NATIONAL OPEN UNIVERSITY OF NIGERIA

FACULTY OF SOCIAL SCIENCES

COURSE CODE: CSS 812

COURSE TITLE:

CYBERCRIMES

COURSE GUIDE

CSS 812
CYBERCRIMES

Course Writer/Developers	Dr. Philip N. Ndubueze Department of Sociology Federal University Dutse
Course Coordinator	Prof. Sam Obadiah Smah CSS, FSS NOUN.
Course Editor	Dr. Dickson Ogbonnaya Igwe CSS, FSS NOUN
Programme Leader	Dr. Dickson Ogbonnaya Igwe Ag. HOD, CSS, FSS NOUN

CONTENTS PAGE

INTRODUCTION

CSS 812: Cybercrimes is a 3-credit unit course. It is a compulsory course for students enrolled in the Bachelor of Science and Postgraduate Programmes in the field of Criminology and Security Studies of the University. The course is also recommended to other students especially those in the School of Arts and Social Sciences, who are interested in the study of cybercrimes. The course can be taken as an elective or required course by other undergraduate or postgraduate students whose main field (s) or disciplines are not Criminology and Security Studies.

However, the Course shall consist of 24 units, which are divided into 6 modules, and each of these modules shall consist of 4 units. The units include: conceptual definition and classification of cybercrime; the history of the internet and evolution of cybercrime; differences between cybercrime and physical space crime; cyber criminology: context/intellectual roots, concerns and future directions; child pornography and child grooming; cyberbullying, cyberstalking and cyber squatting; dark web and cryptomarket operations; digital piracy; hacking and malware; online advance fee fraud; online Identity theft; sexting and revenge pornography; differential association theory; routine activity theory; neutralization theory; space transition theory of cybercrime; cybercrime legislations in Nigeria and selected African countries; regional and international cybercrime legislations/regulations; challenges of cybercrime legislations in Africa and strategies for improvement; cybersecurity: issues and perspectives; the challenges of studying and investigating cybercrime; digital forensics and investigation; third party policing strategies and cybercrime investigation; challenges of the criminal justice system in policing and prosecuting cybercrime.

The course has no compulsory pre-requisites for it to be registered for. The course guide informs us on what this course is all about, what students will learn in each unit, what text materials we shall be using and how we can make the best use of these materials. This course guide also emphasizes on the need for students to take tutor-marked assignments seriously. However, necessary information on tutor-marked assignments shall be made known to students in a separate file, which will be sent to each of them at the appropriate time. This course is also supported with periodic tutorial classes.

What You Will Learn in This Course

CSS 812: Cybercrimes as a course in the field of Criminology and Security Studies at the National Open University of Nigeria will expose you to a wide range of issues that bother on crime and criminality in the cyberspace. You will be able to appreciate the role of the relatively young discipline of cyber criminology in interrogating the issues of deviance, crime and terrorism in the cyberspace. The course will also guide you towards understanding the patterns and prevalence of some emerging cybercrimes and the various theories that can be employed in the explanation of cybercrime. You will also learn about some local, regional and international cybercrime legislations as well as cybersecurity related issues and perspectives. Finally, you will be exposed to the issues, challenges and prospects of policing and prosecuting cybercrime in Nigeria.

AIMS

a) To introduce students to the fundamental issues around the spate of crime in the cyberspace;

b) To enable students appreciate the role of the relatively young discipline of cyber criminology in interrogating the issues of deviance, crime and terrorism in the cyberspace;

c) To guide students to the understanding of the patterns and prevalence of some emerging cybercrimes;

d) To provide students with well balanced understanding of the theories that can be employed to explain cybercrime.

e) To critically evaluate the legal instruments established to control cybercrime and the initiatives at national, regional and international levels to ensure security in the cyberspace.

OBJECTIVES

a) To examine the conceptual definition and classification of cybercrime as well as the differences between crime in the physical space and crime in the cyberspace;

b) To discuss the history of the internet and evolution of cybercrime as well as the context, concerns, and future directions of the discipline of cyber criminology;

c) To discuss the some emerging patterns of cybercrime, such as child pornography, child grooming, cyber stalking, digital piracy, sexting and so on;

d) To critically review some theories that are relevant in the explanation of cybercrime;

e) To discuss some local, regional and international cybercrime legislations as well as some cybersecurity issues and perspectives;

f) To examine the challenges confronting the Criminal Justice System in policing and prosecuting cybercrime.

WORKING THROUGH THIS COURSE

To complete this course you are required to read the study units as well as the recommended books and articles. Each study unit contains a self-assessment exercise, and at some points in the course, you are required to submit assignments for assessment purposes. You will be expected to write a final examination at the end of the course. Stated below are the components of the course and what you are expected to do.

COURSE MATERIALS

For this course, students will require the following materials:

1) The course guide;
2) Study units which are twenty four (24) in all;
3) Textbooks/articles recommended at the end of the units;
4) Assignment file where all the unit assignments are kept;
5) Presentation Schedule.

In addition, you must obtain the text materials. They are provided by the NOUN. You may be able to purchase other reference materials from the bookshop.

STUDY UNITS

There are twenty-four (24) study units in this course broken down into six (6) modules of four units each.

Module 1: Introduction to Cybercrime and Cyber Criminology

Unit 1: Conceptual Definition and Classification of Cybercrime
Unit 2: The History of the Internet and Evolution of Cybercrime
Unit 3: Differences between Cybercrime and Physical Space Crime
Unit 4: Cyber Criminology: Context/Intellectual Roots, Concerns and Future Directions

Module 2: Some Emerging Patterns of Cybercrime I
Unit 1: Child Pornography and Child Grooming
Unit 2: Cyberbullying, Cyberstalking and Cyber Squating
Unit 3: Dark Web and Cryptomarket Operations
Unit 4: Digital Piracy

Module 3: Some Emerging Patterns of Cybercrime II
Unit 1: Hacking and Malware
Unit 2: Online Advance Fee Fraud
Unit 3: Online Identity Theft
Unit 4: Sexting and Revenge Pornography

Module 4: Theories of Cybercrime
Unit 1: Differential Association Theory (DAT)
Unit 2: Routine Activity Theory (RAT)
Unit 3: Neutralization Theory (NT)
Unit 4: Space Transition Theory of Cybercrime (STT)

Module 5: Local, Regional and International Cyber Crime Legislations/Cyber Security Issues and Perspectives
Unit 1: Cybercrime Legislations in Nigeria and Selected African Countries
Unit 2: Regional and International Cybercrime Legislations/Regulations
Unit 3: Challenges of Cybercrime Legislations in Africa and Strategies for Improvement
Unit 4: Cybersecurity: Issues and Perspectives

Module 6: Cyber Crime Policing and Prosecution in Nigeria: Issues, Challenges and Prospects
Unit 1: The Challenges of Studying and Investigating Cybercrime
Unit 2: Digital Forensics and Investigation

Unit 3: Third Party Policing Strategies and Cybercrime Investigation
Unit 4: Challenges of the Criminal Justice System in Policing and Prosecuting Cybercrime.

Each unit contains some exercise on the topic covered, and Students will be required to attempt the exercises. These will enable them evaluate their progress as well as reinforce what they have learned so far. The exercise, together with the tutor marked assignments will help students in achieving the stated learning objectives of the individual units and the course.

TEXTBOOKS AND REFERENCES

Students may wish to consult the references and other books suggested at the end of each unit to enhance their knowledge of the material.

ASSESSEMENT

Assessment for this course is in two parts. Such as the Tutor-Marked Assignments, and a written examination. Students will be required to apply the information and knowledge gained from this course in completing their assignments. Students must submit their assignments to their tutor in line with submission deadlines stated in the assignment file. The work that you submit to your Tutor-marked Assignment for assessment will count for 30% of your total score.

TUTOR MARKED ASSIGNMENT (TMAS)

In this course, you will be required to study fifteen (15) units, and complete tutor marked assignment provided at the end of each unit. The assignments carry 10% mark each. The best four of your assignments will constitute 30% of your final mark. At the end of the course, you will be required to write a final examination, which counts for 70% of your final mark. The assignments for each unit in this course are contained in your assignment file. You may wish to consult other related materials apart from your course material to complete your assignments. When you complete each assignment, send it together with a tutor marked assignment (TMA) form to your Tutor. Ensure that each assignment reaches your tutor on or before the dead line stipulated in the assignment file. If, for any reason you are unable to complete your assignment in time, contact your tutor before the due date to discuss the possibility of an extension.

Note that extensions will not be granted after the due date for submission unless under exceptional circumstances.

FINAL EXAMINATION AND GRADING

The final examination for this course will be for two hours, and count for 70% of your total mark. The examination will consist of questions, which reflect the information in your course material, exercise, and tutor marked assignments. All aspects of the course will be examined. Use the time between the completion of the last unit, and examination rate to revise the entire course. You may also find it useful to review your tutor marked assignments before the examination.

COURSE MARKING SCHEME

ASSESSMENT	**MARKS**
Assignment	Four assignments, best three marks of four count at 30% of course marks.
Final Examination	70% of total course work
Total	**100% of course marks**

COURSE OVERVIEW

Assignment file consists of all the details of the assignments you are required to submit to your tutor for marking. The marks obtained for these assignments will count towards the final mark you obtain for this course. More information on the assignments can be found in the assignment file.

Course Overview and Presentation Schedule

Module 1	**Title of Work**	**Weeks Activity**	**Assessment (End of Unit)**
Unit	Conceptual Definition and Classification of Cybercrime	Week 1	
1			
2	The History of the Internet and Evolution of Cybercrime	Week 2	Assignment 1
3	Differences between Cybercrime and Physical Space Crime	Week 3	

4	Cyber Criminology: Context/Intellectual Roots, Concerns and Future Directions	Week 4	
Module 2			
Unit	Child Pornography and Child Grooming	Week 5	Assignment 2
1			
2	Cyberbullying, Cyberstalking and Cyber Squatting	Week 6	
3	Dark Web and Cryotomarket Operations	Week 7	
4	Digital Piracy	Week 8	
Module 3			
Unit	Hacking and Malware	Week 9	Assignment 3
1			
2	Online Advance Fee Fraud	Week 10	
3	Online Identify Theft	Week 11	
4	Sexting and Revenge Pornography	Week 12	
Module 4			
Unit	Differential Association Theory (DAT)	Week 13	Assignment 4
1			
2	Routine Activity Theory (RAT)	Week 14	

3	Online Identify Theft	Week 15	
4	Sexting and Revenge Pornography	Week 16	
Module 5			
Unit	Cybercrime Legislations in Nigeria and Selected African Countries	Week 17	Assignment 5
1			
2	Regional and International Cybercrime Legislations/Regulations	Week 18	
3	Challenges of Cybercrime Legislations in Africa and Strategies for improvement	Week 19	
4	Cybersecurity: Issues and Perspectives	Week 20	
Module 6			
Unit	The Challenges of Studying and Investigating Cybercrime	Week 21	Assignment 6
1			
2	Digital Forensics and Investigation	Week 22	
3	Third Party Policing Strategies and Cybercrime Investigation	Week 23	
4	Challenges of the Criminal Justice System in Policing and Prosecuting Cybercrime	Week 24	

HOW TO GET THE MOST FROM THIS COURSE

In distance learning, your course material replaces the lecturer.

The course material has been designed in such a way that you can study on your own with little or no assistance at all. This allows you to work, and study at your place, and at a time and place that best suits you. Think of reading your course material in the same way as listening to the lecturer. However, you are advised to study with your course master in the same way a lecturer might give you some reading to do, the study units give you information on what to read, and these form your text materials. You are provided exercise to do at appropriate points, just as a lecturer might give you an in-class exercise.

Each of the study units follows a common format. The first items is an introduction to the of the unit, and how a particular unit is integrated with the other units and the course as a whole. Next to this, is a set of learning objectives. These objectives let you know what you are required to know by the time you have completed the unit. These learning objectives are meant to guide your study. The moment a unit is finished, you must go back and check whether you have achieved the objectives. If you make this habit, it will improve your chances of passing the course significantly.

The main body of the unit guides you through the required reading from other sources. This will usually be either from the reference books or from a reading section. The following is a practical strategy for working through the course. If you run into difficulties, telephone your tutor. Remember that your tutor's job is to help you when you need assistance, do not hesitate to call and ask your tutor for help or visit the study centre.

Read this Course Guide thoroughly in your first assignment.

1) Organize a study schedule. Design a "course overview" to guide you through the course. Note the time you are expected to spend on each unit and how the assignments relate to the units. You need to gather all the information into one place, such as your diary or a wall calendar. Whatever method you choose to use, you should decide and write in your own dates and schedule of work for each unit.

2) Once you have created your own study schedule, do everything to be faithful to it. The major reason students fail is that they get behind with their course work. If you get into difficulties with your schedule, please, let your tutor know before it is too late for help.

3) Turn to unit 1, and read the introduction and the objectives for the unit.

4) Assemble the study materials. You will need the reference books in the unit you are studying at any point in time.

5) Work through the unit. As you work through the unit, you will know what sources to consult for further information.

6) Before the relevant due dates (about 4 weeks before due dates), access the Assignment file. Keep in mind that you will learn a lot by doing the assignment carefully. They have been designed to help you meet the objectives of the course and pass the examination. Submit all assignments not later than the due date.

7) Review the objectives for each study unit to confirm that you have achieved them. If you feel unsure about any of the objectives, review the study materials or consult your tutor.

8) When you are confident that you have achieved a unit's objectives, you can start on the next unit. Proceed unit by unit through the course and try to pace your study so that you keep yourself on schedule.

9) When you have submitted an assignment to your tutor for marking, do not wait for marking before starting on the next unit. Keep to your schedule. When the Assignment is returned, pay particular attention to your tutor's comments, both on the tutor-marked assignment form and also the written comments on the ordinary assignments.

10) After completing the last unit, review the course and prepare yourself for the final examination. Check that you have achieved the unit objectives (listed at the beginning of each unit) and the course objectives (listed in the Course Guide).

FACILITATORS/TUTORS AND MARKED TUTORIALS

There are 15 hours of tutorials provided to support this course. Tutorials are for problem solving and they are optional. You need to get in touch with your tutor to arrange date and time for tutorials if needed. Your tutor will mark and comment on your assignments, keep a close watch on your progress and on any difficulties you might encounter and provide assistance to you during the course. You must submit your tutor-marked assignments to your tutor well before the due date (at least two working days are required). They will be marked by your tutor and returned to you as soon as possible.

Do not hesitate to contact your tutor by telephone, e-mail, or discussion board. The following might be circumstances in which you will find necessary contact your tutor if:

- You do not understand any part of the study units or the designed readings.
- You have difficulties with the exercises.
- You have a question or problem with an assignment, with your tutor's comments on an assignment or with the grading of an assignment.

To gain maximum benefits from this course tutorials, prepare a question list before attending them. You will learn quite a lot from participating in the discussions.

SUMMARY

The course guide has introduced you to what to expect in cybercrimes. It examines a wide range of issues that bother on crime and criminality in the cyberspace; the role of the relatively young discipline of cyber criminology in interrogating the issues of deviance, crime and terrorism in the cyberspace; the patterns and prevalence of some emerging cybercrimes; various theories of cybercrime; some local, regional and international cybercrime legislations as well as cybersecurity related issues and perspectives and the issues, challenges and prospects of policing and prosecuting cybercrime in Nigeria. Upon completion you should be equipped with the foundation for analyzing issues around crime and criminality in the cyberspace.

We wish you success with the course and hope you will find it both engaging and practical.

REFERENCES/FURTHER READING

Bruneau, M. et. al. (2020). Introduction: Challenges and generic research questions for future research on resilience. In Z. Wu, X. Lu, M. Noori (eds.). *Resilience of Critical Infrastructure Systems: Emerging Developments and Future Challenges* (pp. 1-42) Boca Raton: Taylor and Francis – CRC Press.

Cullen, F.T., Agnew, R. & Wilcox, P. (2014). *Criminological theory: Past to present*. NewYork: Oxford University Press.

Diamond, B. and Bachmann, M. (2017). Assessment of cyber criminology: Obstacles, Challenges and the promising path of the new science of cybercrime. In K. Jaishankar (ed.). I*nterpersonal Criminology: Revisiting Interpersonal Crimes and*

Victimization (pp. 247 – 256). Boca Raton, USA: CRC Press, Taylor & Francis Group.

Halder, D. & Jaishankar, K. (2017). Sexting among teens: Are they victims or offenders.. In K. Jaishankar (ed.). I*nterpersonal Criminology: Revisiting Interpersonal Crimes and Victimization* (pp. 215 – 232). USA: CRC Press, Taylor & Francis Group.

Holt, T.J. (ed.) (2016). *Crime online: Correlates, causes, and context*. Durham: Carolina Academic Press.

Holt, T.J. & Brown, S.C. (2018). Contextualizing digital piracy. In S.C. Brown and T.J. Holt (eds.). *Digital Piracy: A Global Multidisciplinary Account*. London: Routledge: Taylor and Francis Group.

Jia, K. & Zang, F. (2018). Between liberalization and prohibition prudent enthusiasm and the goveranance of Bitcoin/blockchain technology. In M. Campbell-Verduyn (Ed.). *Bitcoin and Beyond: Cryptocurrencies, Blockchain, and Global Governance* (pp. 88-109). London: Routledge: Taylor and Francis Group.

Marcum, C.D. (2014). *Cyber Crime*. New York: Wolters Kluwer.

Mcnally, M. (2012). *Identity Theft in Today's World*. California: Praeger.

Ndubueze, P.N. (2017). Cyber Criminology: Contexts, Concerns and Directions'. In P.N. Ndubueze (ed.). *Cyber Criminology and Technology-Assisted Crime Control: A Reader* (1-28). Zaria: Ahmadu Bello University Press.

Nhan, J. & Bachmann, M. (2015). Developments in Cyber Criminology. In M. Maguire and D. Okada (eds.). *Critical Issues in Crime and Justice: Thought, Policy and Practice*, (2nd ed.), pp. 209 -228. Los Angeles: Sage Publications.

Paar, C. & Pelzl, J. (2010). *Understanding cryptography: A Textbook for Students and Practitioners*. London: Springer Heidelberg Dordrechi.

Reid, S.T. (2015). *Crime and Criminology* (14th ed.) New York: Wolters Kluwer.

Sachowski, J. (2018). *Digital forensic and investigations: People, processes, and technologies to defend the enterprise*. Boca Raton: CRC Press-Taylor and Francis Group.

Module 1: Introduction to Cybercrime and Cyber Criminology

Unit 1: Conceptual Definition and Classification of Cybercrime
Unit 2: The Evolution of the Internet and Cybercrime
Unit 3: Differences between Crime in the Physical Space and Crime in the Cyberspace
Unit 4: Cyber Criminology: Context/Intellectual Roots, Concerns and Future Directions

UNIT 1 CONCEPTUAL DEFINTION, CHARACTERISTICS AND CLASSIFICATIONS OF CYBERCRIME

CONTENTS

1.0 Introduction

2.0 Objectives

3.0 Main Content

3.1 Conceptual Definitions of Cybercrime and Cybercriminals

3.2 Difference between Computer Crime and Cybercrime

3.3 Characteristics of Cybercrime

3.4 Classifications of Cybercrime and Characteristics of Cyber Criminals

4.0 Conclusion

5.0 Summary

6.0 Tutor-Marked Assignment

7.0 References/Further Reading

1.0 INTRODUCTION

Earlier the term “computer crime” was commonly used to refer to criminal activities that involved the computer. However, with the emergence of the internet, the term “cybercrime” became increasingly popular. Cybercrime is generally used to refer to criminal activities that occur in the cyberspace. These criminal activities can be categorized in different ways. The characteristics of cybercrime can also be distinguished from other kinds of crime.

2.0 OBJECTIVE

This unit covers the definition of cybercrime; the difference between cybercrime and computer crime; characteristics of cybercrime and classification of cybercrime as well as characteristics of cybercriminals.

3.0 MAIN CONTENT

3.1 Conceptual Definition of Cybercrime

There is no universally accepted definition of cybercrime. However, cybercrime scholars and researchers have attempted to define it in various ways. Arguably, such definitions provide useful insights into the nature and scope of cybercrime. Holt and Bossler (2016, p.7) defined cybercrime as “offences that occur in online environment”. According to Thomas and Loader (2000, p.3) cybercrime refers to “computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks.” The Nigerian Cyber-crime Working Group (2005, p.2) defined cybercrime as “conducts prohibited by law with prescribed punishment, carried out using computers, electronic ancillary devices, processes and/or procedures”. Furthermore, Joseph (2005) noted that it is carried out on the internet with the use of computer as either a tool or a target. However, Halder and Jaishankar (as cited in Ngo and Jaishankar (2017, p.3) offered a more comprehensive definition of cybercrime when they described it as:

> Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including but not limited to Chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS).

They further observed that cybercrime is made up of 30 different types of offences and that they include: hacking, malware, identity theft, online fraud, credit card fraud, spamming, web and email spoofing, dating scam, cyber bullying, harassment and stalking and distributed denial of service attacks.

The aforementioned definitions of cybercrime clearly highlight the following important points about the nature and scope of cybercrimes:

- Cybercrime is a computer/technology-enabled crime
- It is committed through the cyberspace/internet
- It may be committed via computer-mediated communication (CMC), electronic ancillary devices such as cell phones, i-pads, Internet-of-Things etc
- It is an outlawed conduct with prescribed punishment
- A computer may be used as a tool to commit cybercrime or can in actual fact be the target of cybercrime
- Victims of cybercrime may be individuals or groups
- Victims of cybercrime may experience harm, which may be physical or psychological loss.

- It is a transnational crime and as such its prosecution may raise some jurisdictional issues.
- It an emerging and evolving kind of crime.

3.2 Difference between Computer Crime and Cybercrime

The terms computer crime and cybercrime are often used interchangeably to mean the same thing. But the two terms though synonymous do not have the same meaning.

