**CYBERCRIME AND THE ACADEMIC INSTITUTIONS NETWORKS (LAUTECH AS A CASE STUDY)**

**BY**

**ADEBAYO MODINAH GBEMISOLA**

**MATRIC NUMBER: 153302**

**BEGIN A PROJECT PROPOSAL SUBMITTED**

**TO**

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING FACULTY OF ENGINEERING AND TECHNOLOGY, LADOKE AKINTOLA UNIVERSITY OF TECHNOLOGY OGBOMOSO, OYO STATE NIGERIA.**

**IN PARTIAL FULFILMENT OF THE REQUIREMENT FOR THE AWARD BACHELOR OF TECHNOLOGY (B.TECH) DEGREE IN COMPUTER SCIENCE AND ENGINEERING**

**CHAPTER ONE**

**INTRODUCTION**

* 1. **Background of study**

It is obvious that the ICT meets a variety of educational, entertainment, communications, commerce needs, and other areas just few to mention, for its users. ‘With these benefits, though, this same technology has also ushered in a new wave of criminal activity called **cybercrime**’ (Saban, McGivern and Saykiewicz, 2002) defined as ‘any illegal act fostered or facilitated by a computer, whether the computer is an object of a crime, an instrument used to commit a crime, or a repository of evidence related to a crime’ (Royal Canadian Mounted Police, 2000, in Hinduja and Schafer 2009) Cybercrimes are those crimes which are committed in the online or electronic environment.

The role that Information and Communication Technology (ICT) plays in all aspects of human endeavors is well documented and evident. ICT has integrated different economies of the world, through the aid of electronics via the internet. Many corporate organizations, including banks now depend on ICT and computer networks to perform basic as well as complex tasks. The electronic market is now open to everybody, including criminals. It is projected that by 2030, global Cyber security spending will reach $300bn, a 136% increase from $75bn in 2015.

As the Internet came into widespread commercial use, the nature of computer crimes began to shift. ‘While in some crimes, one component of the crime may have been committed using an electronic instrument, in other crimes, the crime as a whole is committed in the online or electronic environment. These crimes are also known as **cybercrimes**; generally occur in the virtual community of the Internet or in cyberspace’ (Heather 2008, Newton 2008).

Viruses, worms, hacking and Trojan horses are another serious threat. There is a variety of Cybercrime committed but these are the most prevalent and appear to be among the most troubling to computer users (Furnell, 2002 in Brett, 2008).

* 1. **Statement of problem**

The implications of cybercrime on international security have risen from the manner of technology use by individuals and a set of people known as cybercriminals. These people have mastered the art of computer networks to their advantage. Hidden behind computer monitors they commit atrocities such as data theft, hacking, espionage, and virus scattering. Most countries of the world have highly developed internet networks. Recently, there have been breakthroughs in the field as major telecommunication companies sprint to introduce 5G networks to the globe. However, there are fears that this network will also be used by criminals to gain access to victims organization network systems causing destruction and losses across all continents. Numerous techniques are being used by criminals of the 21st century to target sensitive data, recording the highest levels of fraud in history. At the hands of cybercriminals, victims lose private information, money, and even their characters. This study seeks to explore the forms of cybercrimes that have rocked the world in the new age. Additionally, the study seeks to examine the impact of such activities on academics institution network security and correspondingly, the measures to curb the situation academically.

* 1. **Aim and Objective**
     1. **Aim**

As cybercrime incidents are increase every day, the aim of this project is to reduce and eliminate cybercrime activities in the academic institutions network most especially in LAUTECH.

* + 1. **Objectives of the study**
    2. **Objective of the study**

1. Collecting of data from all members of academic institutions (LAUTECH) through the use of questionnaire.
2. To identify various cybercrime techniques in academic institution networks.
3. To establish and discuss the possible ways of reducing cybercrime in academic institutions.
4. Creating a taxonomy of cybercrime on it relates to the academic network.
5. Carryout a relationship analysis of data obtained above
6. Make references to recommendations for combating the identified crimes
   1. **SIGNIFICANT OF STUDY**

The study has the significance in observing the weaknesses present in the law governing cybercrime and strategic to initiate cybercrime law in academic institutions . Also identify the driving force succeed to solve that problem.

