Digital Technology Education in Curbing Cyber-Crime in Nigeria for National Development

Abubakar O. Ari
Department of Educational Foundations,
University of Nigeria, Nsukka
abubakar.ari@unn.edu.ng +2348137200235

Bridget O. Dioka
Center for Igbo Studies
University of Nigeria, Nsukka.
bridget.dioka@unn.edu.ng +23490933217027

&

Abu A. Usman
Department of Educational Foundations,
University of Nigeria, Nsukka.
usmanabiabu@gmail.com +2348065523088

Abstract

In recent time, the alarming growth of the digital technology education (on-line learning) resources and its wide acceptance has led to increase in cyber-crime in Nigeria. In Nigeria, digital technology education assisted cyber-crimes are committed on daily bases in various forms such as fraudulent electronic mails, plagiarism, identity theft, hacking, spamming, and so on. The paper was able to discuss and elaborate much about cyber-crime and digital technology education, digital technology for national development, various types of cyber-crime, causes of cyber-crime and different ways of combating cyber-crime was discussed. The

paper therefore recommended, among other things, that this paradigm be adopted by school authorities and cyber-security awareness and training that can make the learners be aware of the danger of cyber-crime or cyber-attacks in schools and colleges to achieve successful teaching and learning as a means to minimize the impact of cyber-crime for effective national development in Nigeria.

Keywords: Digital technology, Education, Cyber-crime, Nigeria, National Development.

Introduction

The world adoption and overwhelming acceptance of digital technology education (internet or online education) in Nigeria and across the globe has facilitated learning, business and other activities that are internet compliance. The introduction of digital technology education has impacted positively in the day to day activities in the various sectors of human endeavours. However, the rapid growth, development and evolution of digital internet, including its global acceptance is generating increasing security threats to individuals, corporations, enterprise and the government as a whole. In Nigeria for instance, digital internet technology has made it possible the perpetration of different forms of cyber-crime on daily basis ranging from fraudulent electronic mails, advanced fee fraud 419 (Yahoonism or Yahoo-yahoo), sending spam email (spamming), stealing personal information (identity theft), breaking into someone's computer to view or alter data (hacking), and tricking someone into revealing their personal information (phishing), making internet services unavailable for users (Denial of service- DOS), credit card fraud (ATM), plagiarism and software piracy, pornography, stealing money bit-by-bit through tricks, virus dissemination, and so on.

Cyber-crime threats have become a major setback to many developing and developed countries of the nation as well as organizations and individuals as most activities are now successfully carried out online with less physical contact. Thus, the existence of the digital internet technology had significantly changed the way people learn, get information, and also construct knowledge about the world through cyber-space. Cyber-crime is a crime committed with the help of computer and smart phones through communication device or a transmission media called the cyber-space and global network called the "internet". According to Chioma (2017) the cyber-space creates unlimited opportunities for legal activities in forms of commercial, social, and educational activities.The coming of the internet has brought about unprecedented breakthrough in every sphere of human endearvour in the world today; providing a medium for distance learning, online-learning, servicing as a source of income, enabling business transactions and online-business advertisement. In fact, with the emergence of computers, the world has long been regarded as a "global village" because computers has shortened the distance, boost the economy and made learning easier even for a common man. However, the cyber-space has also provided a near-safe haven for societal miscreants to perpetrate their criminal acts. One major effect of the digital technology education (internet or online education) is cyber-crime, which has also become a threat to Nigeria's socio-economic and national development.

The term cyber-crime describes a range of offenses including traditional computer- crimes as well as network crimes; it involves a series of organized crimes attacking both the cyber-space and cyber-security. Cyber-security awareness and training can make people be aware of the danger of cyber attacks and can minimize the impact. These attacks are mostly focused on the most vulnerable or fewer inexperienced people. Cyber-security awareness can be applied to help in

minimizing some basic attacks to individuals and governments who are more vulnerable to cyber attacks. The use of digital technology education sources for the intention of learning by students and educators help extend their learning capabilities and also pose remedies to cyber-attacks. Therefore, knowing what, how, and when to access the digital technology education methods and principles to curtail the occurrence of the cyber-crime would be important to all and sundry. This can be done through preventive measures and the knowledge or information about cyber-security which help to increase individual security enlighten.