Holt and Bossler (2016) argued that the term computer crime was generally used to describe almost all criminal activity that involved the computers until the late 1990s. They noted that the terminology started changing with the impact of technology use and access on society. Computer became more user friendly with the development of Windows 95 operating system and easy internet access. More so, they pointed out that the emergence of the web browser like Netscape Navigator and Microsoft Internet's Explorer in the early 1990s enabled home users to have online experience of visual content via images, text, audio and video files. Consequently, dial-up internet services became cheaper and personal computers with inbuilt modems and connection ports for phone lines or Ethernet cables for high-speed connections were became available for sale. The global expansion of internet connectivity resulted in the digitalization of sensitive financial and government information as well as massive accessible database online. Holt and Bossler pointed out that it was this change in the pattern of technology use that prompted researchers such as David Wall in 1998 to start using the term "cybercrime" to refer to crimes that are perpetrated online.

Fundamentally, computer crime refers to any illegal activity that involved the computer. For example, the unauthorized access to a computer system can be referred to as computer crime. On the other hand, cybercrime refers to criminal activity that involves a computer/related device and network. For example, sending a fraudulent email to a target. This will normally involve a computer or a smart-phone. There are several ways a computer can used to commit criminal activity. But unless, the computer is connected to the internet it remains computer crime. It is the network connection that makes the act cybercrime.

3.4 Characteristics of Cybercrime

Clough (as cited in Gillespie, 2016) identified the following characteristics of cybercrime:

i. **Scale:** The number of persons using the internet and related communications is large. This is perhaps because the internet has increasingly become part of the daily routine activities of many people. People use the internet and associated devices not only for work but also for leisure. The implication of this is that the potential number of cybercrime victims and offenders is also large.

ii. **Accessibility**: The digital divide is fast closing up as the internet is reaching areas of the world where it was not found such as Africa and parts of the Middle East. This is largely due to the availability of broadband internet in these areas. This has afforded offenders the opportunity to meet people whom they can partner with in crime.

iii. **Anonymity**: The internet allows users to hide their identity in ways that are not possible in the physical space. Cyber criminals can disguise and make it difficult for investigators to know their true identifies. Anonymity remains one of the most aggravating factors in cybercrime.

iv. **Portability and Transferability**: The continued production of storage media makes it difficult to find the result of a crime or an electronic trace of it. The cloud computing technology allows for data to be stored in the internet. This can frustrate investigation as investigators may find that the evidence they require is held in locations outside of their jurisdiction.

v. **Global Reach**: The internet is a global resource and this raises the question of jurisdiction. The question borders on whether countries can enact laws governing behaviour and whether investigators can be able to access evidence. Jurisdictional issues have remained contentious in transnational cybercrime investigation.

3.4 Classifications of Cybercrime and Characteristics of Cyber Criminals

3.4.1 Classifications of Cybercrime

Cybercrime scholars and international organizations have offered some classifications of cybercrime. Wall (2001) provided four categories of cybercrime namely: cyber trespass, cyber deceptions/theft, cyber pornography and cyber violence.

i. **i. Cyber Trespass**–This refers to the act of trespassing into the property of others online with the intention to cause damage there. Examples include: hacking, virus attack and defacement.

ii. ii. **Cyber Deceptions/theft:** This is the act of stealing money or property online such as credit card fraud, phishing e-mails, violation of intellectual property etc.

iii. iii. **Cyber Pornography**: This includes all activities that violate laws against online obscenity and indecency. Example child pornography, revenge pornography etc.

iv. iv. **Cyber Violence**: This is the act of causing psychological harm to or instigating physical harm against others online and in so doing violating human rights laws. Examples include: online hate speech, cyber stalking etc.

Brenner (2001) classified cybercrime into four legal categories:

- Prohibited conduct (atus resus)
- Capable mental state (mens rea)

- Attendant circumstances and
- Forbidden result or harm

The Council of Europe's Convention on Cybercrime (2001) captured cybercrimes in four main categories.

- Offenses against the confidentiality, integrity, and availability of computer data and systems.
- Computer-related offenses.
- Content-related offenses such as child pornography.
- Offenses related to infringement of copyright and related rights.

3.4.2 Characteristics of Cyber Criminals

Thomas and Loader (2005) have identified three basic categories of cyber criminals as follows:

i. **Hackers and Phreaks**: Computer hackers and phreaks (telephone hackers) illegally use information and communication technologies to access computer systems in order to explore, seek information or satisfy their curiosity. Although the activities of hackers and phreaks do not aim at causing damage to data or getting financial rewards, they are still illegal.

ii. **Information Merchants and Mercenaries**: Information merchants and mercenaries trade in the commercial sale of information. They engage in crimes such as corporate espionage and sabotage, sale and theft of identity information, computer and network break-ins, and large scale software piracy.

iii. **Terrorists, Extremists and Deviants**: These cyber criminals use information and communication technologies (ICTs) for illegal political or social activity. They may use ICTs to engage in terrorism, promote hate or engage in illegal social behaviours like the transmission of child pornography or engaging in pedophilia online.

4.0 CONCLUSION

The landscape of crime and criminality has changed with the emergence of the internet. Several traditional crimes are now easily committed online with less effort and less risk. Today, the term cybercrime seem to have become more popular than the term computer crime. There are different typologies of cybercrime and cyber criminals in the 21st century world that is characterized by growth in digital technologies. These typologies keep expanding as cybercrime and cybercriminals evolve.

5.0 SUMMARY

The unit focused on the conceptual definition of cybercrime; difference between computer and cybercrime; characteristics of cybercrime; classification of cybercrime and characteristics of cybercriminals.

6.0 TUTOR-MARKED ASSIGNMENT

Define the term cybercrime and explain Wall (2001) classification of cybercrime.

7.0 REFERENCES/FURTHER READING

Brenner, S. (2001). Is there such a thing as virtual crime? California Criminal Law Review. Retrieved from http://www.boalt.org/ CCLR/v4/v4brenner.htm

Gillespie, A.A. (2016). *Cybercrime: Key issues and debates*. London: Routledge: Taylor and Francis Group.

Holt, T.J. & Bossler, A. M. (2016). *Cybercrime in progress: Theory and prevention of technology-enabled offenses.* London: Routledge, Taylor and Francis Group.

Joesph, A.E. (2006). Cyber crime definition. Retrieved from http://www.crimeresearch.org/articles/joseph06/

Ngo, F. and Jaishankar, K. (2017). Commemorating a decade in existence of the International Journal of Cyber Criminology: A research agenda to advance the scholarship of cyber crime. *International Journal of Cyber Criminology*, 11 (1), 1-9.

Nigeria Cyber-crime Working Group (NCWG) (2005). Nigeria National Cyber Security policy.A Draft Document by the Nigeria Cyber-crime Working Group, Abuja. Retrieved from www.eshekels.com/downloads/e-government%203.pdf

The Council of Europe's Convention on Cybercrime (2001)

Thomas, D. & Loader, B.D. (2005). *Cybercrime*. London: Routledge, Taylor and Francis Group.

Wall, D.S. (2001). Cybercrimes and the Internet. In D.S. Wall (ed.). *Crime and the Internet*, pp. 1-17. New York: Routledge.

UNIT 2 THE EVOLUTION OF THE INTERNET AND CYBERCRIME

CONTENTS

1.0 INTRODUCTION

The internet when it emerged with first restricted to military purpose. However, today, the internet can be accessed by the general public. The internet revolution has enabled the movement of criminals from the physical space to the cyberspace and vice-versa. It has also led to the emergence of variants of crime that were hitherto not known to society. Since, the 1960s when the internet emerged, it has continued to evolve. In the same vein, cybercrime has continued to evolve and is becoming more complex with the growth of digital technologies.

2.0 OBJECTIVE

This unit discusses the evolution of the internet from a military experiment to general purpose technology. It further traces the evolution of cybercrime across three generations using Marcum (2014) perspective. Finally, it traces the development of computer and cybercrime from the 1960s to the 21st Century using Gercke (2012) perspective.

MAIN CONTENT

3.1 The Evolution of the Internet

The internet evolved from a military experiment to general purpose technology. This evolution has been summarized in two main phases by Naugghton (2016) as follows:

i. Phase One: From Military Experiment to Civilian Utility (1967-1995)

Pre-History: 1956-1966

The emergence of the internet was influenced by the cold war. The doctrine of 'mutual assured destruction' (MAD) governed the nuclear stand-off between the United States and the Soviet Union. It was presumed to ensure national security by guaranteeing a reprisal attack should one side launch a nuclear attack. But this logic is problematic as an attack can incapacitate the command and control system of the enemy to the point that retaliation will be difficult. This situation necessitated the design of a communications system that could withstand a devastating thermonuclear attack. Thus, Paul Baran, a researcher in RAND Corporation designed a mesh network base on high levels of link redundancy and digital communication technology known as packet switching. Furthermore, the Soviet Union successfully launched the Sputnik satellite in October, 1957 to the amazement on the United States defense establishment and the eventual establishment of the Advanced Research Projects Agency (ARPA) within the Department of Defense.

The ARPANET: 1967 -1972

Resource sharing network was first developed in ARPA in 1966. Bolt, Beranek and Newman, a Boston-based consultancy firm that is affiliated to Massachusetts Institute of Technology (MIT) was awarded the contract to build the network in 1969. The ARPANET was speedily built and by 1972, the 15 original sites had been connected and functioning. A major public demonstration of the system took place in Washington, DC, thereby marking the completion of the network. The network was designed for resource-sharing, but it eventually became used mainly for interpersonal communication, sharing files and email correspondence. The ARPANET though based on the packet switching technology of the modern internet, it was a unitary network, which was owned and operated by a single entity known as ARPA.

Development of the TCP/IP-based 'internetwork': 1973-1983

While the ARPARNET was undergoing construction and even after its completion, some important milestones in networking technology were forthcoming. For example, Researchers at the University of Hawaii had built ALOHA, which is a packet-switched network that operated via radio, unlike ARPANET which used leased telephone lines. From early to mid-1970s, ARPA ran three separate experimental networks - ARPANET, PRNET, and SATNET that used packet switching technology in different ways. Hence, there was need for 'internetworking' them so that they could operate as s seamless whole. This 'internetworking' project commenced in 1973. The ideas was to transit from a unitary network like ARPANET to a system that is capable of incorporating a variety of different networks that were owned and operated by independent organizations and entities. A suite of interlocking protocols based on two new ones – TCP and IP were developed. This new system, unlike ARPANET had no gatekeepers to control admission into it. In March, 1981, the Pentagon made it mandatory for all ARPANET host to adopt TCP/IP by January 1983. Although not all sites were able to meet the deadline, the mid 1983, all ARPANET host operated TCP/IP, technically marking the beginning of the internet as it is known today. However, shortly before then, security concerns about the network led to its splitting into civilian and military domains. Effective from October, 1982, the ARPANET continued as a research enterprise, while MILNET was exclusive for military communications. The switch-over commended in April, 1983.

Transition from a Military/Research Network to a 'Civilian' one: 1983-1995

Following the creation of the MILET domain, ARPANET regained its status as a research-oriented network controlled by universities and research institutions. This served as a basic first step in transferring the network to civilian control. Furthermore, in order to encourage the dissemination of TCP/IP technology within the computer industry, ARPA funded various operators to create TCP implementations for various operating systems such as Unix and launched a $20m fund to assist computer manufacturers implement TCP/IP software on their machines. By 1990, TCP/IP was available for most computers particularly in the United States market. With the establishment of computer science as an academic discipline in universities, the exclusiveness of the ARPANET/Internet club was seen as counterproductive. Consequently, the United States National Science Foundation (NSF) funded the creation of the Computer Science Network (CSNET) in the early 1980s. Only researchers funded by the agency had access to ARPANET, while membership of CSNET was open to computer scientists in any institution as long as they pay the annual subscription fees. The development led to the growth of the network from 2000 host computers in 1985, to 185,000 in October 1989, and 1,776,000 in July, 1993. The era of formal military in the operation of the internet ended on 28th February, 1990 with the official decommissioning of the internet. In 1994, the National Science Foundation allowed commercial companies known as Internet Service Providers' (ISPs) to take over internet service.

ii. Phase Two: The Commercial Internet (1995-Present)

The First Internet Boom: 1995-2000

The cyberspace was an unusual space in the 1980s. The cyberspace and the real world existed as parallel universes. However, this distinction was eroded and a gradual merger caused by two developments. The first was the commercialization of the network which was achieved with the handing over of the backbone to ISPs by NSF. The second was the emergence of the network's second 'killer application' known as the World Wide Web. The Netscape's extraordinary Initial Public Offer (IPO) that was filed on 9th August, 1995 facilitated the first internet boom. The boom followed the usual speculative manias and crashed in March, 2000.

'Web 2.0': 2000-2003

From 1993 onwards, there was a continued growth of innovative technologies to facilitate e-commerce and move the web into a medium that enabled transactions. Therefore, 'cookies', 'HTTPS', browsers with specialized 'plug-ins' for audio and video, javaScripts and so on that turned the web into a virtual machine all emerged. These led to the expansion of the web from 1995 onwards. Many of the services on the web were interconnected by means of software tools such as the syndication tool RSS and Application Programming Interfaces (APIs). Consequently, the web services that emerged after 1999 used APIs to determine how the entire web services could work together. Also, in the post-1999 Web, the dominant enterprises and services used the web as a programming platform. Therefore, while web 1.0 was built on the internet platform, web 2.0 services were constructed on web 1.0 platform.

Mobile Connectivity, Surveillance, Cybercrime, Corporate Power, Channing Patterns of Use and Other Implications

The latest phase of internet evolution is marked by changes in the ways the internet is accessed and used and how the infrastructure copes with the changes. The emergence of the Smartphone (a mobile phone that can access the internet) in 2007 was the most significant milestone in the recent history of the internet. Social networking services emerged, Facebook in 2004, Linkedln in 2003, and Twitter in 2006. The Internet enabled systems that spy on people in exchange for services. The war on terror has necessitated the massive expansion in state surveillance of internet and mobile communications witnessed over the past couple of years. A few large digital corporations that have dominated the internet over the last two decades wield power in a networked world. Five companies namely: Apple, Google, Facebook, Yahoo, Amazon, and Microsoft have acquired much power and influence and play significant roles in the daily lives of billions of people through market dominance in retail commerce and computer software and/or hardware. This era is also characterized by several cybercrimes, from sophisticated attacks on government and corporate websites, to spam emails offering fake prices. Notwithstanding that the internet originated in the United States, from the beginning it was meant to be a global network that would transcend national boundaries. However, the expansion of the network created tension between the global network and local customs, culture and laws. The tension between local jurisdictions bent on enforcing their laws and cultural norms on the network have risen over the past decade thereby suggesting that the internet may be ‘balkanized’, in other words split into locally controlled subnets. This fear of balkanization heightened in 2013 with the revelations by the former NSA contractor, Edward Snowden, about the surveillance capabilities of United States and allied governments. More so, the internet transformed into a many-to-many medium, thereby making its users active creators of contents as opposed to passive consumers of contents created by others. While in 1995 all internet users accessed the network through fixed-line connections, today more than half of internet users access it through mobile devices.

3.2 The Evolution of Cybercrime by Marcum (2014)

Marcum (2014) traced the evolution of cybercrime to a continuum of development that spanned three generations.

The first generation is characterized by the illegal exploitation of mainframe computers and their operating system. These criminal behaviors are usually perpetrated for financial gain or to acquire or destroy restricted information. Cybercriminals can research on how to commit crimes such as building a pipe bomb. These types of cybercrimes laid the foundation for a new level of criminality.

The second generation of cybercrime is those that use networks. Hacking and cracking were common forms of cybercrime in this generation. They were used by early phone "phrekers" who "cracked" telephone systems to make free calls. During this era land lines were common but cell phones were not. People had to pay for long distance calls, thus crackers found illegal ways to make free phone calls. Crackers eventually developed into hackers. Hackers used their knowledge of telephone and computer systems to access private information by networked computers. Second generation cybercrimes are known as "hybrid" crimes. This is because they fall between traditional and true cybercrimes. They are traditional crimes already in existence but expanded and adapted through the use of the internet. For example, crackers stole money from telecommunication companies by discovering how to make free calls. Their criminality prepared the ground for hackers to commit the same type of crime on the internet in a better, faster, less detectably way.

The Third generation of cybercrime came into being as a result of the broadband ability of the internet. These crimes would not exist if the internet was not developed as they only occur in the cyberspace. Example, spam mails, viruses, malwares etc.

3.3 The Evolution of Cybercrime by Gercke (2012)

Another way of looking at the evolution of cybercrime is by examining its development over a period of time. Gercke (2012) traced the development of computer and cybercrime from the 1960s to the 21stCentury. This account is summarized below.

The 1960s

The 1960s marked the introduction of transistor-based computer systems, which were smaller and cheaper than vacuum-tube based machines. It led to an increase in the use of computer technology. Offences at this stage had to do with physical damage to computer systems and stored data. Such incidents were usually reported, for example, in 1969, in Canada, a student riot caused a fire that destroyed computer data hosted at the university.

The 1970s

The 1970s, witnessed an increase in the use of computer systems and computer data. By the end of the decade, an estimated number of 100 000 mainframe computers were in use in the United States. As prices crashed, computer technology was more widely used within administration and business, and by the public. The 1970s heralded a shift from the traditional property crimes against computer systems that dominated the 1960s, to new forms of crime. Although physical damage was also a known form of criminal abuse against computer systems at this era, new forms of computer crime emerged. They included the illegal use of computer systems and the manipulation of electronic data. The movement from manual to electronic transactions led to another new form of crime like computer-related fraud, culminating in the loss of millions of dollar. The United States proposed a strategy specifically aimed at addressing cybercrime, while Interpol examined the problem potential legal response.

The 1980s

The 1980s saw the growing popularization of personal computers, culminating in the remarkable increase in the number of computer systems and by implication the number of potential targets for criminal victimization. For the first time, the targets included a broad range of critical infrastructure. There was therefore a growing interest in software, resulting in the emergence of the first forms of software piracy and crimes related to patents. Networks allowed offenders to enter a computer system without necessarily being present at the crime scene. Similarly, offenders could spread malicious software, and several computer viruses were discovered. Some countries began the process of updating their legislation in order to meet the requirements of a changing criminal environment. International organizations were also part of the process. Organization for Economic Co-operation and Development and the Council of Europe established study groups to evaluate the problem and look at the possibilities for legal response.

The 1990s

The graphical interface (“WWW”) was introduced in the 1990s. This led to a rapid growth in the number of Internet users and consequently new challenges. Information legally made available in one country was available globally – even in countries where the publication of such information was outlawed. The speed of information exchange made investigation of transnational cybercrime rather challenging. Also, child pornography distribution moved from physical exchange of books and tapes to online distribution through websites and Internet services. While computer crimes were generally regarded as local crimes, the Internet turned electronic crimes into transnational crime. Thus, the international community tackled the problem more aggressively. This led to the adoption of the United Nations General Assembly Resolution in 1990 and the issuance of the manual for the prevention and control of computer-related crimes in 1994.

The 21st Century

Every passing decade of the 21st century witnessed new trends in computer crime and cybercrime. The first decade of the new millennium saw the new, highly sophisticated methods of committing crimes, such as “phishing”, and “botnet attacks”, and the growing use of technology that is more difficult for law enforcement to handle and investigate, such as “voice-over-IP (VoIP) communication” and “cloud computing”. The methods as well as the impact of computer and cybercrime also changed in this epoch. Offenders are now able to automate attacks, thus the number of offences increased. National governments, regional and international organizations are responding to the growing challenges cybercrime by making it a top priority.

4.0 CONCLUSION

The internet which was dedicated to military operations during its early days have evolved over the years to become a technology that serve the work and leisure needs of billons of users across the world. There are two ways to view the evolution of cybercrime. The first is to look at a continuum of its emergence over a period of three generations. The other is to look at its emergence from 1960 to the 21st century. Both perspectives undoubtedly indicate that cybercrime has been growing in complexity. This therefore underscores the need for concerted efforts by all stakeholders to combat it.

5.0 SUMMARY

The unit discussed the evolution of the internet from a military experiment to general purpose technology. It further traced the evolution of cybercrime across three generations using Marcum (2014) account. Finally, it looked at Gercke (2012) account the development of computer and cybercrime from the 1960s to the 21st century.

6.0 TUTOR-MARKED ASSIGNMENT

Using Marcum (2014) perspective trace the development of cybercrime across three generation with vivid examples.

7.0 REFERENCES/FURTHER READING

Gercke, M. (2012). Understanding cybercrime: Phenomena, challenges and legal response. ITU. Available at: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf

Naughton, J. (2016). The evolution of the Internet: from military experiment to General Purpose Technology. *Journal of Cyber Policy*, 1 (1) 5-28.

Marcum, C.D. (2014). *Cyber Crime*. New York: Wolters Kluwer.

UNIT 3 DIFFERENCES BETWEEN CRIME IN THE PHYSICAL SPACE AND CRIME IN THE CYBER SPACE

CONTENTS

1.0 INTRODUCTION

Before the emergence of the internet, crimes only occurred in the physical space. Boundaries in the physical space can be easily delineated and more easily policed. This explains why law enforcement strategies for combating crime have historically been physical space oriented. Conversely, there are no clearly demarcated territories in the cyberspace in the sense that we know it in the physical space. For example, we cannot accurately estimate the number of computers that are connected to the internet across the world at any point in time. Also, cybercriminals can victimize targets who are located in different countries without physically meeting them. Therefore, there are several differences between cybercrime and physical space crime. The implication of this is that traditional model of law enforcement cannot be effective in combating cybercrime.

7.0 OBJECTIVE

This unit explains the meaning of cyberspace and examines the various differences between physical space crime and cybercrime.

8.0 MAIN CONTENT

3.1 Meaning of Cyberspace

Gibson (1984, p. 51) who coined the term "cyberspace" in 1982 described it as:

> A consensual hallucination experienced daily by billons of legitimate operators, in every nation… A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the non space of the mind, clusters and constellation of data like city lights receding.