Therefore it provided challenges and suggest better recommendations to the government and academic institutions to combat cybercrime.

* 1. **SCOPE OF THE STUDY**

The study was to observe how academic institution combating a cybercrime. The researcher was interest to analyse the legal documents that can be used to stop computer crime. And what effort are taken to make academic institution and rest part of the world to be free from cybercrime. The study was focus on strategies that have been initiated by academic institutions to be free from cybercrime and make a digital life to be better place.

**CHAPTER TWO**

REVIEW OF PREVIOUS LITERATURE

**2.1 Introduction**

There is no doubt that the technology of ICT is growing dramatically with cybercrime. This growth brings a lot of changes and revolutions from traditional methods to electronic means. The change includes governments, institution, business and other activities from paper based to digital. Also introduced new methods of banking and other financial transaction under electronic system. The impact of digital technology is going very fast and cause the number of challenges. This why make a lot of study written which based on cyberspace take part in legal and technique.

In this section, the works done by previous authors with respect to issues bordering on cybercrime and cyber security are examined.

In [4] cybercrime was defined as a type of crime committed by criminals who make use of a computer as a tool and the internet as a connection in order to reach a variety of objectives such as illegal downloading of music files and films, piracy, spam mailing and the likes. Cybercrime evolves from the wrong application or abuse of internet services. The concept of cybercrime is historical. It was discovered that the first published report of cybercrime occurred on the mainframe computer in the 1960s [4]. Since these computers were not connected to the internet or with other computers, the crime was committed by the employers (insider) in the company, hence it was referred to as computer crime rather than cybercrime.

Alkaabi [5], under the study of Combating Computer Crime: An International Perspective examined the approaches used for combating computer crime in Australia, UAE, UK and USA. This four countries represent a spectrum of economic development and culture. He said that, the global nature of the Internet has resulted enormously increased opportunities for the cyber criminals. Computer Crime or Cybercrime is increasingly becoming one of the main threats to the wellbeing of the nations of the world. Therefore, it clear that there is crucial need for common understanding of such criminal activity international to deal with it effectively. It is likewise very important to explore and understand the problem in detail and to identify obstacles to international cooperation in combating computer crime. It is also important to identify and adopt best approaches for combating computer crime. He conclude that, is required to continued research into the extent to which legislation, international initiatives, policy and procedures, and technology to combat and investigate computer crime are consistent globally and can be improved upon. However, the Author look on what approaches to combat computer and cybercrime in developed Countries but the challenges also meet to developing countries like Nigeria as a part of developing country in Africa. The threat flow around the society since the number of computer user increased every day. My study will analysis on legal ways to reduce cybercrime in Nigeria academic institutions network.

According to Lakshmi [3] as at 2003, the United States and South-Korea have the highest cyber-attacks of 35.4% and 12.8% respectively. With the population of Nigeria placed at 160 million from the last census carried out in 2006, a recent statistics revealed that about 28.9% have access to the internet(Hassan, 2012). It was also proven that 39.6% African users of internet are actually Nigerian, hence, the high increase in the rate of internet crime in Nigeria [6]. Presently, cybercrimes are performed by people of all ages ranging from young to old, but in most instances the young. Presently, cybercrimes are performed by people of all ages ranging from young to old, but in most instances the young.

In the study of Das and Patel [1], the issues, challenges and solutions to cyber security for social networking sites (SNS) were highlighted. While stressing the initiatives of government to eradicate serious issues on cyber security, it recommended appropriate ways individuals, institutions, organization and government could adopt in collaboration with private sector to achieve a safe cyber-space.

Makeri [2] studied cyber security issues in Nigeria and challenges. The author makes effort to provide an overview of cybercrime and cyber security. The definition of the concept of cybercrime, identification of motives behind cybercrime and ways to get rid of it were established. The author further looked at the action of cyber criminals and the motive for their involvement. Methods to protect users from the activities of cybercriminals and to checkmate them were emphasized.

