendsng.com/nigeria-and-the-challenges-of-cyber-crime-

[34] Uzor, B. (2014a) Weak legal framework encouraging cybercrime. Accessed July 7, 2014from http://businessdayonline.com/2014/06/weak-legal-framework-encouraging-cybercrime/#.U8CQlSizvIU

[35] Uzor, B. (2014b) NCC advocates multi-stakeholder partnership to combat cybercrime. Accessed July 12, 2014 from http://businessdayonline.com/2014/06/ncc-advocate-multi-stakeholder-partnership-to-combat-cybercrime/#.U8CQIyizvIU

[36] Wada, F. & Odulaja, G.O. (2012) Assessing cybercrime and its impact on e-banking in Nigeria using social theories.