However, according to Manap, Rahim and Taji (2015, p.595) cyberspace is "a space having a digitalized form where all its activities, data and content are transmitted and actualized through a 'networked communication technology' ".

The foregoing definition suggests that cyberspace is virtual in nature and is enabled by a networked communication technology. The features of cyberspace are fundamentally different from those of the physical space or real world. For example, whilst boundaries can be delineated in the physical space, they cannot be done in the cyberspace they way it obtains in the physical space because of the 'deterritorisation' of cyberspace. This therefore explains why there are differences between physical space crime and cybercrime.

3.2 Difference between Cybercrime and Physical Space Crime

Brenner (2004) argued that traditional model of law enforcement is not an effective strategy for combating cybercrime. To buttress her argument she identified the following differences between physical space crime (i.e. real world crime) and cybercrime.

i. **Proximity:** Unlike physical space crime, cybercrime does not require any form of physical proximity between the victim and the offender at the time crime is committed. As an unbounded and borderless crime, it can be committed against a victim who is in another geographical location. For example, an offender in Belgium can victimize a person in Nigeria.

ii. **Scale**: Cybercrime differs from physical space crime in that it is not one-to-one crime. It is not corporeal crime. Cybercrime is largely and increasingly an automated crime. Automation utilizes technology to multiply the number of offences that the cybercriminal can commit in a given period of time. Automation also increases the speed with which such offences are committed. Moreover, automation allows the offender to start a process of victimization and leaves the completion of the process to automated system. For example, while a typical nineteenth-century advance fee fraudster defrauded victim A, then victim B, then victim C, and so on at different period of time; a twenty-first-century online advance fee fraudster can automate the process, thereby defrauding very many victims in different locations simultaneously and with less effort.

iii. **Physical constraints:** Cybercriminals are not restricted by the kind of constraints that govern action in the physical space. Unlike physical space crime, cybercrime can be committed instantaneously with victims spread across different locations. Therefore, more rapid response is required from law enforcement in the investigation of cybercrime than traditional crimes.

iv. **Perfect Anonymity:** Cyberspace allows criminals to disguise or hide their identities in ways that are not possible in the physical space. In the physical space, when an offender tries to conceal his or her identify, for example, by wearing a mask, certain characteristics like height, weight, accent, and age can be discerned. But offenders can achieve perfect anonymity in the cyberspace. For example, a man can disguise as a woman, a teenager can disguise as an adult and so on in the cyberspace.

v. **Patterns**: Unlike with physical space, cybercrime patterns are difficult to identify. This may be due to the fact that cybercrime is still relatively new. As such the crime map that law enforcement used to allocate resources for physical space may not apply to cybercrime. The challenge of identifying cybercrime patterns is also compounded by the fact that cybercrime is not accurately documented and countries do not track the incidence of cybercrime in the same way physical space crime is tracked.

4.0 CONCLUSION

The various differences between cybercrime and physical space crime have made cybercrime policing a difficult task for law enforcement agencies. This is basically because traditional model of law enforcement cannot be effective in combating cybercrime. Not all law enforcement personnel are computer/internet-savvy. Law enforcement personnel who cannot use the computer and internet very well may not be able to detect cybercrime. Similarly, investigators who are not well trained in digital forensics cannot investigate cybercrime. Special training and re-training are required for law enforcement officers in order to orient them towards cybercrime control.

5.0 SUMMARY

The unit explained the meaning of cyberspace and discussed the various differences between cybercrime and physical space crime.

6.0 TUTOR-MARKED ASSIGNMENT

Discuss the differences between cybercrime and physical space crime.

7.0 REFERENCES/FURTHER READING

Brenner, S. (2004). Towards a criminal law for cyberspace: Distributed Security. Available:file:///C:/Users/user/Downloads/Toward_a_Criminal_Law_for_Cyberspace_ Distributed_S%20(1).pdf

Gibson, W. (1984) *Neuromancer*. New York: Acc.

Manap, N.A. Rahim, A.A. & Taji, H. (2015). Cyber identity theft: The conceptual framework. *Mediterranean Journal of Social Science*, 6 (4) 595-605.

UNIT 4 CYBER CRIMINOLOGY: CONTEXT/INTELLECTUAL ROOTS, CONCERNS AND FUTURE DIRECTIONS

CONTENTS

1.0 INTRODUCTION

There are some twenty-first century global social forces that greatly influenced the development of the discipline of cyber criminology. These forces shaped the thoughts, themes and perspectives of the discipline of cyber criminology. Early cyber criminologists were very concerned about the spate of deviance, crime and terrorism in the cyberspace and how to restore social order.

2.0 OBJECTIVE

This unit discusses the context of the emergence of the discipline of cyber criminology, intellectual roots of cyber criminology, concerns of cyber criminology and future directions of cyber criminology.

3.0 MAIN CONTENT

3.1 The Context of the Emergence of Cyber Criminology

Ndubueze (2017) identified four twenty-first century global social forces that greatly influenced the development of the discipline of cyber criminology. These forces which shaped the thoughts, themes and perspectives of the evolving field of cyber criminology are globalization, the Internet revolution, mediatization/digitization and the growth of virtual communities.

i) *Globalization*

Globalization basically refers to the increasing interconnectedness and interdependence of peoples, economies and countries. It is believed that societies across the world are variously influenced by globalization. Globalization has facilitated the development of information and communication technologies and has also led wider and speedy interaction between people in different parts of the world. One of the consequences of globalization is crime and criminality. Thus, early cyber criminologists were interested in investigating how globalization facilitates crime.

ii) *The Internet Revolution*

The growth of the Internet has undoubtedly eased the process of “free” flow of information and movement of goods and services some of which have been “virtualized”. The internet became more widespread in the 2000s with the explosion of Internet access in a scale that is unprecedented in human history across countries of the global north and global south including Nigeria. The internet encourages the development of crime and deviant sub-culture. Therefore, early cyber criminologists were interested in understanding how the Internet is affecting traditional forms of communications and more specifically how deviant, criminal and terrorists elements are exploiting its loopholes to carry out their malicious activities.

iii). *Mediatization and Digitization*

Mediatization and digitization are products of the Internet revolution. Mediatization refers to the increasing facilitation of social communications which occurred on a face-to-face basis by technical intermediation. Digitization refers to the process through which information is converted into a digital format. Digital communication technologies include the Internet, World Wide Web, video conferencing, wireless technology, cloud computing etc. Social media architecture and sites are emerging as platform not only for mediating business and leisure oriented communications but also as platforms for mediating deviant and criminal terror-oriented communications. This was also an area of research interest for early cyber criminologists.

iv). *Growth of Virtual Communities*

Virtual communities are also known as “cyber communities”, “online communities”, “electronic tribes” and “virtual worlds”. They are social aggregations with general values and interest on the internet, and are believed to be made up of people, a common goals, policies, and computer system. Virtual communities are enabled by Internet and Computer Mediated Communications (CMCs) technologies. They constitute an emerging and interesting area of research in cyber criminology. Early cyber criminologists were also interested in investigating how these communities emerge, operate and the impact their formation has on traditional face-to-face communities.

3.2 Intellectual Roots of Cyber Criminology

The term "Cyber Criminology" was academically coined by Karuppannan Jaishankar, an Indian Professor of Criminology in 2007. Cyber criminology is one of the latest sub-disciplines of criminology. According to Jaishankar (2007, para. 1) cyber criminology is "the study of causation of crimes that occur in the cyberspace and its impact in the physical space". He further explained that cyber criminology is a multi-disciplinary field that encompasses researchers from various fields such as criminology, victimology, sociology, internet sciences and computer science. Professor Jaishankar is regarded as the founding father of cyber criminology. He has researched and published extensively on cybercrime and related subjects. He is the Founding President of South Asian Society of Criminology and Victimology, the Founding Editor-in-Chief of International Journal of Cyber Criminology as well as the Founding Editor of the International Journal of Criminal Justice Sciences. He established the first cybercrime-specific theory: Space Transition Theory of Cybercrime in 2008.

Furthermore, Ndubueze (2016, p.33) definition of cyber criminology stated below captures the fundamental concerns of the discipline.

> Cyber criminology is the scientific study of deviance, crime and terrorism in the cyberspace and the concerns that they provoke among a wide spectrum of stakeholders such as internet-active users, families, Faith Based Organizations (FBOs), operators, security companies, Internet Service Providers (ISPs), regulators, the criminal justice system, the government and Non-Governmental Organizations . Cyber criminology is a twenty-first century field of

> criminology that emerged in response to the development of the cyberspace and the super-criminogenic atmosphere it created.

Furthermore, Ndubueze (2017) observed that cyber criminology is broadly focused on the spate of crime, deviance and terror in the cyberspace and the quest for social order. There are other dedicated cyber criminologists who are making serious efforts to advance the evolving field of cyber criminology include: Bachmann, Brenner, Holt, Jewkes, Nhan, Wall, Yar, etc.

3.3 Concerns of Cyber Criminology

The concerns of cyber criminology as a sub-discipline of criminology cover the following three key areas:

i. **Cyberdeviance:** This refers to online behaviours and acts that are considered inappropriate or amoral but not outlawed. For example, use of vulgar language in chatrooms, use of social media language in formal email communication etc.

ii. **Cybercrime:** This refers to online behaviours or activities that are prohibited by law. For example, cyberstalking, online advance fee fraud, child pornography, credit card fraud etc.

iii. **Cyber Terrorism:** This refers to the use of the internet for the advancement of terrorist goals or for the facilitation of terrorist activities. Online malicious behaviours or activities that are politically, ideological, or religiously motivated fall under this category. For example, the recruitment or training of terrorists via the Internet.

3.4 Future Directions of Cyber Criminology

There is a growing global interest in cybercrime scholarship. According to Nhan and Bachmann (2015) with the growing social relevance of cybercrime, mainstream criminology and criminologists have started appreciating the magnitude of the problem.

They also noted that some research are conducted by those in cyber-criminological field who are mainly criminologists and lawyers. Ndubueze (2016) argued that the vulnerability window of cybercrime will increase as a result of the increased internet access worldwide and more dependence on Computer Mediated Communications (CMCs) technology and the Internet of Things (IOTs). This will raise concerns about crime and disorder in the cyberspace and result in calls for more regulations. At the end these developments will make the discipline of cyber criminology popular. Diamond and Bachmann (2017) have argued that the young discipline of cyber criminology is being boosted by the increased awareness of the wider society of the severity and devastating nature of cybercrimes and related issues through the mainstream media. They further contend that more social scientists have developed interest in cyber criminological studies, predicting that more will follow suit in the near future thereby making cyber criminology more mainstream within criminology.

Finally, some universities in the United States, United Kingdom etc. have introduced cyber criminology related programmes at Master degree level. In Nigeria, the Federal University Dutse has incorporated aspects of cyber criminology in the cyber crime course taught at the undergraduate level in the B.Sc. Criminology and Security Studies progamme. It has also included cyber criminology as a taught course in its M.Sc. Criminology and Security Studies programme. These developments will certainly boost cyber criminological scholarship.

4.0 CONCLUSION

The forces of globalization, Internet revolution, mediatization/digitization and the growth of virtual communities influenced the emergence of the discipline of cyber criminology. Cyber deviance, cybercrime and cyber terrorism which are the traditional concerns of the discipline of cyber criminology are evolving and becoming more widespread. The need to critically interrogate these emerging problems will become more critical. Cyber criminology will eventually become more mainstreamed in criminological studies.

5.0 SUMMARY

This unit discussed the context of the emergence of the discipline of cyber criminology, intellectual roots of cyber criminology, concerns of cyber criminology and future directions of cyber criminology.

6.0 TUTOR-MARKED ASSIGNMENT

Discuss the 21st century global social forces that shaped the emergence of the discipline of cyber criminology.

7.0 REFERENCES/FURTHER READING

Diamond, B. and Bachmann, M. (2017). Assessment of cyber criminology: Obstacles, Challenges and the promising path of the new science of cybercrime. In K. Jaishankar (ed.). I*nterpersonal Criminology: Revisiting Interpersonal Crimes and Victimization* (pp. 247 – 256). Boca Raton, USA: CRC Press, Taylor & Francis Group.

Jaishankar, K. (2007). Cyber criminology: Evolving a novel discipline with a new journal. *International Journal of Cyber Criminology*, 1 (1), 1-6.

Ndubueze, P.N. (2017). Cyber Criminology: Contexts, Concerns and Directions'. In P.N. Ndubueze (ed.). *Cyber Criminology and Technology-Assisted Crime Control: A Reader* (1-28). Zaria: Ahmadu Bello University Press.

Ndubueze, P.N. (2016). Cyber Criminology and the Quest for Social Order in Nigerian Cyberspace.*The Nigerian Journal of Sociology and Anthropology*. 14 (1): 32-48.

Module 2: Some Emerging Patterns of Cybercrime I

UNIT 1 CHILD PORNOGRAPHY AND CHILD SEXUAL GROOMING

CONTENTS

1.0 INTRODUCTION

Child pornography is a growing global public health and safety challenge. Sexually explicit pictures, films or other materials involving minors are increasingly been criminally advertized and distributed online. These materials are been subscribed to by pedophiles and this have profound implications for the prevalence of child sexual abuse. Abused children will undoubtedly experience post traumatic stress disorder (PTSD) and this will negatively affect their mental health.

2.0 OBJECTIVE

This unit explains the concepts of child pornography and child sexual grooming. It discusses the categories of child pornography and stages of child grooming. It also discusses the strategies for combating child sexual abuse. In Nigeria, online child pornography is criminalized under section 23 of the Cybercrime (Prohibition, Prevention etc. Act, 2015).

3.0 MAIN CONTENT

3.1 Definition of Child Pornography

According to the U.S. Code (as cited in Marcum, 2014, pp. 26 & 27) child pornography refers to a situation whereby a person:

> advertises, promotes, presents, distributes, or solicits through the mails, or using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, any material or purported material in a manner that reflects the belief, or that is intended to cause another to believe, that the material or purported material is, or contains – (i) an obscene visual depiction of a

minor engaging in sexually explicit conduct; or (ii) a visual depiction of an actual minor engaging in sexually explicit conduct.

Child pornography fundamentally refers to sexually explicit pictures, films or other materials involving a minor. Child pornography is an offense in many jurisdictions. In Nigeria, online child pornography is criminalized under section 23 of the Cybercrime (Prohibition, Prevention etc. Act, 2015).

3.2 Categories of Child Pornography

Copine Unit (as cited in Marcum, 2014, pp. 30 & 31) have developed a ten-point scale for classification of pornographic images based on the victimization suffered by the children as follows:

Level	**Name**	**Description**
1	Indicative	Non-erotic pictures of children featured in underwear, bathing suits etc.
2	Nudist	Semi-naked or naked pictures of children in appropriate nudist settings.
3	Erotica	Secretively taken pictures of children in nudist setting.
4	Posing	Deliberate posing of partially naked or entirely naked children.
5	Erotic posing	Deliberate posing of children partially clothed or entirely naked in sexual poses.
6	Explicit erotic posing	Emphasis of genitals with partially clothed or naked children.

7	Explicit sexual activity	Involvement of touching, masturbation, oral sex and intercourse with another child.
8	Assault	Children subject to sexual assault by an adult.
9	Gross assault	Obscene picture of children subject to sexual assault, sex, masturbation, or oral sex with an adult.
10	Sadistic/Bestiality	Depiction of a child being tied, bound, beaten, or whipped to inflict pain OR involvement with an animal and sexual behaviour.

The above scale shows the nature of child pornography from its mildest form to its worst form. Regardless of where any act of child pornography falls within the scale, child pornography remains an offense that is severely punished in most countries, including Nigeria.

3.3 Definition of Child Sexual Grooming

Predatory child molesters usually start their abusive activities by sexually grooming their targets. According to Craven, Brown and Gilchrist (2006, p. 297) sexual grooming is:

> A process by which a person prepares a child, significant others, and the environment for the abuse of this child. Specific goals include gaining access to the child, gaining the child's compliance, and maintaining the child's secrecy to avoid disclosure. This process serves to strengthen the offender's abusive pattern, as it may be used as a means of justifying or denying their actions.

The above definition underscores the subtle nature of child abuse. It suggests that a child parents, siblings and community can be manipulated or deceived by the abuser in order to facilitate the abuse of the child. The essence of doing this is to conceal their abusive relationship with the child.

3.4 Stages of Child Sexual Grooming

There are several stages that are involved in the sexual grooming of a child. These stages are meant to groom the targeted child in order to prepare him/her for eventual sexual abuse. Winters and Jeglic (2017) discussed the following stages of child sexual grooming:

i. **Selection of a Victim**: The first stage in grooming a child is selection of the target. The criteria for selecting the child to be groomed can be determined by appeal/attractiveness, ease of access, or perceived vulnerabilities of the child. Child molesters may consider physical characteristics of a victim or the way the victim is dressed when selecting a victim. They may also consider the victim's family situation, like those living in single family households, since they may have less adult supervision. In the same vein, children from families with alcoholic or drug addiction, emotional or mental problems, marital discords, domestic violence issues, or that are neglected are more likely to be sexually abused because they may have less parental supervision.

ii. **Gaining Access to the Potential Victim:** The second stage of child grooming process involves gaining access to the potential victim. By this the molester intends to isolate the child both physically and emotionally from those around them. Intra-familial offenders – those who commit offenses against a family member, exploiting the pre-existing relationship between them and the victim, can easily access victims in the home environment. Conversely, extra-familial offenders seek out situations where victims will be readily available, like when they go to school, shopping malls, parks, pools etc. Child molesters often seek jobs that involve children such as teachers, camp counselors, school bus drivers or coaches. When in professional settings they may create reasons to see the child after school hours or offer to take them on outings. These activities which typically do not involve other adults allow them to get the child alone.

iii. **Emotional Recruitment of the Victim:** The third stage of the grooming process involves the offender establishing trust and cooperation with the victim. In order to accomplish this, the offender befriends the child by learning about his/her interest, being helpful, showering the child with gifts and attention, or sharing secrets. These behavaiours are meant to give the child the impression that he or she is specially loved by the offender. Also, depending on the child's age, the offender may engage in peer-like activities with the child such as playing games with younger children or discussing sexual matters with teenagers. The offender may induce the child with money, treats, gifts, fun trips and so on so as to establish a special relationship with the child.

iv. **Gradual Escalation of Physical Contact with the Child:** Having acquired the trust of child, the child molester may gradually increase physical contact with the child in order to desensitize him or her to touch and also prepare the child for the sexual contact that will occur during the intended abuse. This normally begins with seemingly accidental touch or innocent behaviour, and eventually escalates to more intimate touching. The child molesters may start with hugs, pats on the back, wrestling, or back messages and eventually proceed to sexual contact. Other tactics used by child molesters include, playing hide and seek in the dark, playing strip poker, swimming nude, drying a child off with a towel, massaging an injury, playing physical games, cuddling, showing the child pornography, sneaking into the bedroom, offering a message, using sex as a game etc.

3.5 Combating Child Sexual Abuse

To effectively deal with the problem of child sexual abuse a multi-pronged approach is required. Ndubueze (2016) suggested some approaches to combat child sexual abuse below:

i. **Re-engineering of Parenting Practices:** Times have changed and so has parenting practices. The use of corporal punishment as a child correction instrument is fast declining, giving way to counseling and threat of corporal punishment. In our society today, parents need to re-enforce good behaviour with an approving smile, praise, a gift and so on, and discourage bad behaviour with a disapproving frown, shout, may be a spark or some strong disapproving conversations and in extreme cases some mild canning. It is important that parents demonstrate the good virtues they expect to see in their children. They should build a friendly relationship with their children as such relationship would enable them freely tell their parents when they are hurting or are harmed. Pedophiles persuade their victims to keep their victimization secret. They do that by for example, threatening to kill their victims if they report them to their parents or older siblings. It takes a very observant parent to know that his/her child has been sexually abused. Parents should also probe into their children undue fondness of relatives who visit or stay in their homes and as well as fondness with neighbours. Nannies and baby-sitters should also be monitored closely and nothing should be left to chance. Parents should teach their children (especially the prepubescent ones) how to relate with strangers and educate them on the dangers of accepting gifts from strangers. They should also be taught how to identify, resist and report amoral touches and advances. Working mothers' children are perhaps the most vulnerable. Parents who can afford it may install hidden Closed Circuit Television (CCTV) cameras or occasionally check home during works hours (break periods), just to know how their under-age children are faring. Interestingly, today, working mothers can monitor the activities of their baby sitters and nannies using in real-time electronic tracking devices while at work. These measures may help to prevent the abuse of their children by pedophiles.

ii. **Awareness Campaign:** Many parents are not aware of the patterns and extent of the problem of child abuse. They sometimes inadvertently facilitate the victimization of their children. Parents across all social class should be sensitized on the problem; the risk factors associated with it and how to protect their vulnerable children from victimization. Renewed advocacy by government and non-governmental organizations, television adverts, radio jingles, billboards posters and so on will help increase awareness on this problem. The penalty for child sexual abuse should also be clearly spelt out in such adverts. This would perhaps serve to discourage both perpetrators and potential perpetrators from engaging in child sexual abuse.

iii. **Religious and Moral Education:** Religion is known to re-enforces morals. Right from infancy, children should be adequately taught the religious faith of their parents. They should be encouraged to participate in their religious activities as they grow up. This will enable them to imbibe a strong moral character. Moral instruction should constitute a critical component of civic education taught in primary and secondary schools in the country.

iv. **Community Vigilance:** Community and neighbourhood associations can play an important role in the fight against child sexual abuse. There is need for them to sensitize their members on the activities of child abusers as well as it assault on their collective conscience. They should be taught the profile of a typical pedophile and their various tactics. This way, they will be able to raise alarm when one lurks their neighbourhood. They should be encouraged to report suspicious activities in uncompleted buildings in their neighbourhoods to the police especially when they see unaccompanied children within those buildings, or child-hawkers around such buildings.

v. **Legislative and Judicial Action:** There is need for more punitive measures to be taken against convicted pedophiles in Nigeria. Like what obtains in some developed countries such as the United Kingdom, convicted pedophiles in Nigeria should be blacklisted by registering their whereabouts. They should be prevented for working in places, institutions or organizations where as part of their routine job activities they will come in contact and interact closely with vulnerable children such as children in nursery and primary schools. This action should be backed by legislation. Judges should ensure that maximum punishment is melted on convicted child sexual abusers. The prevalence and upsurge of the problem should serve as an aggravating factor in sentencing.

vi. **Offenders Rehabilitation Programme:** There is need for the government and non-governmental organizations to establish special rehabilitation centres for child sexual abusers. The centre should run both psychological and other related tests on the offenders with a view diagnosing the real problem with each offender and offer appropriate treatment. Necessary follow-ups and check-up may be considered for repeat or serial child abusers by such centres.

vii. **Harm Mitigation:** An abused child may be traumatized, depressed and fearful. He or she needs help to be able to get over the harm as quickly as possible and move on with life. Such a child should be adequately counseled and effectively followed up to ensure complete recovery from the traumatic experience.