Concepts Classification

Concept of Digital Technology Education

Digital technologies are electronic tools, systems, devices, and resources that generate store or process data. Well known examples include social media, online education, multimedia and mobile phones. Digital education is any type of learning that uses technology. It can be happen across all curriculum learning areas. Digital technology can help students by making learning more engaging and collaborative rather than memorizing facts, students learning by and through critical thinking skills. Digital technology means the use of computer and technology assisted strategies to support learning within the educational system. In the educational sectors, digital internet and other information technology tools are used to engage in personal communication and conduct educational activities among other several benefits.

From many perspectives, global involvement and active use of science and technology policies to achieve digital technology education goals should constitute the new focus and priority for technology policy advancement. To curtail the situation, the government should as a matter of urgency creates job opportunities for the teeming unemployed youths loitering the streets of major cities in the country.

Social programs like "N-power", "P-Yes", N-Sip, "N-Agro", N-tech and a few others launched by the present administration is a welcome development, if it achieved its stated goals.In pursuance of these goals of technology education as enshrined in the National Policy on Education (2014), states that,

Government shall:

a) adopt measures to develop and encourage the ideas of technology education through student's exposure to practical industrial work experience;
b) improve immediate and long-term prospects of graduates of technology institutions and other professionals with respect to their remuneration; and
c) Encourage technology education institutions to conduct applied research relevant to the needs and aspirations of the nation.

Concepts of Cyber-crime

In defining cyber-crime, there is the need to understand the split meaning of cyber and crime. The term "cyber" is a prefix use to express an idea as a component of the computer and information age. Crime can be defined as any activity that contravenes legal procedure mostly completed by individuals with criminal motive. By synthesis of the concept cyber and crime, what then is cyber-crime? Cyber-crime or computer related crime is a crime that involves the computer and the network. Cyber-crime is defined as (i) computer-aided crime originating in Nigeria internet domain space (ii) computer-aided crime perpetrated by Nigerians located outside the Nigerian internet domain space.

The term cyber-crime can be used to describe any criminal activity which involves the computer or the internet networks. This term is used for crimes such as fraud, theft, blackmail, forgery, and embezzlement, in which computers or

networks are used. According to Maitanmi (2013) cited in Omodunbi et al defined cyber-crime as a type of crime committed by criminals who make use of a computer as tool and the internet as a connection in order to reach a variety of objectives such as illegal downloading of information and data, piracy, spam mailing and the likes. Carter (1995) cited in Chioma et al (2017) defines cyber-crimes as any activity in which computers or networks are use as a tool, a target or a place of criminal activity.Criminal activities done using computers and digital technology which include anything from downloading illegal data, or information or fraudulent electronic mails from the online sources. Cyber-crime according to Laura (1995) cyber-crime is a criminal activity involving illegal access (unauthorized access), illegal interception (by technical mean of non-public transmissions of computer data to, from or within a computer system), data interference (unauthorized damaging, deleting, deterioration, alteration or suppression of computer data), system interference (interfering with the functioning of a computer system by inputting, transmitting computer data), misused of devices, forgery (ID theft), and electronic fraud.

Cyber-crimes in the education sectors continue to gather pace and momentum, taking major systems offline and impacting lessons in both schools and universities globally. Thus, it is crucial that educational institutions take time to review their current cyber-security threats and develop a holistic cyber strategy that spans people, process and technology. At a time where the global pandemic has stretched academia resources beyond limits, universities and schools must focuses relentlessly on cyber-security education, digital technology education and internet crime knowledge to identify areas of potential weakness and what steps are taken to mitigate the risks of cyber-crime. According to Ugwu et al (2021) view that one of the ways through which cyber-crime can be mitigated is by improving the cyber-hygiene culture of

the internet users. These can only be done through digital knowledge of education. Cyber-hygiene refers to those cyber-security attitudes and behaviour which internet users are expected to adopt to ensure the safety and integrity of their data and also their devices in the case of cyber attacks by the internet fraudsters.

Apart from implementing basic digital technology skills, technical measures such as cyber-security education, end-point protection, patching and application of security in schools and universities, there should be an active role in cyber-security programmes. Therefore, the research gap here is the lack of cyber-security awareness programs to students at the university level for identifying their awareness in Nigeria. Using the internet for a long time can put students into a vulnerable condition by exposing them to online risks and threats. Thus, the following awareness be created for both the students and teachers alike.

a) Are individual or groups accountable for cyber-security for our school/university?
b) Is knowledge of cyber-security included as a major risk register?
c) How soon would one know about the crime tactics? Do we have effective monitoring systems in place to know when a breach has occurred?
d) Is there awareness about cyber threats amongst staff and students? How are education sectors measuring the effectiveness of this training?
e) How can we identify the high-value critical assets within our digital technology education? How confident are we that they are secured appropriately.
f) Is there cyber-security insurance to protect the internet users?