Observers are warning that developing countries are fast becoming a major source of Internet crimes. For instance, Nigeria is ranked first in the African region as the target and origin of malicious cyber activities; and this is spreading across the West African sub-region[7]. Egypt is also known to be one of the most phished countries in the world with approximately 2000 phishing incidents, followed by other nations in the region such as South Africa [8], and recently Ghana. There remains a lack of consensus over the forms of computer misuse that should attract a criminal sanction, as opposed to a civil remedy such as those attaching to intellectual property and commercial laws. Certainly, some of the cybercrimes listed here do not fall properly within the province of the criminal law. Cybercrimes originating in America often implicate national boundaries; plenty of these cases fall under federal laws. National collaboration with local law enforcement and prosecutors to share information and efforts through cooperation has proved efficient in curbing traditional crimes.

Statistically, Nigeria ranked 43 in EMEA and ranked third among ten nations that commits cyber-crime in the world.[9] As a corrective measure, the then President of Nigeria, Olusegun Obasanjo set up National Cyber security Initiative (NCI) in 2003. The Nigerian cybercrime working group (NCWG) is to meet the objectives of NCI but their effects did not match up to the rate of growth of cybercrime. Professor Oliver Osuagwu, relating cyber-crime to the collapse of the educational sector, points out that cybercrime is causing near total collapse of the education community, particularly in Nigeria, with over 90% of criminals coming from this sector. Wrong value system has been identified as key factor encouraging cybercrime in Nigeria and the desire to get rich quick without working for it. Cyber-crime is complex and committed mostly from remote locations making it difficult to police. The absence of enabling law makes policing even more difficult.[9]

2.2 METHODOLOGY

This study uses the qualitative method that intends to collect comparable records on cybercrime and computer crime activities across the both students and staffs in LAUTECH. The study will be conduct purposely to elaborate and provide more knowledge on the concept of cybercrime and cybersecurity in academic institutions networks. The research will utilizing instruments such as questionnaires, virtual interviews, and reports from radio and electronic media. I will conduct a survey covering a variety of internet users among them students, business persons, and academic staffs. The impact of cybercrime on societies across the world is immense and consequential most especially in academic institutions network (LAUTECH). There also exists an upward trend in the cases of cybercrime activities across the world. Currently, there is a disconnect in the manner the academic institutions network has handled this form of criminal activity. Cybercriminals have taken advantage of this gap to undermine academic institution efforts. Undoubtedly, this vice has been deleterious to economies costing countries billions of Naira every year. Research efforts must be boosted towards understanding criminal activity globally through international initiatives, legislation, and procedures.

REFERENCES

1. R. Das, and M. Patel (2017). Cyber Security for Social Networking Sites: Issues, Challenges and Solutions. International Journal for Research in Applied Science & Engineering Technology (IJRASET), Vol. 5, No. 4,833-838.
2. Y. A. Makeri (2017). Cyber Security Issues in Nigeria and Challenges. International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 7, No.4, 315-321.
3. Lakshmi P. andIshwarya M. (2015), Cyber Crime: Prevention & Detection," International Journal of Advanced Research in Computer and Communication Engineering, vol. Vol. 4(3).
4. Maitanmi, O. Ogunlere, S. and Ayinde S. (2013), Impact of Cyber Crimes on Nigerian Economy, The International Journal of Engineering and Science (IJES, vol. vol 2(4), 45–51.
5. Alkaab, Ali, Combating Computer Crime: An international and Perspective, Oct 2010, Queensland University of Technology, http://eprints.qut.edu.au/43400/1/Ali\_Alkaabi\_Thesis.pdf ( accessed 04th July)
6. A. B. Hassan, F. D. Lass, J. Makinde (2012). Cybercrime in Nigeria: Causes, Effects and the Way Out. ARPN Journal of Science and Technology, Vol. 2, No. 7, 626-631
7. Ribadu N (2007), “Cyber-Crime and Commercial Fraud: A Nigerian Perspective”, Presented at the Congress Celebrating the 40 th Annual Session of the United Nations Commission on International Trade Law, July 9-12, Vienna, Austria.
8. Ojedokun A A (2005), “The Evolving Sophistication of Internet Abuses in Africa”, The International Information and Library Review, Vol. 37, No. 11, pp. 11-17.
9. Background check international, “Information Technology/Cyber Security Solutions”