4.0 CONCLUSION

Child pornography and child grooming have become more prevalent with the proliferation of the internet and smartphones. Both problems accounts for the rise in cases of child sexual abuse. Parents and guardians are therefore expected to be conscious of the tactics employed by child molesters to groom children and prepare them for eventual sexual abuse. There is need for parents to make every effort to protect their children from such victimization.

5.0 SUMMARY

The unit looked at the definition of child pornography and child sexual abuse. It also examined the categories of child pornographic images, the stages of child sexual grooming and strategies for combating child sexual abuse.

6.0 TUTOR-MARKED ASSIGNMENT

With good examples, discuss the various stages of child sexual grooming.

7.0 REFERENCES/FURTHER READING

Marcum, C.D. (2014). *Cyber Crime*. New York: Wolters Kluwer.

Craven, S., Brown, S, & Gilchrist, E. (2006). Sexual Grooming of Children: Review of Literature and Theoretical Considerations. *Journal of Sexual Aggression*, 12(3) 287-299.

Ndubueze, P.N**.** (2016). Paedophilia and child sexual abuse in digital Nigeria: Fault lines in parenting practices. *Kaduna* J*ournal of Sociology.* 4 (4): 154 - 170.

Winters, G., & Jeglic, E.L. (2017). Stages of grooming: Recognizing potentially predatory behaviour of child molesters. *Deviant Behaviour*, 38 (6) 724-733.

UNIT 2 CYBERBULLYING, CYBERSTALKING AND CYBERSQUATTING

CONTENTS

1.0 INTRODUCTION

Bullying, stalking and squatting are phenomena that existed before the advent of internet technology. However, the emergence of the internet and smartphones has made it possible for these activities to be carried out through the internet in a speedy and anonymous manner. Today, people are chased, harassed, intimidated and humiliated online by their acquaintances and strangers. Also, people hijack the internet domain names of others, sell the address or set up an antagonistic site.

2.0 OBJECTIVE

This unit explains the concepts of cyberbullying, cyberstalking and cyberquatting. It discusses the forms of cyberbullying as well as the types of cyberstalking and cyber squatting.

3.0 MAIN CONTENT

3.1 Definition of Cyberbullying

According to Marcum (2014, p.90) "cyberbullying is intentional, aggressive behaviour that is performed through electronic means (.i.e. computers, cell phones, PDAs)"**.** For Hinduja and Patchin (2014, p.2) "it is the willful and repeated harm inflicted through the use of computers, cell phones, and other electronic devices". Cyberbullying primarily refers to the use of technological devices by adolescents to harass, threaten, humiliate and embarrass their peers. For example, a teenager can spread rumor about his/her classmate on a WhatsApp group with a view to humiliating the person. Essentially, teenagers may repeatedly make fun of others online or repeatedly pick on others through email or text messages, they may also post something online about their peers that they may consider offensive.

Although bullying is an age long phenomenon, it seems to have escalated with the proliferation of digital devices. Cyberbullying now occurs across different mediums in the cyberspace among adolescents. It is estimated that about 10 to 40 percent of youth experience bullying.

3.2 Forms of Cyberbullying

Marcum (2014, p. 90-91) identifies the various forms that cyberbullying can occur in electronic communication as follows:

i. **Harassment**: Its cyber form entails repetitive messages that are offensive to the recipient. The offender may send email or text messages insulting or taunting the victim.

ii. **Outing and Trickery**: This refers to the unintended sharing of personal information with others. A victim may have his or her Social Security number or telephone number exposed without permission.

iii. **Flaming:** This occurs in a public environment such as chat rooms or discussion board, and is a brief exchange of insults between two or more parties.

iv. **Denigration**: This has to do with posting information about another that is disparaging and untrue. For example, an offender may post on a victim's Facebook page that he is a drug addict, when in actual fact he is not.

v. **Exclusion/Ostracism:** This is the perception of feeling left out. This isolates the victim.

3.3 Definition of Cyberstalking

Stalking in the physical space basically involve unduly monitoring of a person, continuous communication, showing up at home or workplace without invitation and other forms of intimidating behaviours. Cyber stalking is stalking in an electronic form. Osayi (2017, p. 30) defined cyberstalking as "any threatening behaviour or unsolicited advances directed at unsuspecting users of the internet and other forms of online and computer communications".

3.4 Types of Cyberstalking

Nuccitelli (as cited in Osayi, 2017) identified the following types of cyber stalkers:

i. **Rejected Stalkers:** They pursue their victims so as to reverse what they consider as a wrongful set of circumstances that led to a prior divorce, separation or breaking of a relationship. The stalker may feel misunderstood and wants to restore the relationship or feel angry and seek revenge because of their past failure to reconcile with the victim.

ii. **Resentful Stalkers:** They know that their victim is aware of the stalking but continues a distorted vendetta that they consider warranted. The goal of this stalker is to cause their victim fear and distress. This is because the stalker believes that the victim should be frightened for causing him/her or others anguish and distress.

iii. **Intimacy Seekers:** They usually do have ill will towards their victims but just want to engage in a loving relationship with them. They see their victims as their soul mate and believe that they are destined to be together at all cost. Thus, being carried away by their distorted perception of destined love, they do not realize that they are causing their victim distress and fear. Intimacy seekers often harass celebrities and public figures.

iv. **Incompetent Suitors:** They are deeply in love with their victims. Their interest in their victim may get to a state of fixation whereby they are hoping to get married and become couple someday. They usually lack social, communication or courting skills and may get engrossed in their fantasy of a loving relationship. Their feeling of entitlement to the relationship with the victim encourages them to increase their frequency of contact. Unlike intimacy seekers, they are more gradual in their means and methods of contact.

v. **Predatory Stalkers:** They are motivated by a perceived sexual need. Their preoccupation is how they will engage in sexual act (s) with their victim. They neither have feeling of love for their victim nor are they motivated by the belief of predestination. They are the most dangerous and determined of the five categories as they actively plan an attack against their victims.

The above classification of stalkers shows that stalking behaviour can be driven by different motives. It also demonstrates how desperate some stalkers can be and the extent they can go to achieve their sinister goals. It is believed that once offenders become comfortable at stalking a person online, they can move to the physical space for potentially more threatening forms of stalking.

3.5 Definition of Cybersquatting

Cybersquatting refers to the act of buying internet domain names that are linked to other people's trademarks or intellectual property. According to Section 25, Sub-section (1) of the Cybercrime (Prohibition, Prevention etc.) Act, 2015:

> A person who, intentionally takes or makes use of name, business name, trademark, domain name or other word or phrase registered, owned or in use by any individual, body corporate or belonging to the Federal, State or Local Government in Nigeria, on the internet or any other company network, without authority or right, and for the purpose of interfering with their use by the owner, registrant or legitimate prior user, commits an offence under this Act and is liable on conviction to imprisonment for a term of not more than 2 years or a fine of not more than N5,000,000.00 or both.

3.6 Types of Cybersquatting

There are different types of cybersquatting. Jain (2015) identified three types of cybersquatting as follows:

i. **Typo Squatting**: This refers to the act of registering several popular trademarked names by cyber squatters.

ii. **Identity Theft**: Internet domain names are re-registered with an internet registrar prior to their date of expiration. This is because the domain name can be purchased by someone else once it expires. However, a cybersquatter can use automated software tools to register the expired name immediately it expires. This tactics is a variant of identity theft schemes including renewal snatching, extension exaggeration and alert angling.

iii. **Name Jacking:** This refers to the act of purchasing an individual's name as a top-level domain name, for example John Jones = Johnjones.com. Setting up a website makes it possible for the purchaser to capitalize for any searches done for that name. People often search the web for information as such name jacking provides low-cost web traffic to the name-jacked website.

4.0 CONCLUSION

Cyberbullying, cyberstalking and cybersquatting are increasingly becoming prevalent in the internet age. While cyberbullying is common among young people, cyberstalking behaviours are usually associated with adults. The registration of domain name system which has become popular and commercially viable with the development e-economy has led to the incessant hijacking of other people's domain name.

5.0 SUMMARY

The unit focused on the definition of cyberbullying, cyberstalking and cybersquatting. It also discussed the forms of cyberbullying as well as types of cyberstalking and cyber squatting.

6.0 TUTOR-MARKED ASSIGNMENT

Explain the various types of cyberstalking.

7.0 REFERENCES/FURTHER READING

Jain, S. (215). Cyber Squatting: Concept, Types and Legal Regimes in India & USA . Available at SSRN: https://ssrn.com/abstract= 2786474 or http ://dx.doi.org /10.2139/ssrn.2786474

Marcum, C.D. (2014). *Cyber Crime*. New York: Wolters Kluwer.

Osayi, K.K. (2017). Cyberstalking, cyberbullying and cybersquatting: A conceptual analysis. In P.N. Ndubueze (ed.). *Cyber Criminology and Technology-Assisted Crime Control: A Reader* (29-46). Zaria: Ahmadu Bello University Press.

UNIT 3 DARK WEB AND CRYPTOMARKET OPERATIONS

CONTENTS

1.0 INTRODUCTION

Cybercrime is a high-technology crime that thrives on anonymity and pseudonymity. Criminals are always seeking novel ways to conceal their identities in order to avoid law enforcement tracking and arrest. The dark web allows people to utilize special software/browser that enables them to access the internet anonymously. Similarly, cryptomarkets are enabled by anonymizing technologies such as Tor networks and virtual currencies which hide the identity of participants in order to shield them from arrest by law enforcement agencies.

2.0 OBJECTIVE

This unit focuses on the concept of darkweb and examines the benefits and drawbacks of the use of dark web. It also explains the concept of cryptomarket and discusses how cryptocurrency is associated with criminality.

3.0 MAIN CONTENT

3.1 Definition of Dark Web

Cyber criminals have always sought ways to conceal their identities and illegal activities in order to avoid detection by law enforcement. This quest for anonymity which is one of the attributes of cybercrime is provided by the dark web. The dark web is basically a collection of several websites that utilize special software/browser such as Tor (The Onion Router) and I2P to hide their Internet Protocol address. This is to enable users to access the sites anonymously. The dark web is highly patronized by people who engage in criminals activities as it offers them a platform on which to carry out their clandestine online activities away from government scrutiny.

3.2 Benefits and Drawbacks of the Dark Web's Use

According to Chertoff (2017) it is not all those who access the dark web do so for illegal purposes. He noted that some people who reside in a country where free and open access to the internet is not allowed may use Tor to browse the surface web anonymously, some may use it because of privacy concerns and others use it to perform Deep Web research. He further identified some benefits and drawbacks of using the dark web.

Chertoff (2017) explained that the creators of Tor are the strong advocates of Tor as they believe that it is useful to human rights activists who use them to access Facebook or to blog anonymously. Tor advocates also acknowledge the importance of anonymity in the protection of human rights activists in authoritative regimes; even though this anonymity poses some challenges to law enforcement agencies. Tor is also considered beneficial because it is used by many people to protect browsing privacy such as enabling people access a collection of e-book of subversive works on the dark web and allowing journalists share negative stories about authoritarian regimes.

Furthermore, Chertoff (2017) stated some of the drawbacks of the use of the dark web. He noted that it is impossible to create a tool that allows users to browse anonymously, and at the same time be able to track their activity to ensure that they do not access illegal websites. He went on to argue that while those who created Tor may think that the browser is mainly used by journalists who write stories from countries that do not have laws that protect press freedom, the fact remains that majority of Tor traffic is associated with viewing and distribution of child abuse images and purchasing of illegal drugs.

3.3 Definition of Cryptomarkets

The landscape of illegal drug business has been altered with the development of internet technology which eventually enabled the creation of new drug market known as cryptomarket. In order to understand the concept of cryptomarket it is important to first look at the meaning of cryptography. According to Paar and Pelzl (2010, p. 3) “cryptography is the science of secret writing with the goal of hiding the meaning of a message”. The above definition clearly suggests that the essence of using cryptographic writing is to mask the meaning of the writing in order to perhaps remain anonymous. Decray-Hetu, Mousseau and Vidal (2018) defined cryptomarkets as online illicit marketplaces for the advertisement and sale of illicit drugs by drug dealers using anonymizing technologies such as Tor networks and virtual currencies which mask participants’ identity and protect them from arrest by law enforcement agencies.

Cyber criminals are exploiting innovative ways of covering their tracks in order to escape law enforcement searchlight and therefore find it convenient to buy and sell various illegal goods and services in crypto markets. The market seems to be well structured with expectations clearly defined between operators. But the market facilitates crime and criminality.

3.4 Cryptocurrency and Criminality

Cryptocurrency is an encrypted independent virtual currency that can be used for anonymous international and instant payment. Cryptocurrencies and particularly Bitcoin have become increasingly popular and used for investment purposes. Brown (2016) argued that while there is nothing inherently criminal in the development of cryptocurrency, the absence of independent regulation and the chances of evading anti-money laundering principle of ‘know your customer’ have made it attractive to criminals. He further pointed out that the United States Federal Bureau of Investigation (FBI) in a 2012 assessment identified Bitcoin as specially susceptible to illicit money transfers, and manipulation through the use of malware and botnets.

3.5 Challenges for Formal Governance of Bitcoin

Crypotocurrencies are not under the regulatory control of central bank of states. This undoubtedly has profound implications for the stability of the cryptocurrency. Jia and Zang (2018) opined that although Bitcoin is not necessarily regulated by states, the expansion of its market and growing influence will make its negative effects glaring and result in a rise in its governance challenges. They identified the governance challenges as follows:

i. **Volatility**: Bitcoin is prone to market risks and volatile speculation. This is because, unlike fiat currencies, it is a decentralized peer-to-peer network that does not have a centralized authority to closely monitor the market changes and make necessary adjustments. Bitcoin is said to have experienced about six fluctuations since 2011. Therefore, government needs to intervene when the price fluctuation of Bitcoin adversely affects the entire economy.

ii. **Vulnerability:** Despite that Bitcoin source code is relatively simple, computer science literature suggest that its protocol cannot be hacked. A renowned computer security researcher has publicly declared that he could not hack Bitcoin protocol after attempting severally. However, it does not mean that the entire global Bitcoin network is secure. This is because applications built on the Bitcoin protocol, as well as wallets or exchanges, are very vulnerable security risks that are capable of affecting the entire system's stability.

iii. **Illegal Use:** The pseudonymous attribute of Bitcoins means that it could be used for legitimate and illegal activities. Illegal use of Bitcoin across jurisdictions is mostly associated with digital black markets and money laundering. Digital black markets involve the buying and selling of illicit goods and services. Bitcoin has created new opportunities for online black marketers because of its quasi-anonymity that makes it difficult to identify the operator and user. International money laundering constitutes another illegal use of Bitcoin. Its global network makes it easy for ill-gotten money to be transmitted across national borders. However, Bitcoins has its drawbacks. It has a limited transaction scope. Also, its transaction records are open and accessible to the public. Even though users addresses and identifies are protected through encryption technology, law enforcement can still confirm suspects, especially when Bitcoins are exchanged with some fiat currency such as in the case of Silk Road.

4.0 CONCLUSION

The dark web which is also referred to as darknet is generally perceived as a tool used by criminals. However, the fact remains that there are people who use the dark web for other purposes. Journalists may use the dark web to access some e-book that are critical of authoritative regimes and that otherwise would be censored by the government. Also, there are people who are concerned about their privacy who use anonymous browsers such as the onion router (TOR).

5.0 SUMMARY

The unit defined the concept of dark web and examined the benefits and drawbacks of the use of dark web. It also defined the concept of cryptomarket and explained how cryptocurrency is associated with criminality.

6.0 TUTOR-MARKED ASSIGNMENT

a. Define the concept of dark web.
b. Explain the benefits and drawbacks of dark web.

7.0 REFERENCES/FURTHER READING

Brown, S.D. (2016). Cryptocurrency and criminality: The Bitcoin opportunity. Police *Journal: Theory, Practice and Principles*, 89 (4) 327-339.

Chertoff, M. (2017) A public policy perspective of dark web. *Journal of Cyber Policy*, 2 (1), 26-38.

Decary-Hetu, D. , Mousseau, V. & Vidal, S. (2018). Six years later: Analyzing online blackmarkets involved in herbal cannabis drug dealing in the United States. *Contemporary Drug Problems.* 45 (4) 366-381.

Jia, K. & Zang, F. (2018). Between liberalization and prohibition prudent enthusiasm and the goveranance of Bitcoin/blockchain technology. In M. Campbell-Verduyn (Ed.). *Bitcoin and Beyond: Cryptocurrencies, Blockchain, and Global Governance* (pp. 88-109). London: Routledge: Taylor and Francis Group.

Paar, C. & Pelzl, J. (2010). *Understanding cryptography: A Textbook for Students and Practitioners*. London: Springer Heidelberg Dordrechi.

UNIT 4 DIGITAL PIRACY

1.0 INTRODUCTION

Piracy of creative works existed before the emergence of the internet. However, the development of internet and digital technologies exacerbated the problem. Following agitations from copyright owners, the Federal Military Government promulgated into law, the Copyright Decree No.47 of 1998, which is now known as Copyright Act Cap C28 Laws of the Federation of Nigeria, 2004. The Act also established the Nigerian Copyrights Commission. The Commission has been leading the war against the theft of intellectual works of people in Nigeria.

2.0 OBJECTIVE

This unit defines the concept of digital piracy. It examines the various types of digital piracy and the economic cost of digital piracy.

3.0 MAIN CONTENT

3.1 Definition of Digital Piracy

According to Gopal et al (as cited Marcum (2014, p.12) digital piracy is “the illegal act of coping digital goods, software, digital documents, digital audio (including music and voice), and digital video for any reason other than to create a backup without explicit permission and compensation to the copy right holder”.

Digital piracy therefore entails the theft of materials online like software, music, movies and books without the consent of the legal owner of the material. These information products (i.e. software, music, movies and books) are usually regarded as being hardly excludable. This is because their creator often have difficulty excluding other persons particularly non-payers from using them. This problem may serve as a disincentive to some people who want to create digital products as they may be concerned about the difficulty in appropriating the revenue from their creative works. The internet and digital tools have facilitated an increase in digital piracy in recent years. People pirate digital products for various reasons such as for economic benefit, personal/group use or the sheer desire to prevent the product from generating the desired revenue.

Types of Digital Piracy

The various types of digital piracy as follows:

i. **Music Piracy:** This is the unauthorized downloading and sharing of music files. Music piracy is a growing problem across the world. Music piracy is perhaps of the commonest types of digital piracy. This is because of its small size when compared to video; it can be easily shared from peer to peer. It believed that digital piracy is largely responsible for the drop in the physical sale of CDs and DVDs.

ii. **Software Piracy:** This is the unauthorized copying and distribution of software that are copyrighted. It also entails downloading and installing the software more than what the software license permits. This kind of piracy can be done in several ways such as downloading, selling, sharing, and installing copies on multiple computers. Software piracy is a global problem. Its rate has risen to 88 percent in Venezuela and 77 percent in China (Marcum, 2014).

iii. **Movie Piracy:** This is the unauthorized copying and distribution of copyrighted movies. This can be done through several ways. The Motion Picture Association of America observed that majority of film piracy is committed by offenders using camcorders to record movies in theaters. These bootleg copies can be easily distributed online to thousands of consumers. There is also a peer-to-peer (P2P) network which enables internet users, through the exchange of digital files among individual computers (peers), to make files, search for file stored on other users' computers and transfer copies of the files from one computer to another. Illegal streaming sites also allow users to view illegal content (Marcum, 2014).

iv. **Online Book Piracy:** The advancement in digital technologies has facilitated the conversion of books into digital formats. This allows for easy distribution of books across the world. However, electronic books are illegally reproduced and distributed online. This growing problem has led to the deprivation of authors of the reward of their intellectual output. It has also resulted in huge losses to publishers.

3.3 Economic Cost of Digital Piracy

The economic cost of digital piracy is enormous. Aguiar and Waldfogel (as cited in Holt and Brown, 2018) observed that the recorded music revenues have dropped globally since the proliferation of file sharing technologies. This is not surprising given that peer-to-peer file sharing of music is common especially among young people. This problem is not peculiar to music as movies, software and books are also pirated. The U.S. Institute of Policy Innovation estimates a $12.5 billion yearly loss, including the loss of about 71,000 jobs. U.S. workers lose $2.7 billion in earnings annually as a result of music piracy, while their federal and state governments $422 million in tax revenues (Marcum, 2014). A study by Ahmadu (2017) which investigated the effects of book piracy on publishing in

Nigeria found that educational books, religious books, trade books, recreational books and reference books are being pirated in Nigeria and that book piracy affects investment in publishing business; discourage creativity among Nigerians; increase unemployment in publishing sector; lowers profitability to publishing companies and revenue generation to government.