Digital Technology for National Development in Nigeria

The role of the digital technology in the development of Nigerian's education sector and foreign direct investment on education cannot be overemphasis. The digital technology education (internet) is one of the most revolutionary innovations of the 21st century. It has enabled instant information, transactions through e-mail, SMS, twittering, Google search, and video-conferencing. It has opened up doors and opportunities to free information, data and exposure as well as offering a cheaper information or data in educational sectors. Unfortunately, the digital technology (internet) is a double edge sword. Cyber-crime is a new trend that is gradually growing as the internet continues to penetrate every sector of our society and no one can predict its future. The digital technology education usually requires a hectic task to trace the perpetrator of cyber-crime. Generally, cyber-crime may be divided into one or two types of categories.

i. Crimes that affects computer networks and devices directly. Examples are malicious code, computing viruses, malware and so on.

ii. Crimes facilitate by computer networks or devices, the primary targets of which is independent of the computer networks or devices. Examples include cyber stalking, fraud and identity theft, phishing scams and information warfare.

The contribution of digital technology education (internet) to the development of Nigeria has had positive impacts on the various sectors of the country's educational sectors. The life wire of the education, business and banking sectors is the internet. Currently, the use of digital technologies in education has been widely advocated and institutionalized in Nigeria's educational system. Successful application of digital technology education depends not just upon sufficient access to equipment, tools and resources, but also on the availability of sufficient training, knowledge and

support networks for teachers and students alike. Providing teachers with this support will allow them to achieve technological education effectively in teaching and learning process. Thus, if all this need are met, then the cyber-hygiene or cyber-security provides strong evidence that use of digital technologies education can aid teaching and learning, as well as enhance the ability to curtail cyber-crime.

As a consequence, successful implementation of digital technology education in teaching and learning requires support from teachers in the form of opportunities to learn (both formally and informally), embedding digital learning in continuing professional development and initial teacher training, direction and leadership within a school system, functioning digital equipment and tools, and provision of an enabling environment that gives teachers the flexibility to introduce and use of digital technology in learning process. The effective selection of software and devices is only part of the technique use in curtailing cyber-crime. The consideration of what learning will be achieved and how the technology may help is fundamental to its effective deployment to schools and colleges. The rapid development of educational technology does not manifest itself in teaching/learning practices along, but to help in developing knowledge in curtailing cyber-crime.

To achieve the transformation in education sectors, one must invest in digital technology education for effective improvement in learning outcomes. The world is a global village is a saying which is over a decade old, but it's gradually but becoming a daily reality in Nigeria and across the sub-Saharan region, with the increase in mobile devices and high-speed in internet which serve as platforms for many socio-economic technologies that bring about national development.

Various Types of Cyber-Crimes in Nigeria

In Nigeria, as the internet grows to become more accessible, cyber-crime has become one of the main avenues for shoplifting money and business intelligence. The internet has experienced an explosive growth with the number of hosts connected to the internet increasing daily at an exponential rate. Hassan et al (2012) Categorized cyber-crimes into cyber terrorism, cyber fraud, malware, cyber stalking, spam, plagiarism, wiretapping, logic bombs and password sniffing.

a. **Cyber terrorism**: Lewis (2012) defines cyber terrorism as the malicious act of using computer network to disrupt the normal processes of critical national infrastructures (such as education, energy, transportation, government operation). Hassan further described cyber extortion as a sort of cyber terrorism whereby website, e-mail server, e- computer system leveraging on ransom ward is put under attack by hackers for denial of services and demand for ransom.

b. **Phishing**: Phishing is simply the theft of an identity. It involves stealing personal information from unsuspecting users and it is also an act of fraud against the authentic, unauthorized education system, businesses and financial institutions that are victimized. Phishing scams are ubiquitous and are exponentially increasing. It has become one of the fastest growing cyber-crimes in Nigeria. In this jet age of digital technology, masses subscribe to a plethora of sites using their e-mail addresses and are therefore expecting to receive mails of up-dates of their membership or subscription. Fraud (identity theft): Fraud refers to the act of depriving a person dishonestly of something, which such an individual are supposedly entitled to posses.

c. **Malware**: Malware also known as malicious software refers to the use of software or code designed to by-

pass some security checks in computer/mobile devices and harness data without consent.