4.0 CONCLUSION

Piracy of creative works is a global problem that has endured over time. Today, music, movies, software and books are more easily pirated and shared among peers than they were decades ago. This is because of the growth and proliferation of internet access and digital devices. However, this problem can be mitigated through more aggressive enforcement of the extant copyrights laws in Nigeria.

5.0 SUMMARY

This unit defined the concept of digital piracy and examined its various types. It also discussed the economic cost of digital piracy globally, including Nigeria.

6.0 TUTOR-MARKED ASSIGNMENT

With relevant examples, explain the various types of digital piracy.

7.0 REFERENCES/FURTHER READING

Ahmadu, I. (2017). Effects of book piracy on publishing in Nigeria. *Information Impact: Journal of Information and Knowledge Management*, 8 (3), 103-115.

Holt, T.J. & Brown, S.C. (2018). Contextualizing digital piracy. In S.C. Brown and T.J. Holt (eds.). *Digital Piracy: A Global Multidisciplinary Account*. London: Routledge: Taylor and Francis Group.

Marcum, C.D. (2014). *Cyber Crime*. New York: Wolters Kluwer.

Module 3: Some Emerging Patterns of Cybercrime II

Unit 1: Hacking and Malware
Unit 2: Online Advance Fee Fraud
Unit 3: Online Identity Theft
Unit 4: Sexting and Revenge Pornography

UNIT 1 HACKING AND MALWARE

1.0 Introduction

2.0 Objectives

3.0 Main Content

3.1 Definition and Types of Hacking

3.2 Classifications of Hackers

3.3 Motivations of Hacking

3.4 Definition of Malware

3.5 Classification of Malware

3.6 How Criminals Launder Banking Malware Profits

4.0 Conclusion

5.0 Summary

6.0 Tutor-Marked Assignment

7.0 References/Further Reading

1.0 INTRODUCTION

The roots of evolving hacker communities have been traced to the Massachusetts Institute of Technology (MIT) in the late 1950s. It is believed that early hackers comprised of creative young people who used their talents to build and programme MIT's early mainframes. They also reportedly developed hardware and software for existing functionalities and invented many new algorithms and applications that were incorporated into subsequent generations of computers. However, today, hackers are perceived as dangerous individuals who attack systems, steal sensitive information from other people's computers, spread virus and carry out other malicious activities. Nonetheless, it should be noted that there are ethical hackers who may hack into the system of criminals groups for some non-criminal purpose.

2.0 OBJECTIVE

This unit defines the concept of hacking, types of hacking, classification of hacking and motivation of hacking. It also defines the concept of malware, explains it classification and how cybercriminals launder profits from banking malware.

3.0 MAIN CONTENT

3.1 Definition and Types of Hacking

Hacking refers to the unauthorized access to a computer system or network. This can be done using different methods such as guessing password, using sniffer – an application that can catch password and other information and travel inside the computer or over the network, virus/worm, social engineering – which involves posing as a professional so as to gain information about the victim's computer or network etc.

Kumar and Agarwal (2018) categorized hacking into the following seven types:

i. **Inside Job**: Inside occupation involves taking passwords which are offered or used by hackers at that material time, performing mechanical secret activities, causing hurts, or conferring simple abuse.

ii. **Rouge Access Points**: These are unsecured wireless access points that can be breached without much effort. Nearby hackers usually promote access points to each other. Rouge access points are usually associated with good natured but unaware representatives.

iii. **Back Door**: Another way hackers can access a network is through exploiting back doors authoritative easy routes, setup blunders, effortlessly decoded passwords, and unsecured dial-ups. Computerized searchers (bots) can enable hackers discover any shortcoming in a system.

iv. **Denial of Service**: Denial of Service (DOS) attack enables hackers to cut down a network without increasing inward access. This kind of attack flood the access switches with sham movement which can be emailed or parceled through transmission control protocol (TCP).

v. **Distributed Denial of Service (Doss)**: Distributed denial of service attacks are facilitated denial of service assaults from numerous sources. This kind of attack is more difficult to square because it utilizes numerous, changing, source internet protocol addresses.

vi. **Anarchist, Crackers and Kiddies**: Anarchists exploit any slightest opportunity to break into a system. Crackers are professionals who break passwords to create Trojan horses or the like. They either use them for gloating rights or offer it for profit. Content kiddies have no genuine hackers' aptitudes; they simply purchase or download products and dispatch them.

vii. **Sniffing and Spoofing**: Sniffing is basically about the catching of the transmission control protocol (TCP) bundles. It can be done through quietly listening or some more malicious way. Spoofing involves sending a malicious bundle with normal affirmation, which can be figured, foreseen, recognized and acquired by the hacker through spoofing.

3.2 Classifications of Hackers

Hackers have been classified in various ways. These classifications are often informed by hackers' motivation and techniques. Kumar, Khera, Sujay, Garg and Jain (2018) classified hackers into three broad categories as follows:

i. **White Hat Hackers**: These are hackers that are authorized and paid by companies to work for the company. They are also referred to as "IT Technicians". They are used by the company that hired them to check the strength of the company's security with a view to indentifying loopholes and blocking them. Ethical hackers fall under this category as they may hack into the system of clandestine groups for good reasons.

ii. **Black Hat Hackers**: These hackers are also referred to as crackers or malicious hackers. They look out for banks and other companies with weak security, make their network less secure and steal credit card and other information from them. It is usually done for money, but sometimes it is done for fun and the organization is not harmed.

iii. **Grey Hat Hackers:** These hackers have the attributed of white and black hackers. They may find a loophole, break the security and be paid for providing its remedy. In other words, their aim of breaking into an organization's computer system without authorization is to identify weaknesses and inform the owner. These hackers who are in between the ethical and black hackers make up most of the hacking world.

Kumar et. al (2018) further identified other types of hackers to include:

- **Script Kiddies**: These are unskilled hackers who use certain tools and script to hack.
- **Suicide Hackers:** They attack any system or network because they are not bothered about being imprisoned as a result of the act.
- **Cyber Terrorists**: This category of hackers includes individuals or groups that are sponsored by terrorist or relational people. They usually target large computer networks.
- **Spy Hackers**: They are sponsored by a company to steal the trade information of another company (usually their competitor in the industry).
- **Hackivists:** These hackers may be motivated by religion or politics, or the desire to expose wrong doing, or exert revenge, or may harass their victim for their own entertainment.

3.3 Motivations of Hackers

Marcum (2014) discussed the following motivations of hackers:

i. **Addiction:** Addiction is attributed to the continued participation in hacking. The attraction in hacking is often acquired through the power felt by gaining access to forbidden areas in computer system or the knowledge gained from the access. Hackers want to keep pace with changes in technology and the security issues related to such changes.

ii. **Curiosity:** Hackers are curious to learn as much information as possible, often through inappropriate or illegal means. They can be motivated by pure curiosity of how operating systems work or the best way to crack the source code of a computer or they may just want to explore the personal information on their victim's computer.

iii. **Excitement and Entertainment**: Many hackers have claimed that their lives online are more exciting than that at work or home. Thus hackers may crack systems and codes for their own entertainment. They can move from one target to another without the intention of causing much damage.

iv. **Money:** Hackers can be financially motivated. This may be in two ways: a) for personal gain or b) to prevent large companies from financial success. Today many hackers participate in financial fraud schemes by blackmailing others or stealing credit cards.

v. **Power, Status and Ego:** The media usually portray hackers as super-intelligent beings who can crack the toughest security codes. This impression is attractive to others who have hacked in popularity. Also power and status are acquired by continuing to lead on knowledge and skills in the hacking world.

vi. **Ideologies:** Given that today information gathering is so easy due to the accessibility of the Internet, hackers can obtain certain information that could change their current belief on some topics. A social movement that hackers always support is freedom of information by the general public.

vii. **Peer Recognition:** Hackers form social communities with online friends and seek recognition from these individuals. This recognition can be obtained by demonstrating their level of knowledge and skills.

viii. **Revenge:** The hacker may decide to attack the victim as a payback for the wrong done him/her. Such attacks are usually effective if the hacker attacks an individual or organization that is not skilled enough to counter-attack, or quickly prevent the attack.

3.4 Definition of Malware

Malware (the short form of malicious software) refers to software that is created or used to exploit the loopholes in a computer system in order to gain unauthorized access to it, disrupt its operation or steal sensitive information from it.

3.5 Classification of Malware

There are different types of malicious software. Zalavadiya and Sharma (2017) categorized malware based on their propagation processes and reaction in the infected system as follows:

i. **Contagious Threats**

- **Virus**: This is a kind of malware that takes unauthorized control of the infected computer and cause harm such as performance degradation and Denial of service (DOS) without the user's knowledge. Virus programmes are hidden in another harmless programme like executable file and this way infection is spread from one computer to another.
- **Worm**: Worms are malicious software that can operate independently without hooking itself to propagate. They exploit security loopholes in computer or network resources and spread through storage devices such as USB devices, or communication media such as emails. They consume large portion of systems memory and affect network performance.

ii. **Masked Threats**

- **Trojan:** This is a dangerous malware that hide itself and acts like a legitimate programme so as to take unauthorized control of the computer or system. Trojan can be downloaded or copied through user activity such as downloading a file from the internet or other devices. It can result in the stealing of password or login details, digital money theft, deletion/modification of files and monitoring of user activity.

- **Backdoors**: They enable the attacker to bypass the normal security controls and gain unauthorized access. Backdoors are installed through programmes or other malicious activities. They result in the modification and deletion of system file and system activity monitoring.
- **Adware**: This kind of malware provides advertisers with information about users browsing habits with a view to enabling the advertiser provide targeted adverts. They spread through websites and cause clickjacking, phishing, or create malicious activity using browser.
- **Rootkits**: They are the masking techniques for malware that are designed for malicious intent of the programme. They can be installed through a software exploit or Trojan. They steal password or install keyloggers.

iii. **Financial Threats**

- **Ransomware:** This is software that blocks access to a targeted computer system until a sum of money is paid as ransom. It can spread or be delivered through social engineering or user interaction such as opening a malicious email attachment or clicking on a malicious link in an email or a social network site.
- **Spyware:** This kind of malware tracks the activity of users without their knowledge and sends sensitive information to the attacker. Spyware can be installed with other software such as freeware or dropped by Trojans. This can result in sniffing network interface, digital certificate, encryption key and other sensitive information compromise.
- **Keylogger:** It secretly record keystrokes. It can be installed by another malicious programme or by visiting an infested site. It can capture user’s sensitive information such as username, password, credit card number etc.

iii.6 How Cybercriminals Launder Banking Malware Profits

Banking malware is malicious software designed to steal money from victim's bank accounts through manipulating the bank transfers that the victim makes through online banking. Custers, Pool and Cornelisse (2018) observed that after generating profits through banking malware cybercriminal launder such profit so at to conceal its illegal origin and avoid its confiscation. They pointed out that profits of banking malware are normally in digital profits such as digital Euros, dollars etc. in an online banking environment. Therefore, in order to launder such profits cybercriminals will first transfer it from that environment to where they want. They also opined that besides the aforementioned traditional laundering methods, cybercriminals can employ other two models: a) the use of money mules and quick cash out, and b) direct spending of the profit in online banking environment.

4.0 CONCLUSION

Unlike in its early days when it was basically used for inventions and innovations, today hacking is used not only by individual criminals but also by many organized cyber criminal networks to illegally access computer systems and networks to achieve some criminal goals. Malware is also increasingly been used by cyber criminals to illegally access computer systems and networks, steal users sensitive information including financial information and monitor their activities without their knowledge. This problem is complicated in many developing countries such as Nigeria where many people are not conversant with the workings of digital technologies and how vulnerable they are to cyber victimization.

5.0 SUMMARY

This unit explained the concept of hacking and its various types as well as classification and motivation of hacking. It also explained the concept of malware, its classification and the various ways cybercriminals launder profits from banking malware.

6.0 TUTOR-MARKED ASSIGNMENT

a. Define the concept of hacking.

b. Explain the various motivations of hackers.

7.0 REFERENCES/FURTHER READING

Custers, B.H.M., Pool, R.L.D., & Cornelisse, R. (2018). Banking malware and the laundering of its profits. *European Journal of Criminology*, 1-18.

Kumar, D. et. al. (2018). Towards the impact of hacking on cybersecurity. *IOABJ*, 9 (2) 61-77.

Kumar, S. & Agarwal, D. (2018). Hacking attacks, methods, techniques and their protection measures.*IJSART*, 4 (4) 2253-2257.

Marcum, C.D. (2014). *Cyber Crime*. New York: Wolters Kluwer.

Zalavadiya, N. & Sharma, P. (2017). A methodology of malware analysis, tools and techniques for windows platform – RAT Analysis. *International Journal of Innovative Research in Computer and Communication Engineering*, 5 (3) 5042-5054.

UNIT 2 ONLINE ADVANCE FEE FRAUD

1.0 INTRODUCTION

Advance fee fraud also referred to “419 scam” is an age-long problem that existed in different forms before the coming of the internet. Criminals used various deceitful ways in the pre-internet era to rip-off their targets of their hard-earned money. However, with the emergence of the internet and proliferation of smartphones advance fee fraud is now perpetrated online. It has become very prevalent and more transnational in terms of its perpetration and victimization.

2.0 OBJECTIVE

This unit explains the concept of advance fee fraud and its various types. It also explained the elements the elements of advance fee fraud.

3.0 MAIN CONTENT

3.1 Definition of Advance Fee Fraud

In order to understand the concept of advance fee fraud, there is need to first examine the concept of fraud. Well (2011) defines fraud as any crime of gain that uses deception as its main tactics. He identified the following four elements under the common law that must be present before an act can be considered as fraud:

i. A material false statement
ii. Knowledge that the statement was false when it was made
iii. Reliance of the victim on the false statement
iv. Damaging resulting from the victim's reliance of the false statement.

The foregoing elements underscore the critical role of deception in fraudulent schemes. It suggests that right from the outset the offender deliberately wanted to trick the victim. This is because having known that a statement is false, the offender goes on to present such false statement as factual to the victim. The victim, perhaps after being persuaded or manipulated by the offender believes the statement to be true, acted on it and eventually suffered some damages.

According to Whitty & Buchanan (2012) advance fee fraud involves the use of deceit by an offender to secure a benefit from the victim with the promise of a future pay-off for the victim. The benefit that is secured from the victim is usually financial in nature and the promised pay-off may be a financial reward or a romantic relationship. In Nigeria, advance fee fraud is criminalized under the Advance Fee Fraud and Other Fraud Related Offences Act, 2006 as well as under the Cybercrime (Prohibition, Prevention Etc.) Act, 2015. The online variant of advance fee fraud popularly known as "yahoo-yahoo" and its advanced form where offenders also use fetishism, referred to as "yahoo-plus" has become widespread in Nigeria.

3.2 Types of Advance Fee Fraud

There are various types of advance fee fraud schemes used by fraudsters to defraud their victims. Some of these scams include:

i. **Romance Scam**: Romance scam is a variant of advance fee fraud that is based on a romantic relationship between the fraudster and the victim. In this scam, the fraudster enters into a romantic or dating relationship with the victim. Although the contact and interactions can be done in-person, with the internet revolution and in order to ensure the anonymity of the offender, it is increasingly done via email or the social media. Single or divorced foreigners are usually targeted by romance scammers.

ii. **Lottery Scam**: In the lottery scam the fraudsters may float a bogus lottery scheme that is targeted at gullible members of the public. They may also contact targeted victims whom they inform of their emergence as lucky winners of a lottery and demand an advance fee to enable them process their rewards. The gullible victims may pay the requested money and never get to hear from the fraudster again. The victim will eventually realize that he/she has been swindled.

iii. **Investment Scam**: This involves the advertisement of bogus investment opportunities to the public or some targeted individuals or groups. Those who respond to such adverts are deceived into making advance payments which the fraudster criminally coverts to his advantage. Investment scams are not new in Nigeria as they have always existed in diverse shades and forms and have been part of the painful experiences of the most gullible among the citizenry. Example of this kind of scam in Nigeria is the Ponzi scheme.

iv. **Inheritance Scam**: The scam is about the inheritance of the estate of a deceased person. The fraudsters usually come up with a story about a wealth individual or a politician who died suddenly. They may claim that the deceased did not have a spouse or child to claim his/her estate and did not write a will. The target may be made to believe that he or she bears the same surname with the deceased and therefore can be assisted to claim the estate. An advance payment is requested and collected for the purpose of facilitating the inheritance of the estate. The fraudster disappears and cut-off all communication channels with the victim after receiving the payment. Foreigners usually fall for this kind of scam.

v. **Employment scam**: Nigeria has a growing youth unemployment problem. This problem is exploited by employment racketeers who operate both offline and online to defraud gullible citizens. Today, there are many fake recruitment firms in Nigeria who exploit the desperation of unemployed job seekers to collect fees from these applicants for non-existing positions.

3.3 Elements of Advance Fee Fraud

Nwokeoma, Ndubueze and Igbo (2017) identified the following five basic elements of advance fee fraud:

- **Criminal Intent:** This presupposes that the offender from the outset intended to defraud the victim.
- **Deception:** This implies that there was a deliberate misrepresentation of facts by offender to the victim.
- **Criminal Gain:** The offender must have succeeded in obtaining something of value from the victim through illegal means.
- **Unfair Loss:** The transaction between the offender and the victim must have resulted in an unfair loss of something of value to the victim.
- **Pain:** The said loss must have caused the victim some form of pain or grief. This pain may be immediate or otherwise.

Therefore, for any act to qualify as advance fee fraud in the strict sense of the word, it must be characterized by the above listed basic elements. These elements are applicable to both offline and online advance fee fraud popularly known as *yahoo yahoo.*

4.0 CONCLUSION

Advance fee fraud is a continuing problem in Nigeria. It is driven by the get rich quick syndrome that is fall-out of the idolization of wealth in the contemporary Nigerian society. Today, online advance fee fraud is glamorized in songs and many young people are carried away by the flamboyant lifestyle of advance fee fraudsters such as use of exotic cars, designers wears and so on,

5.0 SUMMARY

This unit explained the concept of advance fee fraud and its various types. It also explained the elements of advance fee fraud.

6.0 TUTOR-MARKED ASSIGNMENT

Define advance fee fraud and explain its various types.

7.0 REFERENCES/FURTHER READING

Nwokeoma, B.N., Ndubueze, P.N. and Igbo, E.U.M. (2017). Precursors of Online Advance Fee Fraud in South-East Nigeria. In P.N. Ndubueze (ed.). *Cyber Criminology and Technology-Assisted Crime Control: A Reader* (195-218). Zaria: Ahmadu Bello University Press

Wells, J.T. (2011). *Principles of fraud examination* (3rd ed.). New Jersey: John Wiley & Sons, Inc.

Whitty, M. & Buchanann, T. (2012). The online romance scam: a serious cybercrime. *Cyberpsychology, Behvaiour and Social Networking* 15 (3) 181-183.

UNIT 3 ONLINE IDENTITY THEFT

1.0 Introduction

2.0 Objectives

3.0 Main Content

3.1 Definition of Online Identity Theft

3.2 Types of Online Identity Theft

3.3 Techniques of Online Identity Theft

3.4 The Cost of Identity Theft Victimization

4.0 Conclusion

5.0 Summary

6.0 Tutor-Marked Assignment

7.0 References/Further Reading

1.0 INTRODUCTION

The internet revolution has created new opportunities for identity thieves. The nature of internet activities has made it possible for vast amounts of personal information of individuals to be stored online. Identity thieves are leveraging on this to steal and use people's personal information for various fraudulent activities. Identify theft and impersonation is criminalized under section 22 of the Cybercrime (Prohibition, Prevention, Etc.) Act, 2015.

2.0 OBJECTIVE

This unit explains the concept of online identity theft, types of online identity theft, techniques of online identity theft and the costs of identity theft victimization.

3.0 MAIN CONTENT

3.1 Definition of Online Identity Theft

According to Reyns (2013) the term “Identity theft” is used to categorize several offenses involving the fraudulent use of an individual’s personal information for criminal purposes and without their consent. He further pointed out that crimes typically associated with identity theft include credit card fraud, banking fraud, and document fraud, and so on.

Furthermore, the Canadian Internet Policy and Public Interest Clinic (CIPPIC) (2007, p.1) opined that identity thieves are likely to steal the following personal information:

- Credit card numbers
- CW2 numbers (the back of credit card)
- Credit reports
- Social Security (SIN) numbers
- Driver’s license numbers
- ATM numbers
- Telephone calling cards
- Mortgage details
- Date of birth
- Password and PINs
- Home addresses
- Phone numbers

Online identity theft also known as “cyberspace identity theft” refers to the unauthorized collection and use of an individual’s personal information that is facilitated through the internet. In the digital age, identity thieves do not necessarily need to meet their victim in-person before stealing their personal information. There is vast amount of personal information of individuals that are on the internet. It is believed that that an increasing number of cases of identity theft involve the theft of personal information of individuals through the Internet. These cases of identity fraud take many forms, and involve various aspects of internet use (e.g., e-mail, banking), with offenders increasingly finding new ways to access their targets personal information.