d. **Cyber-stalking**, harassment and blackmailing scam: Threatening and blackmailing acts carried out on the victim by fraudsters on the internet. According to Ellison and Akdenzi (1998), cyber-stalking refers to the use of the internet, e-mail, or other electronic devices to stalk another person.Cyber stalking can be used interchangeably with online abuse or online harassment. The perpetrator does not present a direct physical threat to a victim, but follows the victim's online activity, gather information and eventually makes threat towards the victim.

e. **Spam**: Spam is refers to the unsolicited bulk electronic mail (e-mail, and short message services (SMS) sent indiscriminately to prospective victims of crime via electronic messaging systems. It is possibly the most practical cyber attack weapons because of its low operating cost. The perpetrators known as spammers rely on users not reading the first print of agreements resulting in them agreeing to send messages indiscriminately to their contacts.

f. **Cyber-crimes in education sectors**: The educational sector in Nigeria suffers greatly from electronic crimes which are perpetrated mostly by students in tertiary institutions. **Cyber-plagiarism**, cyber-plagiarism can be defined as copying and pasting online sources into word processing documents without reference to the original writer or ownership be acknowledge accordingly. In the educational sector in Nigeria, students, particularly those in the tertiary institutions carry out this crime without enforcing the due penalty. Another is **cyber-pornography**, cyber-pornography is the act of using cyber space to create, display, distribute, import or publish pornography or

obscene materials, especially materials depicting children engaging in sexual assault all in the name of educating the populace.

Causes of Cyber-Crimes in Nigeria

The following are some of the identified causes of cyber-crime in Nigeria;

(a) Unemployment is one of the major causes of cyber-crime in Nigeria. It is a known fact that over 20 million graduate in the country do not have gainful employment. This has automatically increased the rate at which they take part in criminal activities for their survival.

(b) Quest of wealth and certification is another cause of cyber-crime in Nigeria. Youths of nowadays are very greedy, they are not ready to start up an educative venture with hard work, and hence they strived to level up with their rich counterparts by engaging in crime such as examination mal-practice.

(c) Weak implementation of cyber-crime laws and inadequately equipment of law enforcement agency. Weak/fragile laws regarding cyber criminals exist in Nigeria, unlike in the real world were criminals such as internet crime are treated with maximum penalties. Nigeria is not well equipped with sophisticated hardware to tract down the virtual forensic criminals. Lack of strong cyber-crime laws also encourages the perpetrators to commit more crime knowing that they can always go uncaught and unpunished. There is need for our government to come up with stronger laws, to be able to enforce such laws so that criminal will not go unpunished. Laura (2012) states that "African countries have been criticized for dealing inadequately with cyber-crime as their law

enforcement agencies are inadequately equipped in terms of personnel intelligence and infrastructure and the education sector is also lagging behind in curbing cyber-crime".

(d) Incompetent of security personnel on personal computers system in Nigeria. They do not have proper or competent security control; it is prone to criminal activities hence the information on it can be stolen either by the users or personnel.

(e) Urbanization is one of the causes of cyber-crime in Nigeria. It is the massive movement of people from rural settlement to cities. According to Wikipedia, urbanization is looked at as the massive physical growth of urban areas as a result of rural migration in search for better life.

The Challenges of Digital Technology in Curbing Cyber-Crimes

As digital technology education (internet) related challenges increase such as cyber attacks, the need for safe practices among users to maintain computer system's health and on-line security has become imperative, and this methods is called cyber-hygiene. Poor cyber-hygiene among internet uses are very critical issues undermine the general acceptance and adoption of digital technology (internet technology). It has become a global issue and concern in this digital technology era when virtually all learning, business transactions, information and communication technology (ICT) and many other activities are performed on-line. This therefore called for concerted effort to curb the menace of cyber-crime activities on individuals, education sectors, organization and governments. The challenges or criticism of digital technologies in curbing cyber-crime in Nigeria are as follow:

a. A lot of time and resources are currently being invested into technologies and applications that have yet to be prone to be effective and efficient when compared to more traditional learning contexts. Teachers and schools need to think carefully about when, why and how to use technologies as well as evaluating their efficiency and effectiveness.

b. There is "digital divide" the divide between those who have access to digital technology and the internet, and those that do not.

c. Implementation and then maintaining technology is costly particularly as system can quickly become out-dated.

d. There may be problem with the existing infrastructure, for example internet connections may be inconsistent and/ or slow.

e. Safety for students and teachers is a key challenge with prevention of cyber-crime, the hacking of personal information, across to illegal or banned materials and distractions from learning (such as social networking and mobile phone use) all being high on institutional agendas.

f. Some use of the technologies can be harmful. For example, poor posture and eyestrain are common problems when working at desktop computer for a prolonged period. Also Repetitive Strain Injury (RSI) is a risk that occurs from the repeated actions necessary to control mobile devices.

g. Evidence suggests that at the moment the potential of digital technologies in the classroom is not been realized. What is clear is that no technology has an impact of learning in its own; rather, their impacts depend upon the way in which it is used.