3.2 Types of Online Identity Theft

There are several types of online identity theft. Manap, Rahim and Taji (2015) identified the following cyberspace identity theft.

i. **Financial Identity Theft**: This refers to the unauthorized use of another person's identity to obtain some benefits such as goods, services, and credit or to gain access to a bank account. There are two ways the thief can achieve this. The first is that the thief can use the stolen personal information to open a credit card account that gives him/her access to credit, or a checking account that allows him/her obtains bank checks in the name of the victim. The second is that the thief can access the victims existing account using his/her stolen personal information.

ii. **Medical Identity Theft:** Medical identity theft involves the use of a victim's name without his/her knowledge and permission as well as other items of information that may relate to insurance to secure medical benefits involving goods or services. It may also entail falsely securing reimbursement for goods and services that are purportedly enjoyed. This action may result in the distortion of the victim's medical records and wrongful medical decisions taken on the victim.

iii. **Criminal Identity Theft:** This entails the criminal claiming to be the victim when arrested by the police. The identity which the criminal claimed may have been processed by the government, but may have been obtained using personal information stolen from the victim. This leads to a situation whereby the criminal's real identity is concealed, while the victim is charged instead of the criminal.

iv. **Synthetic Identity Theft:** This entails the partial or full fabrication of an identity. An example of this kind of identity theft is a case where a real social security number is combined with a name, and birth date that are not those of the real owner of the social security number. Tracing crimes committed using this form of identity theft is more challenging because they are not reflected directly in the victim's record such as his/her credit report. However, they may come up as entirely new files or an auxiliary part of the credit report of the victim.

v. **Identity Cloning and Concealment:** This is a kind of identity theft where the thief impersonates another person while keeping his/her identity discreet. This may be done to maintain anonymity on personal grounds, but the motive is often to commit a crime. If the identity thief has successfully acquired false documents to pass routine authentication test, this fraud may not be uncovered. They are not seeking financial or medical gains, rather they want to gain employment or use the victim's name in all settings.

vi. **Child Identity Theft:** This involves the use of a child's social security number by an identity thief who usually preys on children or a relative to obtain some benefits like access to credit. Social security numbers of minors do not carry any information as such they are useful to identity thieves.

3.3 Techniques of Online Identity Theft

Online identity thieves employ several techniques to carry out their fraudulent activities. Some of these techniques have been examined by Manap, Rahim and Taji (2015) as follows:

i. **Phishing**: identity thieves use phishing to impersonate legitimate organizations. They can send out fake text messages, emails (spoofing) or telephone calls in the name of such organizations in order to trick victims to disclose personal information such as, full name, date of birth, credit card details etc.

ii. **Pharming, Smishing and Vishing**: Pharming also known as domain spoofing originated from the word phishing and entails using a spoofed website to lure gullible individuals into giving their personal information. It can be done in two ways. First, entries compromised computer host file sends legitimate domain names to illegitimate IP addresses. Second, weaknesses in the Domain Name System (DNS) software is exploited by the DNS positioning to gain control over the domain name of an existing website and change the numeric address. The affected website will automatically redirect internet users to the spoofed site, while their browser's address retains the original correct address. This will make them believe that the site is legitimate. Smishing involves the receipt of text messages by cell phone users from a company confirming their signing up one of its dating services for which they will be charged certain amount of money each day unless they cancel the order at the company's website. The said website is compromised by the thieves and used to steal personal information. Vishing has to do with typical spoofed email appearing from legitimate businesses or institutions, recipients are asked to call a telephone number, where their personal information such as account number or password are requested for the purpose of security verification.

iii. **Abuse of Privileged Access:** This refers to a situation where personnel of government and credit institutions who have access to databases containing personal information collude with strangers and avail them of the information. For example, a bank employee may use customers' personal information and account details to open credit accounts.

iv. **Hacking:** Hacking refers to the unauthorized access to a computer system or network. Identify thieves may hack into computer systems, networks and databases so as to steal large amounts of personal information.

v. **Fake Job Advertisement:** Identify thieves can issue fake job advertisements in order to lure people into submitting resumes containing their personal information like full names, qualifications, residential addresses, cell phone numbers, emails addresses, account numbers etc.

vi. **Use of Malware:** Identity thieves can use malware such as key loggers or other forms of spyware like Zeus to attack communications between users and their computers so as to steal personal information. The attack can also be between a user's computer and the internet or designed to interfere with Wi-Fi signals. This can lead to the diversion of emails and interception of personal information of users.

vii. **Preying on Social Network Sites:** Identity thieves can infiltrate social networking sites such as Facebook so as to collect personal information disclosed by users. For example, they can use poorly protected downloadable photographs to impersonate the victim. They may also befriend the user with a view to deceiving him/her into revealing their personal information like home address, bank account number etc.

3.4 The Cost of Identity Theft Victimization

The cost of identity theft victimization can be measured in both monetary and non-monetary terms. McNally (2012) discussed the following cost of identity theft victimization.

i. **Economic Costs:** This comprise of hard costs which are the monetary losses resulting from identity theft that is shared between identity owners and collectives. Collective victims of identity fraud can bear the losses that have to do with some activity, or decide to offset them through the marketing of personal services or commercial sale of personal information. The hard costs for a nation may come in the form of higher taxes. It also comprise of soft costs which are monetary costs which are difficult to fully estimate because of some future contingencies. Example is the ongoing but unforeseeable maintenance costs of identity theft detection technologies.

ii. **Human Costs:** This refers to the lived realities of identity theft victimization, excluding the monetary aspect. However, the distinction between economic and human cost of identity theft is difficult to draw in some cases. For example if someone loses his/her job as the result of identity theft victimization or losing his/her job and home because the person was wrongly arrested. Whilst such cases may have economic consequences, they may also have some human costs which are often intangible.

iii. **Opportunity Costs**: This comes with the closing of a social door that was once opened to a person like those that leads to a mortgage or a new job. These are regarded as the soft human costs of identity theft because of how difficult it is to calculate what the scenario would have looked like if the target was not victimized. Individuals and corporate entities may suffer opportunity cost.

iv. **Societal Costs**: The social costs of identity theft basically refer to the threats it poses to national or public security. This is as it affects social problems such as tax evasion, immigration offenses, welfare fraud or terrorism. It may also constitute a threat to national or public stability if it affects the foundation of society. A government may lose public credibility if there is a breach and this may lead to instability or insecurity in the society.

4.0 CONCLUSION

The identity theft problem is compounded by the availability of vast personal information of individuals online. In the digital age, law enforcement agencies across the world are confronted with several cases involving the fraudulent use of the personal information of individuals. The fear of falling victim of identity theft tends to discourage some individuals from doing online financial transactions such as online shopping, online banking etc. However, there are security software programmes that can assist in protecting individual users from online identity theft victimization.

5.0 SUMMARY

This unit defined the concept of online identify theft and the types of identity theft. The various techniques used by online identity thieves to obtain personal information of their victims were examined and the costs of identity theft victimization were discussed.

6.0 TUTOR-MARKED ASSIGNMENT

Discuss the various techniques used by online identity thieves to steal the personal information of their victims.

7.0 REFERENCES/FURTHER READING

CIPPIC (2007). Working Paper No.2. Techniques of Identity Theft. Ottawa: Canadian Internet Policy and Public Interest Clinic.

Manap, N.A. Rahim, A.A. & Taji, H. (2015). Cyber identity theft: The conceptual framework. *Mediterranean Journal of Social Science*, 6 (4) 595-605.

Mcnally, M. (2012). *Identity Theft in Today's World*. California: Praeger.

Reyns, B.W. (2013). Online routines and identify theft victimization: Further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency*, 50 (2) 216-238.

UNIT 4 SEXTING AND REVENGE PORNOGRAPHY

1.0 INTRODUCTION

The creation and distribution of sexually graphic images among young people have generated much concern among parents, educators and government across the world. This is because of the potential mental health, legal and other implications such behaviours may have for young people and their parents. Similarly, the non-consensual distribution of the sexual images of other people is a growing global social problem that has left victims depressed, traumatized, and humiliated. It should be noted that because of the moral panic generated by these behaviours perpetrators can be prosecuted under various related state and federal laws in many jurisdictions, including those that seem not to have expressly criminalized the acts.

2.0 OBJECTIVE

This unit focuses on the definition of sexting; nature and prevalence of sexting; forms of teen sexting; and consequences of sexting. It also covers the definition of revenge pornography; nature and prevalence of pornography and the effects of revenge pornography.

3.0 MAIN CONTENT

3.1 Definition of Sexting

According to Hassinoff (2014, p.449) sexting is the "creation and sharing of sexual images or text messages via mobile phone or internet applications". Sexting generally involves the creation and transmission of sexual texts messages, images and videos through electronic means such as cell phones, computer, digital camera or the internet to friends or others. This behaviour which is common among young people in the digital age has profound implications for their physical and mental health.

3.2 Nature and Prevalence of Sexting

Scholes-Balong, Francke and Hemphill (2016, p.1) classified sexting into six as follows:

- Sexually suggestive photos or videos;
- Photos or videos wearing lingerie;
- Nude photos or video;
- Sexually suggestive text messages;

- Text messages propositioning sex; and
- Forwarding or sending other sexts which were meant to be kept private.

Sexting usually involves teenagers sending nude or semi-nude pictures or videos of themselves to someone. These nude or semi-nude pictures are often redistributed without the permission or knowledge of the original sender. Sexing often take place within existing or desired romantic relationships and in some cases serve as a substitute to sexual intercourse. It is also believed to be generally associated with other risky behaviours such as cyberbullying and the like.

Halder and Jaishankar (2017, pp. 218 – 219) outlined the unique characteristics of sexting that differentiate it from child pornography as follows:

- Sexting is done by teenagers of adolescent age (13-18);
- In cases of sexting among teens, both the original creators and the recipient are teens. In other words in such cases adults are not participants;
- A mobile phone with a camera is the main device used for sexting;
- Adolescent teens take pictures of their nude bodies or bare private parts or genitals only and sent it to their friends either with some written messages or without any message as such;
- This may include taking pictures in compromising positions and sending them to others;
- The majority of sexting cases first start among boyfriends or girlfriends either on demand or to impress the other person;
- It can also be done by teen taking pictures of other friends, including himself or herself, and sending them to a large number of friends;

- In some cases, the self-captured or received pictures are distributed to known or even unknown individuals either by cell phone or by email and social networking sites. It is only in this stage that an adult receiver, who receives the message in bulk, accidentally becomes a participator. But the adult is never the first recipient;
- Such distribution can happen even to take revenge due to breaking of an emotional relationship;
- Sexting is mainly done by and among children of the same school; however, sometimes there can be involvement of children of different schools when they know the sender personally or through social networking sites, or even when the angry teen wants to spread the picture to a wider audience randomly;
- Sexting is done by teenagers who do not know that it can create legal trouble;
- Sexting can create terrible mental trauma on the creator as well as the recipient. It can even lead the creator to commit suicide. It can also lead some recipients to turn to instant bullies toward the creator.

There is a growing concern that youths are creating images of themselves or other minors and such images may meet criminal definitions of child pornography. In many jurisdictions, any sexually explicit images of minors under 18 years of age are regarded as child pornography, even if the minors created the images themselves.

With the growing access to digital devices and the popularity of the selfie culture, there seems to be an increase in sexting behaviour not only among young people but adults as well. A recent large scale meta-analysis that statistically summarized 39 studies published before 2017 with 110 380 participants revealed the following prevalence of sexting behaviour: sending a sext (14.8%), receiving a sext (27.4%), forwarding a sext without consent (12.0%), and having sext forwarded without consent (8.4%). The meta-analysis was based on studies conducted in the United States, Europe, Australia, Candada, South Africa, and South Korea (Strasburger, Zimmerman, Tmple, Madigan and Psych, 2019).

It has been argued that sexting behaviour can have legal, sociological and or psychological implications for the sending, receiver, and forwarder

3.3 Forms of Teen Sexting

Strasburger et. al. (2019, p.2) argued that teen sexting can be consensual or nonconsensual. They explained that consensual teen sexting involve:

i. **Purely consensual, from one teen to another**: Though potentially risky given that digital images can be permanent (eg, even Snapchat sexts can be intercepted by third-party applications), it falls within the context of normative adolescent sexual development and brain maturation. Concerning this latter point, the human brain is not fully mature until age 25 years or older, especially areas of the frontal cortex (dealing with judgment) and the limbic system (dealing with impulsiveness).

ii. **Consensual but coerced sexting**: This may involve pressure to engage in other sexual activities and could be a legitimate topic for ongoing discussions about implicit and explicit sexism as well as acceptable and consensual sexual behaviour. A more precise definition of what constitutes coercion and the degree to which it is consensual is critical to the understanding of this form of sexting.

They further explained that nonconsensual teen sexting (which entails anything that goes beyond the boundary of the initially intended teen recipients) involve:

i. **Disseminated sexts**: This occurs when a sext has been disseminated against the wishes of one of the partners or without the initial sender's knowledge (eg, forwarding of sexts and revenge porn). Although the prevalence of this form of sexting is lower than that of consensual sexting, the implications are qualitatively and potentially more given their nonconsensual nature

and resulting psychosocial consequences (embarrassment, shame, and rejection).

ii. **Sextortion**: Sextortion is an emerging phenomenon which involves the threatened dissemination (for money, sex, or more images) of explicit or embarrassing sexual images without consent.

iii. **Teen sexts that have been requested or accessed by an adult:** This behavior fits within the traditional definition of child pornography except in "Romeo and Juliet" cases, in which a statute prohibits prosecution or provides an affirmative defense to prosecution if the parties are close enough in age as defined by the statute.

3.4 Consequences of Teen Sexting

There are several negative consequences associated with of teen sexting. Some of these consequences include:

i. Depending on the jurisdiction, teen sexting can be prosecuted by state and federal laws. Prosecution may destabilize the affected teen and their families. It may cause them emotional pains and financial loss.

ii. Sexting may violate the privacy of those who engage in it. This is because images or videos sent by mobile phones or through the internet can get into wrong hands. Once this happens they may eventually go viral.

iii. Sexts that are exposed to audience that they are not intended for will damage the reputation of the teens involved.

iv. Sexting may be associated with various risky sexual behaviour such as cyberbullying, child pornography etc.

v. Victims of sexting may be exposed to potentials online predators and may suffer depression that may cause them to contemplate or commit suicide.

3.5 Definition of Revenge Pornography

Revenge pornography also known as “non-sensual pornography” refers to the sharing of sexually graphic image or video of a person without his or her consent. Often times this distribution is done by a partner with whom the person shared an intimate relationship without the consent of such partner after the relationship is severed. It may also be distributed by hackers seeking revenge or entertainment or simply by mischief makers.

3.6 Nature and Prevalence of Revenge Pornography

Revenge pornography which is also called “revenge porn” typically involves the distribution of private sexually graphic images of other people without their knowledge and consent. The sources of these images may include:

- Images obtained within the context of an intimate relationship (including those taken by the victim but not intended for the consumption of a third party).

- Images of the victim illegally obtained through spy cameras. For example, hidden cameras can be installed in a restroom used by the victim without the victim’s knowledge.

- Images stolen from the victim’s cell phone, computer or other electronic devices. The victim’s cell phone, computer or other electronic devices can be hacked with a view to obtaining such images without the victim’s knowledge.

- Morphed images of the victim (i.e. the victim face is copied, cropped and pasted on the body of another person engaged in an explicit sexual act).

The motivation for revenge pornography varies and includes the following:

- To harm an ex-romantic partner after the termination of the intimate relationship.

- To bully, harass, humiliate, shame or intimidate the victim.
- To entertain the perpetrator (s) not minding the harm it may cause the victim.
- To generate revenue. The perpetrators here run it as profit making venture.

It is widely believed that the perpetrators of revenge pornography are usually boys and men and the victims' are girls and women. However, this is not always the case as girls and women can sometimes be perpetrators and boys and men may also fall victim of revenge pornography.

3.7 The Effects of Revenge Pornography

Revenge pornography has some devastating implications for its victims. Scholars have identified some of these effects to include:

- Victims of revenge pornography suffer posttraumatic stress disorder (PTSD). They reported depression, lack of trust, feeling out of control, loss of confidence, loss of self esteem, anxiety and engaging in a combination of positive and negative coping mechanisms (Bates, 2017).
- Revenge pornography can significantly affect the mental health of victims. They must cope with long-term personal and psychological effects as the disseminated images may haunt them for the rest of their lives (Kamal, William & Newman, 2016).
- The distribution of images with personal details of the victims, such as full name, address and social media profile link may expose victims to stalking, sexual harassment and rape (see, Starr & Lavis, 2018).

4.0 CONCLUSION

Sexting and revenge pornography are emerging types of cybercrimes that have become increasingly prevalent with the development of smartphones and other potable electronic devices that allow people to create, record and disseminate images with ease. These behaviours which are criminalized in most jurisdictions have profound implications for the mental health of victims.

5.0 SUMMARY

This unit explained the term sexting, the nature and prevalence of sexting, forms of teen sexting and the negative consequences of sexting. It also explained the concept of revenge pornography, the nature and prevalence of revenge pornography and the negative effects of revenge pornography on its victims.

6.0 TUTOR-MARKED ASSIGNMENT

a. What are the unique characteristics of sexting?

b. Explain the negative effects of revenge pornography.

7.0 REFERENCES/FURTHER READING

Bates, S. (2017). Revenge porn and mental health: A qualitative analysis of the mental health effects of revenge porn on female survivors. *Feminist Criminology*, 12(1), 22–42.

Halder, D. & Jaishankar, K. (2017). Sexting among teens: Are they victims or offenders.. In K. Jaishankar (Ed.). I*nterpersonal Criminology: Revisiting Interpersonal Crimes and Victimization* (pp. 215 – 232). USA: CRC Press, Taylor & Francis Group.

Hassinoff, A.A. (2014). Sexting as media production: Rethinking social media and sexuality. *New Media and Society*, 15 (4) 449-465.

Kamal, M., & Newman, W.J. (2016). Revenge pornography: Mental health implications and related legislations. *The Journal of the American Academy of Psychiatry and the Law*, 4 (3) 359-367.

Scholes-Balong, K., Francke, N. & Hemphill, S. (2016). Relationships between sexting, self-esteem, and sensation seeking among Australian young adults. *Sexualization, Media & Society*, 1-8.

Starr, T.S. & Lavis, T. (2018). Perception of revenge pornography and victim blame. *International Journal of Cyber Criminology*, 12 (2) 427-438.

Strasburger, V.C., Zimmerman, H., Temple, J.R., Madigan, S., & Psych, R. (2019). Teenagers, sexting, and the law. *PEDIATRICS*, 143 (5) 1-9.

Module 4: Theories of Cybercrime and their Applicability

UNIT 1 DIFFERENTIAL ASSOCIATION THEORY (DAT)

1.0 INTRODUCTION

The differential association theory is a variant of learning theories. Learning theories argue that criminal behaviour is learned in much the same way that other kinds of behaviour are learned. Sutherland’s differential association theory argues that criminal behaviour is learned through intimate group interaction and not inherited.

2.0 OBJECTIVE

This unit focuses on the background of differential association theory, the nine propositions of the theory, the strengths and weaknesses of the theory as well as its applicability to cybercrime.

3.0 MAIN CONTENT

3.1 Background of the Differential Association Theory

Edwin Sutherland (1883 – 1950) developed the differential association theory (DAT) in 1939 in the third edition of his book titled: *Principles of Criminology*. He was influenced by the work of Shaw and Mckay on the geographical distribution of delinquency in Chicago; the work he did with Sellin, Wirth, that found that crime in modern societies was a fallout of conflicts between different cultures and his work on professional thieves, which indicated that for one to become a professional thief, the person must join a group of professional thieves and learn from them. The differential association theory was revised in the fourth edition of *Principles of Criminology* in 1947.

3.2 Propositions of the Differential Association Theory

Sutherland (1947, pp.6-7) outlines nine propositions that describe the process by which an individual engages in criminal behaviour.

i. *Criminal behavior is learned*.

ii. *Criminal behaviour is learned in interaction with other persons in a process of communication*.

iii. *The principal part of the learning of criminal behaviour occurs within intimate personal groups*.

iv. *When criminal behaviour is learned, the learning includes (a) techniques of committing the crime, which are sometimes very complicated, sometimes simple; (b) the specific direction of motives, desires, rationalizations and attitudes*.

v. *The specific direction of motives and drives is learned from definition of legal codes as favourable or unfavorable*.

vi. *A person becomes delinquent because of an excess of definitions favourable to violation of law over definitions unfavourable to violation of law*.

vii. *Differential association may vary in frequency, duration, priority, and intensity*.

viii. *The process of learning criminal behaviour by association with criminal and anticriminal patterns involve all of the mechanisms that are involves in any other learning*.

ix. *While criminal behaviour is an expression of general needs and values, it is not explained by those general needs and values, since non-criminal behaviour is an expression of the same needs and values*.

As can be seen from his nine propositions, Sutherland argued that criminal behaviour is not inherited at birth or invented by an individual but learned through interpersonal communication, which involves gestures as well as verbal interactions. He obviously did not recognize the role of the media in influencing criminal behaviour as he emphasized the role of the of intimate personal groups such as families. His argument is perhaps based on the fact that the family is a primary agent of socialization.

Furthermore, the learning includes simple and complex criminal skills, which are associated with clear-cut motives, drives, rationalization and attitudes. These are designed to prepare the individual for a potential criminal operation. The way legal codes are defined will determine the specific direction of the motives and drives of the individuals. An Individual who is surrounded by people who believe that laws are meant to be obeyed, is likely to be law abiding. However, an individual that is surrounded by people who have no regards for the law, will be lawless. But, in a society such as ours where some people are law abiding and others are not creates some kind of cultural conflict. According to Sutherland, the implication of this kind of scenario is that individuals who often come in contact with those who violate the law than those who obey the law, will end up becoming criminals. Frequency, duration, priority and intensity will influence association with criminal behaviour and association with anti-criminal behaviour. For Sutherland, the same process involved in learning non-criminal behaviour is involved in learning criminal behaviour. Finally, he opined that criminal behaviour cannot be explained by a person's needs or desires since for example, thieves steal to secure money, as honest people work to secure money.

3.3 Strengths and Weaknesses of the Differential Association Theory

Since its formulation, differential association has remained one of the dominant theories of crime. Some studies have been conducted to determine whether individuals associate with delinquents or criminal others. While it is possible for an individual to learn definitions favourable to crime from persons who are law-abiding, it is most probable that such definitions would be learnt from delinquent friends or criminal family members (Cullen, Agnew & Wilcox, 2014).