The prevalence of cyber-crime has also created a bad image for Nigeria amongst the nations that are most corrupts

and criminal activities in the world. Cyber-crime has also had an implication in the foreign direct investment in education advancement into the country, as information flowing from the country is been characterized as questionable because of criminal elements which make it unreliable, inaccurate and untrustworthy. Cyber-crime has negatively impacted on Nigerians confidence in digital technology.

Ways of Combating Cyber-Crime in Nigeria

The increasing use of the digital technology education (internet or online education) in Nigeria has also led to an increase in cyber-crime. The recent decision by the Federal Government of Nigeria to setup a working group, the Nigeria Cyber-crime Working Group (NCWG), and other law enforcement agencies in Nigeria spend countless hours fighting cyber-crime, but no positive effort was achieved in combat cyber-crime. Thus, the knowledge of cyber-crime is important. Learning the different types or ways of cyber-crimes and their criminality will always help in combat these crimes. It is also an important step in helping to catch these cyber-criminals and keep them away from continuing to commit cyber-crimes against others. Cyber-crime cannot be easily and completely eliminated, but can be minimized. However, collaborative efforts of individuals, corporate organizations and government could go a long way to reduce it to a minimal level. Educational institutions should secure their network information systems to combat the frequency of the cyber crime.

The following are some of the suggested ways in combating cyber-crime in Nigeria's institutions of learning.

a. Laws to enforce educational system in the country should be properly enforced, proper enforcement of educational laws to check-mate the irregularities of work in the institutions of learning to rebost the teaching and learning and reasonable take steps to

protect education sectors. Even where laws are adequate, education sectors' dependent on the network, institutions must check-mate the network system failure, information and computer system must also be secure.

b. Government should ensure that their laws apply to cyber-crimes be enforceable. African countries are bedeviled by various socio-economic problems such as poverty, covid-19, fuel price crisis, political and ethnic instability and other related crimes. This limits their strength to effectively combat cyber-crime. Nevertheless, it is important that Nigeria as a nation take measures to ensure that panel and procedural laws are adequate to meet the challenges pose by cyber-crimes. The government must ensure laws are formulated and strictly adhered to.

c. Individuals should observe simple rules guiding the knowledge of digital technology crimes and also acquire information about cyber-space. Individuals on their parts should ensure proper anti-malware protection on their computer systems, they should be encouraged to avoid pirated software, never to share their personal identification number (PIN), e-mail access code to unknown persons, never disclose any confidential information about your secret network system to anybody as none of these networks were designed to be ultimately secure. Ignore any e-mail requiring any financial information. All ill intended cyber-space or spam in educational institution must be reported immediately to the appropriate authorities. The success in harnessing cyber-space will help Nigerians achieve unprecedented personal productivity and prosperity in education sectors. The government must take immediate steps to protect cyber-space for becoming a criminal haven. Cyber-

criminals must be denied the anonymity they are seeking while at the same time protecting the privacy of Nigerian educational sectors.

Recommendations

Cybercrime cannot be easily and completely wiped out, but can be reduced. However, collaborative efforts of individuals alongside with government intervention could go a long way to minimize it to a reasonable level. The laws should be formulated by the government and should strictly be adhered to. The full implementation of this law will hopefully bring a strategic approach to fight against cybercrime. The society should constantly show interest in their children's behaviour for them to conform to the right norms and values that is charitable in the environment. This is enshrined in the National Policy on Education (2004), it is clearly states that the quality of instruction at all levels of educational system should be tailored towards the inculcation.

i. Respect for the worth and dignity of the individual

ii. Faith in man's ability to make rational decision

iii. Moral and spiritual values in interpersonal and human relation

iv. Shared responsibility for the common good of the society

v. Respect for the dignity of labour

vi. Promotion of the emotional, physical and psychological health of all children.

Digital technology knowledge should be constantly taught in schools and colleges to review the tactic of criminal activities: It has been discovered that cyber criminals can get very careless hence it is advisable to review the system

regularly to discover unusual mistakes. Use of digital internet network intrusion detection system this is applicable for more serious attacks like breaking into a bank network to steal customers' sensitive data which cannot be discovered by mere inspection or reviewing. Intrusion detection techniques such as Honey pots, Tripwires, Anomaly detection systems, Operating system commands and Configuration checking tools are always employed. Inspecting of mails before opening is a very useful way of detecting unusual or strange activities. E-mail spamming and cyber stalking can be detected by carefully investigating the e-mail header which contains the real e-mail address, the internet protocol address of the sender as well as the date and time it was sent. Another well-known system is Snort, it is a robust open source tool which exists for monitoring different network attacks the system by employs the rules established by the administrator to monitor traffic and detect strange behaviours in the educational system.

Conclusion

Cybercrime is a menace that should be eradicated or reduced to a very minimal level for our great nation to break even. The rising spate of cyber-crime globally and its attendant negative consequences has continued to call for immediate actions. As digital technology advances, novel methods are used to perpetrate cyber related crimes. Several cyber-crimes and causes have been discussed in this paper. It is recommended that our government should make the welfare and wellbeing of the citizens a priority so as to lessen the burden of individuals by providing good educational systems, paying jobs with other basic amenities. This will in no little way make life comfortable for people hence reduce their participation in criminal activities for survival. It is only after this is done that any bill or law against cybercrime can really take effect. Individuals are also enjoined to be smart and

adhere to the preventive measures listed above in order not to fall victims. Moreover, since youths are the most involved in this crime, there is need for them to be well educated and empowered with digital technology for the country to have a greater future.

The rising spate of cyber-crime globally and its attendant negative consequences has continued to call for immediate actions. There is therefore, the need to take proactive steps to curb the menace. Cybercrime poses a great risk to the economy, especially education sectors, hence the need to institute an effective risk management system through digital technology education and enhancement of the capacity to carry out forensic investigation to tackle the menace of cyber-crime. Also, collaborative efforts of governments, corporate entities and the citizenry could play a vital role in checking cyber-crimes.

References

Chioma, C. O. (2017) Proliferation of cyber insecurity in Nigeria: A root causes analysis. *International Journal of Science and Technology* (STECH). 6(2).

Chioma, C. O. (2017). Proliferation of cyber insecurity in Nigeria: A root cause of analysis. *International Journal of Science and Technology* (STECH), 6 (2). pp 14-55.

Ellison L. and Akdeniz Y. (1998). Cyber stalking: the Regulation of Harassment on the Internet. Criminal Law Review, Special Edition: Crime, Criminal Justice and the internet, 29-48.

Epron, S. (2019). Emerging security threats: Factors and implications for Nigeria's socio-economic development 2015-2019. *Nigerian Journal of Economics and Development Studies*, 7(2). pp 143-144.

Federal Republic of Nigeria. National Policy on Education, 4th edition. Lagos: NERDC Press, 2004, 8.

Folarin, B. J. (2014). Race and gender effects on fear of crime: An interactive model with age, Criminology, 25(1), pp 133-152.

Hassan, A. B., Lass, F. D., & Makinde, J. (2012). Cyber-crime in Nigeria: Causes, effects and the way out. *International Journal of Science and Technology.* 2 (7), pp 626-631 .

Ibikunle, F., et al. Approach to cyber-security issues in Nigeria: Challenges and solutions. *International Journal of Cognitive Research in Science Engineering and Education* (IJCRSEE). 2013 1 (1).

Laura, A. (2012) Cyber-crime and national security: The role of the penal and procedural law. *Research Fellow, Nigerian Institute of Advanced Legal Studies*. Retrievedfromhttp://nialsnigeria.org/pub/lauraani.pdf.

Laura, A. (2012), Op. Cit.

Lewis, A. J. (2012). Assessing the risks of cyber terrorism, cyber war and other cyber threats: *Center for Strategic and international studies*, Washington, D.C.

Omodubbi, B. A., Esan, A. & Olaniya, O. (2016). Cyber-crime in Nigeria: Analysis, Detection and Prevention. *International Journal of Engineering and Technology*, 1 (1), p 38

Omodunbi, B., Esan, A. & Olaniya, O. (2016), 1 (1), Op. Cit.

Ugwu, C., Ani, C. (2021). Towards determining the effect of Age and educational level of cyber-hygiene. 21(03). Retrieved from http://arxiv:2103.06621vi(CS.CY).11March,2021.