The theory has produced a consistent research finding in the delinquency literature on the relationship between peer association and delinquency. Peers are believed to play a critical role in the learning process of individuals who become criminals, even though some studies have found that those peers must not necessarily be delinquent before they can influence others to become deviant. Therefore, the effect of peer influence can be studied from both perspectives (Reid, 2015).

Fagin (2015) argued that although learning theories (including differential association theory) remain relevant in criminological thoughts and rehabilitation programs, they have failed to adequately explain why an individual chooses to learn criminal behaviour.

Igbo (2007) argued that the differential association theory may be useful in the explanation of professional theft, pick pocketing, armed robbery, hijacking, drug trafficking and many other crimes that require skills but cannot adequately explain murder, rape and assault which can be impulse driven and do not require expertise to commit.

3.4 Applicability of the Differential Association Theory to Cybercrime

Although the differential association theory was developed before the internet revolution, several studies have attempted to use it in the explanation of crime and deviance in the cyberspace. For example, Hawdon (2012) used differential association theory to explain online hate groups. He found that theory fit the current online environment and that recent trends of personalizing online experience further facilitates the fit. He argued that the personalization of online hate group visitors virtual world and tailoring of their interest will likely be directed to those who share their ideology and directed away from those who do not. This process, which may be inadvertent, will eventually increase their exposure to definitions of the world that teach them the motives for, techniques of, attitudes towards, and rationalization of hate-inspired violence. He also observed that the use of information and communication technology makes it easy for them to by-pass the control and censorship of parents, neighbours, public bodies and state officials, since they can share their opinions and goals from peer to peer. The implication is that those who habour extreme hate are more likely to find like-minded friends online than they would offline and their extreme ideology is less likely to be discovered by those who can exercise social control over them or offer a counter-ideology to discourage the hate. He concluded that the more hate groups increase online, the more likely hate-inspired groups will increase online.

Maloku (2020) showed that a wide range of empirical studies have established an association between different forms of communication that associate delinquent friends with delinquent behaviour, or youth drug use.

Walkley (as cited in Holt, 2016) examined the extent to which differential association can explain a number of cybercrimes, including hacking and online fraud. She focused on open source data and findings that have been previously reported, on whether offenders interact or operate in isolation, like learning definitions that are favourable to committing crime. Apart from observing that hackers communicate online, at conference and by telephone, she concluded that most hackers acted alone. She finally concluded that that this implies that differential association cannot be applied to all forms of fraud since some fraudsters operate alone.

4.0 CONCLUSION

Differential association theory has remained relevant in the explanation of crime decades after it was developed by Sutherland. This is despite the criticisms that have been advanced by scholars about its applicability to some types of crime. Donald Cressey after Sutherland's death, have continued to revise the theory thereby making it even more relevant to contemporary times.

5.0 SUMMARY

This unit discussed the background of differential association theory, the nine propositions of the theory, the strengths and weaknesses of the theory as well as its applicability to cybercrime.

6.0 TUTOR-MARKED ASSIGNMENT

Discuss the nine propositions of the Differential Association Theory.

7.0 REFERENCES/FURTHER READING

Cullen, F.T., Agnew, R. & Wilcox, P. (2014). *Criminological theory: Past to present*. NewYork: Oxford University Press.

Fagin, J.A. (2015). *Criminal Justice 2015.* Boston: Pearson.

Hawdon, J. (2012). Applying differential association theory to online hate groups: a theoretical statement. *Research on Finnish Society*, 5, 39-47.

Holt, T.J. (ed.) (2016). *Crime online: Correlates, causes, and context*. Durham: Carolina Academic Press.

Igbo, E.U.M. (2007). *Introduction to Criminology*. Nsukka: University of Nigeria Press.

Maloku, A. (2020). Theory of differential association. Academic *Journal of Interdisciplinary Studies*, 9 (1) 170-178.

Reid, S.T. (2015). *Crime and Criminology* (14th ed.) New York: Wolters Kluwer.

Sutherland, E.H. (1947). *Principles of Criminology* (4th ed.).Philadelphia: Lippincott.

UNIT 2 ROUTINE ACTIVITY THEORY (RAT)

1.0 INTRODUCTION

The routine activity theory is a variant of environmental criminology. Environmental criminology is a generic term for various scholarly contributions that focus on explaining crime events and the determining the casual role of opportunity. The three constructs of routine activity (i.e. offender, target and guardian) have been used by scholars to examine RAT's relevance to our understanding of crime in the cyberspace. The theory is useful in demonstrating how some online risky behaviours of internet users can expose them to motivated offenders and cyber victimization.

2.0 **OBJECTIVE**

This unit focuses on the background of routine activity theory, the major propositions of the routine activity theory, the strengths and weaknesses of the routine activity theory and the applicability of the routine activity theory to cybercrime.

3.0 **MAIN CONTENT**

3.1 Background of the Routine Activity Theory

Routine activity theory was developed by Lawrence E. Cohen and Marcus K. Felson in 1979. The theory is a variant of environmental criminology which focuses on how the features of the physical and social environment determine the availability of criminal opportunities and the eventual occurrence of crime.

According to Cullen, Agnew and Wilcox (2014) routine activity theory is anchored on two premises. First, for crime to occur, motivated offenders must meet with suitable targets while capable guardians are absent. Second, the likelihood that this scenario will occur is determined by our 'routine activities', which includes our family, work, leisure and consumption activities. Therefore, Cohen and Felson showed that these ideas can be useful in explaining the upsurge in crime in the United States after World War II.

3.2 Propositions of the Routine Activity Theory

The theory posits that structural changes in routine activity patterns influence crime rates by affecting the convergence in time and space of three elements of direct-contact predatory crimes namely: i) motivated offenders ii) suitable targets, and ii) the absence of capable guardians. The absence of any of these three elements will prevent crime from occurring. In other words, the presence of one or more of these factors creates a higher risk of victimization. They defined routine activities as "any recurrent and prevalent activities which provide for basic population and individual needs, whatever their biological or cultural origins" (Cohen & Felson, 1979, p. 593).

Motivated Offender

The first element of routine activity theory is the motivated offender. It refers to individuals who have the tendency or desire to commit crime. They are usually incentivized by the perceived benefits that will accrue to them from committing the crime. Routine activity theory assumes offender motivation is constant, and as such does not explain why offenders are motivated to commit crime. Instead, the focus is upon the offender's opportunity to act on his or her motivation. For example a teenager boy who steals an expensive smartphone from an electronic shop because he believes that carrying such an expensive phone will earn him respect from his peers.

Suitable Target

The presence of a suitable target is an important element of any criminal offense. A suitable target is an individual or a property that an offender desires to possess or to control. Target suitability is often determined by how attractive it is and is a function of a target's objective and/or symbolic value, visibility, accessibility, and other physical characteristics of the target. For example, a laptop will normally be more attractive to a potential burglar than a refrigerator. This is because it will be easier for the burglar to move the laptop than the refrigerator.

Absence of a Capable Guardian

The last element routine activity theory is the absence of a capable guardian. A capable guardian is a person or an object that can prevent crime from occurring. Targets that are lacking capable guardianship are often more attractive to offenders. Conversely, potential targets that are more heavily guarded are believed to be less attractive to potential offenders and as such are less likely to be victimized. A capable guardian may include for example, burglary proofs, Close Circuit Television (CCTV) cameras, perimeter fences, intruder alarms etc. Social guardians are another important aspect of guardianship and include other individuals such as friends, relatives, neighbours, private security guards, and law enforcement officers who may intervene on a target's behalf (Felson, 2002).

The absence of any one of the above mentioned three elements reduces the chances that victimization will occur. Thus, routine activities can inhibit, as well as facilitate victimization by affecting the convergence of motivated offenders, suitable targets, and capable guardians. Routine activity theory predicts the greatest risks for predatory crime when potential victims have high target suitability (i.e., high visibility, accessibility, and attractiveness) and low levels of guardianship. For example, low neigbourhoods are generally believed to have low crime rates, despite the availability of high value goods. This can be attributed to the availability of capable guardianship in the form of security systems, as well as a lack of motivated offenders.

3.3 Strengths and Weaknesses of the Routine Activity Theory

According to Reid (2015) researchers have demonstrated that the routine activity theory is useful in the explanation of urban homicide, the relevance of places like bars and barrooms, in the explanation of crime rates, the victimization of youths as well as single-parent families, the difference between violence among men and women, and the violence subculture. She further explained that the routine activity theory has been linked with property crime, consumer fraud as well as street robberies, and also been used to study sexual assaults of female college students.

Cullen, Agnew and Wilcox (2014) argued that the value of the routine activity theory lies in the complimentary role it plays to traditional theories of crime. They opined that the traditional crime theories basically focus on the factors that incentivize individuals to commit crime, i.e. the factors that produce motivated offenders. But, the routine activity theory takes the availability of motivated offender for granted. It rather emphasizes the opportunity for crime on the basis that unless there is opportunity, the presence of a motivated offender cannot lead to the occurrence of crime.

The routine activity theory has been criticized for its shortcomings. Finkelhor and Asdigian (1996) pointed out that RAT does not explain intimate family violence. Using the routine activity theory to explain intimate violence shows how faulty reasoning, such as improved security, can be in protecting victims from intimate crime in their own homes or that of the perpetrators. Increased police patrols, stricter law enforcement and teaching children to say no to strangers will have little impact on checking the prevalence of domestic and intimate violence.

Also, according to Vito and Holmes (1994) the explanation of the routine activity theory is not wide enough. Thus, to explain the full range of victimization, RAT needs to be modified. Concepts like exposure, guardianship, and proximity when it comes to victimization by intimates need to be seen not as aspects of routine activities, but as environmental factors that expose or protect victims from victimization.

3.4 Applicability of the Routine Activity Theory to Cybercrime

Several scholars have examined the applicability of the routine activity theory to cybercrime. Reid (2015) observed that recently, the routine activity theory has been used in the explanation of internet crimes, such as targeting potential victims of fraud, and that result indicated that the more time individuals spend on the internet, the more likely they believe that are targets of fraud.

Reyns and Henson (2016) used a nationally representative sample of individuals from the Canadian General Social Survey to examine the link between victims’ online routine activities and their online identify theft victimization. The result of the study indicated that certain routine activities directly influence possibility of identity theft victimization.

A study by Nasi, Rasanen, Kaaakinen, Keipi and Oksnen (2016) examined the relevance of routine activity theory in predicting online harassment victimization of people who are 15 to 30 years of age in the United States, Finland, Germany and the United Kingdom.

The study used logistic regression models controlled for socio-demographic factors, exposure to offenders, target suitability and absence of guardianship. The study found that between 15 percent and 20 percent of respondents have fallen victim of online harassment. Among the variables of routine activity theory tested, exposure to offenders was the only statistically significant variable in each of the selected four countries. The study also found that females were more likely to be victims than their male counterparts in Finland, but not in other countries. It was also found that immigrants are more likely to be victims in Germany, but not in other countries, and that the efficacy of guardianship was supported in the United States and Germany. The researchers therefore concluded that while routine activity is relevant in predicting online victimization, the extent to which it does so varied across countries.

Pratt, Holtfreter and Reisig (2010) examined how routine activity theory and consumer behaviour research can be used to understand how personal characteristics and online routines increase people's exposure to motivated offenders. The study which used a representative sample of 922 adults from a statewide survey in Florida found that socio-demographic characteristics influence routine online activity, such as spending time online and making online purchases. It also found that indicators of routine online activity fully mediate the effect of socio-demographic characteristics concerning the chances of being targeted for fraud online. They concluded that the findings support the routine activity theory.

Marcum, Ricketts and Higgins (2010) investigated the differences in online victimization between genders, using variables that represented the three constructs of the routine activity theory. The study administered survey to 100-level courses at a medium-sized university in the northeast of the United States. The study found that participation in behaviours that increased exposure to motivated offenders and target suitability ultimately increased the likelihood of victimization for males as well as females. On the other hand, they found that taking protective measures to improve capable guardianship was the least effective measure, because it did not reduce the chances of victimization.

4.0 CONCLUSION

Routine activity theory was originally developed for the explanation of crime in the physical space. However, recently, the theory is increasingly been used by scholars in the explanation of crime in the cyberspace. Several studies have indicated that routine activity theory is useful in the explanation of crime and deviance in the cyberspace. Therefore, RAT is one of the most frequently used criminological theories in the explanation of cybercrime. It has undoubtedly gained popularity in contemporary cybercrime discourses.

5.0 SUMMARY

This unit discussed the background of routine activity theory, the major assumptions of the theory, the strengths and weaknesses of the theory as well as its applicability to cybercrime viz-a-viz online victimization.

6.0 TUTOR-MARKED ASSIGNMENT

Discuss the applicability of the routine activity theory to cybercrime.

7.0 REFERENCES/FURTHER READING

Cohen, L.E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review,* 44, 588-608.

Cullen, F.T., Agnew, R. & Wilcox, P. (2014). *Criminological theory: Past to present.* NewYork: Oxford University Press.

Felson, M. (2002). *Crime and everyday life* (3d ed.). Thousand Oaks, CA: Sage

Finkelhor, D. & Asdigian, N.L. (1996). Risk factor for youth victimization: Beyond a lifestyle/routine activities theory approach. *Violence and Victims,* 11(1) 3-19.

Marcum, C.d., Ricketts, M.l., & Higgins, G.E. (2010). Assessing sex experiences of online vciyimzation: An examination of adolescent online behaviour using routine activity theory. *Criminal Justice Review*, 35 (4) 412-437.

Nasi, M. , Rasanen, P., Kaakinen, M., Keipi, T., & Oksanen, A. (2016). Do routine activity help predict young adults' online harassment: A Multi-national study. *Criminology & Criminal Justice*, 1-15.

Pratt, T.C., Holtfreter, K., & Reisig, M.D. (2010). Routine activity and internet fraud targeting: extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency*, 47 (3) 267-296.

Reid, S.T. (2015). *Crime and Criminology* (14th ed.). New York: Wolters Kluwer.

Reyns, B.W. & Henson, B. (2016). The thief with a thousand faces and the victim with none: Identifying determinants for online identity theft victimization with routine activity theory. *International Journal of Offender Therapy and Comparative Criminology*, 60 (10) 1119-1139.

Vito, G.F. & Holmes, R.M. (1994). *Criminology, Theory, Research and Policy*. Belmot, C.A.: Wadsworth Publishing Co.

UNIT 3 NEUTRALIZATION THEORY (NT)

1.0 INTRODUCTION

The neutralization theory explains how offenders seek to violate the norms that they believe in with little or no feeling of guilt. This they achieve by using some techniques of neutralization that provides them with some kind of justifications or excuse for their deviant behaviour. However, these justifications or excuse are not consistent with the provisions of the legal system or the larger society.

2.0 **OBJECTIVE**

This unit focuses on the background of the neutralization theory, the major propositions of the neutralization theory, the strengths and weaknesses of the neutralization theory and the applicability of the neutralization theory to cybercrime.

3.0 MAIN CONTENT

3.1 Background of the Neutralization Theory

Gresham Sykes and David Matza developed the neutralization theory in 1957. In their seminal article titled “techniques of neutralization: a theory of delinquency” they were influenced by the work of Sutherland and Cressey who argued that managers and embezzlers do some kind of rationalization. Neutralization theory is built on the exiting works on sub-cultural theories of delinquency that posits that delinquent individuals reject law-abiding norms and values and settle for an alternative set of norms that permits delinquency. Matza updated the theory in 1964.

3.2 Propositions of the Neutralization Theory

Sykes and Matza (1957, pp.664-670) identified five basic techniques of neutralization as follows:

i. *Denial of responsibility*. Insofar as the delinquent can define himself as lacking responsibility for his deviant action, the disapproval of self or others is sharply reduced in effectiveness as a restraining influence. It may also be asserted that delinquent acts are due to forces outside of the individual and beyond his control, such as unloving parents, bad companions, or a slum neigbhourhood.

ii. *Denial of injury*. The delinquent frequently, and in a hazy faction, feel that his behaviour does not really cause any harm, despite the fact that it runs counter to the law.

iii. *Denial of Victim*. Even if the delinquent accepts the responsibility for his deviant actions and is willing to admit that his deviant actions cause an injury or hurt, the moral indignation of self and others may be neutralized by an insistence that the injury is not wrong in the light of the circumstances. The injury, it may be claimed, is not really an injury; rather, it is a form of rightful retaliation or punishment.

iv. *Condemnation of condemners*. The delinquent shifts the focus of attention from his own deviant acts to the motives and behaviours of those who disapprove of his violations. By attacking others, he feels the wrongfulness of his own behaviour is more easily repressed or lost to view.

v. *Appeal to higher loyalties*. Internal and external social controls may be neutralized by sacrificing the demands of the larger society for the demands of the small social groups to which the delinquent belongs, such as the sibling pair, the gang, or the friendship clique. The conflict of the claims of friendship and the claims of law, or a similar dilemma, has of course long been recognized. If the juvenile delinquent frequently resolves the dilemma by insisting that he must ‘’always help a buddy’’ or “never squeal on a friend,” even when it throws him into serious difficulties with the dominant social order, his choice remains familiar to the supposedly law-abiding public.

The neutralization theory recognizes that most delinquents are part of the larger society; they live and carry out their daily activities within the society. Therefore, they experience the pressure to conform to the conventional norms of society like other members of society do. However, in order to circumvent these societal norms, they use techniques of neutralization. Skyes and Matza describe these techniques as justifications for deviance that are considered genuine by the delinquent, but not the legal system or larger society. Such justification can come after a deviant act has been committed so as to protect the delinquent from remorse or guilt. However, they can also come before the deviant act and facilitate it. For example, a child rape suspect may claim that it was the devil that pushed him into committing the offense. The essence of this claim is to attempt to absorb him of blame or guilt arising from the reprehensible act.

3.3 Strengths and Weaknesses of the Neutralization Theory

Neutralization theory has been supported by several researches particularly on juvenile delinquency. For example, a study by Chi-mei (2008) that used the qualitative data abstracted from semi-structured interviews with 30 Hong Kong subjects that were 10 to 17 years of age investigated the decision making of juvenile thieves. The study found that neutralization techniques significantly influenced their decision to offend and that majority of the respondents used the denial of possible risk and harm, denial of responsibility and condemnation of others to release themselves from discomfort and guilt feeling associated with criminal acts.

Also, Agnew (1994) used data from the second and third waves of the National Youth Survey to investigate the effect of neutralizations about violence on violent behaviour. The result showed that a large percentage of adolescents used neutralization to justify their violent behaviour.

However, Peretti-Watel (2003) found that the neutralization techniques listed by Matza and Sykes are not relevant to the study of cannabis use because its consumption is labeled as deviant as well as risky.

Furthermore, Greenberg (as cited in Beirne & Messerschmidt, 2015) have argued that the theory did not sufficiently consider the link between social class and socioeconomic status on the one hand and value distribution on the other hand. For example, the question of whether working-class youth are more likely to use neutralization techniques than their counterparts from other sections of the society. If they are, then why?

3.4 Applicability of the Neutralization Theory to Cybercrime

The neutralization theory has been used in the explanation of crime in the cyberspace. For example, Smallridge and Roberts (2013) in a survey administered on 304 graduate and undergraduate students examined music, movie, software, and gaming piracy using a cross-sectional survey method. Though, the findings of the survey were mixed, they showed strong support for a number of neutralization techniques, including the defense of necessity, appeal to higher loyalties, claim for normalcy, and the newly created digital rights management defiance.

A recent study by Brewer, Fox and Miller (2019) examined how individual cyber-delinquents have applied the techniques of neutralization as justification for their deviant behaviour. They found a mixed support for neutralization theory and noted that conceptual and methodological limitations that has to do with the assessment of neutralization across the existing cybercrime literature underscore the need for more research and theoretical development.

4.0 CONCLUSION

People often times seek justifications and excuses for their deviant behaviour. This is in order to possibly relieve them of the guilt that may result from such behavior or to avoid the sanction that may be melted on them for engaging in such behaviour. The neutralization theory captures the five techniques that people often employ to rationalize their deviant behaviour. This neutralization is not only restricted to offline crimes as empirical evidence have shown that it is also applied to cybercrimes.

5.0 SUMMARY

This unit discussed the background of neutralization theory, the major assumptions of the theory, the strengths and weaknesses of the theory as well as its applicability to cybercrime viz-a-viz online victimization.

6.0 TUTOR-MARKED ASSIGNMENT

With good examples, explain the various techniques of neutralization identified by Sykes and Matza (1957).

7.0 REFERENCES/FURTHER READING

Agnew, R. (1994). The techniques of neutralization and violence. *Criminology,* 32(4), 555-580.

Beirne, P. &Messerschmidt, J.W. (2015). *Criminology: A sociological approach* (6th ed.).

New York: Oxford University Press.

Brewer, R., Fox, S. & Miller, C. (2019). Applying the techniques of neutralization to the study of cybercrime. In T. Holt, A. M. Bossler (eds.), The Palgrave Handbook of International Cybercrime and Cyberdeviance, https://doi.org/10.1007/978-3-319-90307-1_22-11

Chi-mei, J.L. (2008). Neutralization techniques, crime decision-making and juvenile thieves. *International Journal of Adolescence and Youth*, 14, 251-265.

Matza, D. (1964). *Delinquency and Drift*. New York: John Wiley & Sons.

Peretti-Watel, P. (2003). Neutralization theory and the denial of risk: Some evidence from cannabis use among French adolescents. *British Journal of Sociology*, 54 (1), 21-42.

Smallridge, J. L. & Roberts, J.R. (2013). Crime specific neutralizations: An empirical examination of four types of digital piracy. *International Journal of Cyber Criminology*, 7 (2), 125-140.

Sykes, G.M., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American Sociological Review*. 22 (6) 664-670.

UNIT 4 SPACE TRANSITION THEORY OF CYBERCRIME (STT)

1.0 INTRODUCTION

Historically, conventional criminological theories have been used in the explanation of crime and deviance in the cyberspace. These theories include the ones discussed in the preceding three units: differential association theory, routine activity theory and neutralization theory among others. Whilst these theories as have been demonstrated earlier, have proven to be relevant to our understanding of cybercrime, they all have their limitations. This is partly because they were not originally designed to explain online crimes. The upsurge of crime in the cyberspace necessitated the establishment of a cybercrime specific theory. This was achieved in 2008 with the development of the space transition theory of cybercrime by Professor K. Jaishankar.

2.0 **OBJECTIVE**

This unit covers the background of the space transition theory of cybercrime, the major propositions of the space transition theory, the strengths and weaknesses of the space transition theory and the applicability of the space transition theory to cybercrime.

3.0 **MAIN CONTENT**

3.1 Background of the Space Transition Theory of Cybercrime

The Space Transition Theory of Cybercrime (STT) was formally established in 2008 by an Indian Criminologist, Professor Karuppannan Jaishankar. He first espoused the theory at the John Jay College of Criminal Justice, the University of New York, USA in 2007. However, he later published the theory in the book: *Crimes of the Internet, edited by Frank Schmallager and Michael Pittaro (2008)* and published by Prentice Hall, USA.

3.2 Propositions of the Space Transition Theory of Cybercrime

The theory focuses on the behaviour of people who exhibit their conforming and deviant behaviour in the physical space and cyberspace. Jaishankar offers intriguing reasons why people behaviours change when they move from the physical space to the cyberspace and vice versa. The propositions of the theory are as follows (Jaishankar, 2008, pp. 293-296):

i. *Persons with repressed criminal behaviour (in the physical space) have a propensity to commit crime in cyberspace, which, otherwise they would not commit in the physical space, due to their status and position*.

ii. *Identity flexibility, dissociative anonymity, and lack of deterrence factor in the cyberspace provide the offender the choice to commit cybercrime*.

iii. *Criminal behaviour of offenders in cyberspace is likely to be imported to physical space, which, in physical space may be exported to the cyberspace as well.*

iv. *Intermittent venture of offenders in the cyberspace and the dynamic spatiotemporal nature of cyberspace provide the chance to escap*e.

v. *(a) Strangers are likely to unite in cyberspace to commit crime in the physical space, (b) Associates of physical space are likely to unite to commit crime in cyberspace.*

vi. *Persons from closed society are more likely to commit cybercrime than persons from open society.*

vii. *The conflict of norms and values of physical space with the norms and values of cyberspace may lead to cybercrimes.*

The space transition theory explains how some people who occupy high positions of responsibility in the society, but who are criminally minded may resort to the cyberspace in order to carry out the criminal activities that they would not commit in the physical space. This kind of scenario is made possible because the cyberspace allows internet users to be anonymous or use pseudo identities. Besides, unlike in the physical space regulation seems to be less strict in the cyberspace and as such deviants are not easily deterred.

Furthermore, the internet revolution has changed the dynamics of crime. Today, traditional criminal gangs having realized the new criminal opportunities that the internet creates, are increasingly exploiting the internet to commit some traditional crimes such as extortion, fraud, money laundering, theft and so on more efficiently and with less risk. Their activities for example may result in cyber attacks such as distributed denial of service or may result in the physical harming of victim whom the offender first met via the social media. Also, cybercrime is not restricted by socio-temporal boundaries. Cyber criminals can launch a cyber attack within a short period of time and such attacks can affect victims in several countries of the world.

Moreover, the internet is a veritable platform for criminal recruitment and criminal training. Therefore, people who never knew themselves before can meet, for example via social networking sites and connive to commit crime in the physical space. Similarly, people who are friends in the physical space can also connive to launch cyber attacks.

People who live in open society normally have a way of venting their feeling such as demonstration and protest. But people who live in closed society do not have such option and may resort to the cyberspace. They may be engaged in different kinds of criminal activities online such as posting hate messages in blogs or cyber terrorist attacks.

Finally, the cyberspace brings together people from different nation-states. The cyberspace has its norms and values which may not conform to the norms and values of different groups of people. The conflict of norms among the people who converge in the cyberspace may eventually lead to cybercrime.

3.3 Strengths and Weaknesses of the Space Transition Theory of Cybercrime

The space transition theory of cybercrime was the first and perhaps the only cybercrime-specific theory so far developed. The proponent of the theory Professor K. Jaishankar incidentally is the founding father of the academic discipline of cyber criminology. He was particularly interested in explaining criminal behaviour in the cyberspace and was able to demonstrate that with the seven propositions of the theory. Since its establishment in 2008, several cybercrime studies have adopted the space transition theory as their theoretical framework.

One of the shortcomings of the space transition theory is that unlike conventional criminological theories, it cannot be applied in the explanation of crime in the physical space. Danquah and Longe (2011) in their study tested the propositions of the space transition theory and found some limitations in the variety of cybercrimes committed and experienced in Ghana. They therefore concluded that the theory is not applicable to all categories of cybercrime.

3.4 Applicability of the Space Transition Theory of Cybercrime

The space transition theory from the outset was designed to explain crime in the cyberspace. Each of its seven propositions is tailored to the explanation of the dynamics of crime in the cyberspace. Several works on cybercrime both theoretical and empirical over the years have demonstrated support for the relevance of the theory in the explanation of crime and criminality in the cyberspace.

4.0 CONCLUSION

A wide range of criminological theories have been used in the explanation of crime in the cyberspace, albeit with some limitations. Jaishankar's space transition theory of cybercrime is a deviation from conventional criminological theories as it is entirely focused on cybercrimes. Jaishankar stated from the outset that his theory is intended to explain only online crimes and not traditional crimes. Over a decade after its development, the theory has shown some promise in the explanation of criminal behaviour in the cyberspace. However, more empirical studies are needed to be able to further test the efficacy of the theory in the explanation of cybercrime.

5.0 SUMMARY

This unit discussed the background of space transition theory of cybercrime, the major propositions of the theory, the strengths and weaknesses of the theory as well as its applicability to cybercrime.

6.0 TUTOR-MARKED ASSIGNMENT

Discuss the propositions of the space transition theory of cybercrime.

7.0 REFERENCES/FURTHER READING

Danquah, P. & Longe, O.B. (2011). An empirical test of the space transition theory of cyber criminality: Investigating cybercrime causation factors in Ghana. *African Journal of Computing and ICT*, 4 (2), 37 – 48.

Jaishankar, K. (2008). Space transition theory of cybercrime. In Schmallagar, F, and Pittaro, M. (eds), *Crimes of the Internet* (pp.283 – 301). Upper Saddle River, NJ: Prentice Hall.

Module 5: Local, Regional and International Cyber Crime Legislations/Cyber Security Issues and Perspectives

Unit 1: Cybercrime Legislations in Nigeria and Selected African Countries
Unit 2: Regional and International Cybercrime Legislations/Regulations
Unit 3: Challenges of Cybercrime Legislations in Africa and Strategies for Improvement
Unit 4: Cybersecurity: Issues and Perspectives

UNIT 1 CYBERCRIME LEGISLATIONS IN NIGERIA AND SELECTED AFRICAN COUNTRIES

1.0 INTRODUCTION

There are several legislations that law enforcement and regulatory agencies in Nigeria can rely on in the policing of cybercrime and prosecution of cybercrime offenders. These laws include: Cybercrime (Prohibition, Prevention Etc.) Act, 2015, Money Laundering (Prohibition) (Amendment) Act, 2012, Evidence Act, 2011, National Information Technology Development Agency (NITDA), Act 2007, Advance Fee Fraud and Other Fraud Related Offences Act, 2006, Economic and Financial Crimes Commission (Establishment) Act, 2004, Nigerian Communications Act, 2003 etc. However, it is important to note that of all these laws, the Cybercrime (Prohibition, Prevention Etc.) Act, 2015 is the most comprehensive legislation on cybercrime in Nigeria. Furthermore, legislations on cybercrime in some African countries are explicit on cybercrime, while in other African countries they are not comprehensive enough.

2.0 **OBJECTIVE**

This unit discusses some of the various legislations that are related to cybercrime that law enforcement and regulatory agencies in Nigeria rely on in the combating cybercrime and related offences. It also examines cybercrime legislations in selected African courtiers: Republic of South Africa, Republic of Ghana and Republic of Kenya. At the end of the unit you will learn about the various cybercrime and related offences criminalized in these legislations and how the legislations are similar in some African countries.

3.0 **MAIN CONTENT**

3.1 Cybercrime (Prohibition, Prevention Etc.) Act, 2015

The explanatory memorandum of the Act stipulates that:

> The Act provides an effective, unified and comprehensive legal, regulatory institutional Framework for the prohibition, prevention, detection, prosecution and punishment of Cybercrimes in Nigeria. This act also ensures the protection of critical national information infrastructure, and promotes cybersecurity and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights.

The Act is arranged into eight parts (8) and fifty-nine (59) sections as follows:

Part I – Object and Application

1. Objective.
2. Application.

Part II – Protection of Critical National Information Infrastructure

3. Designation of certain computer systems or networks as critical national information infrastructure.
4. Audit and inspection of critical national information infrastructure.

Part III – Offence and penalties

5. Offences against critical national information infrastructure;
6. Unlawful access to a computer;
7. Registration of cybercafés;
8. System interference;
9. Interpreting electronic massages, emails, electronic money transfers;
10. Tampering with critical infrastructure;
11. Willful misdirection of electronic messages;
12. Unlawful interruptions;
13. Computer related forgery;
14. Computer related fraud;
15. Theft of electronic devices;
16. Unauthorized modification of computer systems, network data and system interference;
17. Electronic signature;
18. Cyber terrorism;
19. Exceptions to financial institutions posting and authorized options;

20. Fraudulent issuance of e-instructions;
21. Reporting of cyber threats;
22. Identity theft and impersonation;
23. Child pornography and related offences;
24. Cyberstalking;
25. Cybersquatting;
26. Racist and xenophobic offences;
27. Attempt, conspiracy, aiding and abetting;
28. Importation and fabrication of e-tools;
29. Breach of confidence by service providers;
30. Manipulation of ATM/POS Terminals;
31. Employees responsibility
32. Phishing, spamming, spreading of computer virus;
33. Electronic cards related fraud;
34. Dealing in card of another;
35. Purchase or sale of card of another;
36. Use of fraudulent device or attached e-mails and websites.

Part IV – Duties of Financial Institutions

37. Duties of financial institutions.
38. Records retention and protection of data.
39. Interception of electronic communication.
40. Failure of service provider to perform certain duties.

Part V – Administration and Enforcement

41. Co-ordination and enforcement.
42. Establishment of Cybercrime Advisory Council.
43. Functions and powers of the Council.

44. Establishment of National Cyber Security Fund.

Part VI – Arrest, Search, Seizure and Prosecution

45. Power to arrest, search and seize.
46. Obstruction and refusal to release information.
47. Prosecution of offences.
48. Order of forfeiture of assets.
49. Order for payment of compensation or restitution.

Part VII – Jurisdiction and International Cooperation

50. Jurisdiction.
51. Extradition.
52. Request for mutual assistance.
53. Evidence pursuant to a request.
54. Form of request from a foreign state.
55. Expedited preservation of computer data.
56. Designation of contact point.

Part VIII – Miscellaneous

57. Regulations.
58. Interpretation.
59. Citation.

The structure of the Cybercrime (Prohibition, Prevention etc.) Act, 2015 as outlined above indicates that the Act is both specific and comprehensive on cybercrime. Some laws that were hitherto used in the prosecution of cyber criminals such as the Advance Fee Fraud and Other Fraud Related Offences Act, 2006 are not as comprehensive as the Act. Also, there are some emerging cybercrimes which are captured in the Act such as cyberstalking, cybersquatting etc. Moreover, perhaps to serve as a deterrent to cybercriminals and potential cybercriminals the penalties imposed for most of the offences are relatively severe.

3.2 Advance Fee Fraud and Other Fraud Related Offences Act, 2006

The Advance Fee and other Fraud Related Offences Act, 2006 (Act N0. 14) repeals the Advance Fee Fraud and Other Fraud Related Offences Act No.13 of 1995 and the Advance Fee Fraud and Other Fraud Related Offences (Amendment), 2005. The Advance Fee and other Fraud Related Offences Act, 2006, which was enacted by the National Assembly of the Federal Republic of Nigeria on the 5th day of June 2015 is meant to prohibit and punish certain offences pertaining to advance fee fraud and other related offences and to repeal other Acts related therewith.

The Act comprise of four (4) parts and twenty-two (22) sections as follows:

Part I – Offences. It covers the following sections:

1. Obtaining property by false pretence, etc.
2. Other related offences.
3. Use of premises.
4. Fraudulent invitation.
5. Receive of fraudulent document by victim to constitute attempt.
6. Possession of fraudulent document to constitute attempt.
7. Laundering of fund obtained through unlawful activity, etc.
8. Conspiracy, aiding, etc.
9. Conviction for alternative offences.
10. Offences body corporate.

11. Restitution

Part II - Electronic Telecommunication Offences etc. It covers the following sections:

12. Duty to obtain subscriber’s name and address.

13. Duties of telecommunication Internet Service Providers and Internet Cafes.

Part III – Jurisdiction. It covers the following sections:

14. Jurisdiction to try offences, etc.

15. Possession of pecuniary resources not accounted for.

16. Power to control property of an accused person.

17. Power to make order of forfeiture without conviction of an offence.

18. Power of arrest.

19. Power to grant bail.

Part IV – Miscellaneous. It covers the following sections:

20. Interpretation.

21. Repeals the Advance Fee Fraud and Other Fraud Related Offences Act No.13 of 1995 and the Advance Fee Fraud and Other Fraud Related Offences (Amendment), 2005.

22. Citation.

The Act re-enacts a consolidated Advance Fee Fraud and Other Fraud Related Offences Act, 2006 and provides the Federal High Court, the High Court of the Federal Capital Territory, the High Court of the States, with the jurisdiction to try offences and impose penalties provided under it.

Before the enactment of the Cybercrime (Prohibition, Prevention Etc.) Act, 2015, law enforcement agencies in Nigeria such as the Nigerian Police Force and the Economic and Financial Crimes Commission relied on the Advance Fee Fraud and other Fraud Related Offences Act, 2006 and other related laws to persecute cybercriminals. It is important to note that in the early days of cybercrime in Nigeria, online advance fee fraud otherwise known as "yahoo-yahoo" was the most prevalent type of cybercrime in Nigeria. This is because broadband internet was not well developed in Nigeria and the public could only access the internet from cyber cafes. However, today, with the breakthrough in e-economy and increased internet access, other types of cybercrime have emerged.

3.3 **Other Cybercrime Related Legislations**

Apart from the Cybercrime (Prohibition, Prevention etc.) Act , 2015 and Advance Fee Fraud and Other Fraud Related Offences Act, 2006, there are other legislations that are not explicit on cybercrime but can be relied on in the policing of cybercrime and prosecution of cyber criminals. Some of these legislations include:

i. **Money Laundering (Prohibition) (Amendment) Act, 2012**. The Act amends the Money Laundering (Prohibition) No. 11 2011 to expand the scope of money laundering offences and enhance customer due diligence measure. The Act clearly prohibits the laundering of proceeds of crime and illegal activities. Section 15 (1) stipulates:

> Money laundering is prohibited in Nigeria. (2) Any person or body corporate, in or outside Nigeria, who directly or indirectly (a) conceals or disguises the origin of; (b) converts or transfers; (c) removes from the jurisdiction; or (d) acquires, uses, retains or takes possession or control of; any fund or property, knowingly or reasonably ought to have known that such property is, or forms

> part of the proceeds of an unlawful act; commits an offence of money laundering under this Act.

The penalty for contravening Section 15, Sub-section 2 is stated in Section 15 (3):

> A person who contravenes the provisions of subsection (2) of this section is liable on conviction to a term of not less than 7 years but not more than 14 years imprisonment. (4) A body corporate who contravenes the provisions of subsection (2) of this section is liable on conviction to- (a) a fine of not less than 100% of the funds and properties acquired as a result of the offence committed; and (b) withdrawal of licence. (5) Where the body corporate persists in the commission of the offence for which it was convicted in the first instance, the Regulators may withdraw or revoke the certificate or licence of the body corporate

The unlawful act which Section 15; Sub-section 2 of the Act referred to is elaborated in Section 15, Sub-section 6 of the Act:

> The unlawful act referred to in subsection (2) of this section includes participation in an organized criminal group, racketeering, terrorism, terrorist financing, trafficking in persons, smuggling of migrants, sexual exploitation, sexual exploitation of children, illicit trafficking in narcotic drugs and psychotropic substances, illicit arms trafficking, illicit trafficking in stolen goods, corruption, bribery, fraud, currency counterfeiting, counterfeiting and piracy of products, environmental crimes, murder, grievous bodily injury, kidnapping, hostage taking, robbery or theft, smuggling (including in relation to customs and excise duties and taxes), tax crimes (related to direct taxes and indirect taxes), taxes crimes (related to

> direct taxes and indirect taxes) extortion, forgery, piracy, insider trading and market manipulation or any other criminal act specified in this Act or any other law in Nigeria.

There are several organized cybercrime groups operating across the globe. These cybercriminals usually target financial institutions, businesses and other institutions. For example, they may use malware or social engineering tactics to access targeted bank accounts and make illegal fund transfers. The illegal proceeds of crime are laundered using cryptocurrencies in order to conceal it. It has been argued that cybercriminals account for 10 percent of the total illegal profits that are laundered globally.

Obviously, the laundering of proceeds of cybercrime described above which is a fraudulent activity not only contravenes the provisions of the Cybercrime (Prohibition, Prevention Etc.) Act, 2015 but also contravenes the Money Laundering (Prohibition) (Amendment) Act, 2012.

ii. **Evidence Act, 2011**

The Evidence Act, 2011 repeals the Evidence Act, Cap. E14, Laws of the Federation of Nigeria, 2004 and enacts a new Evidence Act, 2011 which applies to all judicial proceedings in or before Courts in Nigeria. The old evidence Act did not explicitly recognize electronic or computer generated documents. The implication is that electronically generated evidence was not admissible during proceedings in the court of law. However, following the enactment of the Evidence Act, 2011, electronic evidence became admissible. Section 84 (1) of the Evidence Act 2011 provides:

> In any proceeding, a statement contained in a document produced by a computer shall be admissible as evidence of any fact stated in it of which direct oral evidence will be

> admissible, if it is shown that the conditions in subsection (2) are satisfied in relation to the statement and computer in question.
>
> (2) The conditions referred to in subsection (1) are –
>
> (a) that the document containing the statement was produced by the computer during a period over which the computer was used regularly to store or process information for the purpose of any activities regularly carried on over that period, whether for profit or not, by anybody, whether corporate or not, or bay any individual.
>
> (b) that over that period there was regularly supplied to the computer in the ordinary course of those activities information of the kind contained in the statement or of the kind form which the information so contained is derived;
>
> (c) that throughout the material part of the period the computer was operating properly or, if not, that in any respect in which it was not operating properly or was out of operation during that part of that period was not such as to affect the production of the documents or the accuracy of its contents; and
>
> (d) that the information contained in the statement reproduces or is derived from information supplied to the computer in the ordinary course of those activities.

Furthermore, Section 93 of the Evidence Act, 2011 provides for the recognition of electronic signature. It stipulates:

> If a document is alleged to be signed or to have been written wholly or in part by any person, the signature or the handwriting

> of so much of the document as is alleged to be in that person's handwriting must be proved to be in his handwriting.
>
> (2) Where a rule of evidence requires a signature, or provides for certain consequences if a document is not signed, an electronic signature satisfies that rule of law or avoids those consequences.
>
> (3) An electronic signature may be proved in any manner including by showing that a procedure existed by which it is necessary for a person, in order to proceed further with a transaction, to have executed a symbol or security procedure for the purpose of verifying that an electronic record is that of the person.

The above cited sections of the Evidence Act, 2011 clearly underscores the relevance of the Act to effective prosecution of cybercrime cases. Evidence required in most cybercrime cases are electronic in nature. This means that they are often stored in computers and other electronic devices. Therefore, the retrieval and presentation of such evidence in the court of law during trial can assist the prosecutors in proving their case against a cybercrime suspect. Of course, this Act will compliment the Cybercrime (Prohibition, Prevention, Etc.) Act, 2015.

3.4 **Cybercrime Legislations in Selected African Countries**

There are cybercrime legislations in other African countries. While some of these legislations seem old and not explicit on emerging patterns of cybercrime, others are recent and quite explicit on cybercrime. Some of these legislations will be discussed below.

The Republic of South Africa - Electronic Communications and Transactions Act 25 of 2002

The Republic of South Africa - Electronic Communications and Transactions Act 25 of 2002 was assented to on 31 July, 2002 and amended by the Consumer Protection Act 68 of 2008 which became effective from 31 March, 2011. It provide for the facilitation and regulation of electronic communications and transactions; to provide for the development of a national strategy for the Republic; to promote universal access to electronic transactions by SMMEs; to provide for human resource development in electronic transactions; to prevent abuse of information systems; to encourage the use of e-government services; and to provide for matters connected therewith.

The object of the Act is listed in section 2.

> The objects of this Act are to enable and facilitate electronic communications and transactions in the public interest, and for that purpose to-
>
> (a) recognise the importance of the information economy for the economic and social prosperity of the Republic;
>
> (b) promote universal access primarily in underserviced areas;
>
> (c) promote the understanding and, acceptance of and growth in the number of electronic transactions in the Republic;
>
> (d) remove and prevent barriers to electronic communications and transactions in the Republic;
>
> (e) promote legal certainty and confidence in respect of electronic communications and transactions;
>
> (f) promote technology neutrality in the application of legislation to electronic communications and transactions;
>
> (g) promote e-government services and electronic communications and transactions with public and private bodies, institutions and citizens;

ensure that electronic transactions in the Republic conform to the highest international standards;

(i) encourage investment and innovation in respect of electronic transactions in the Republic;

(j) develop a safe, secure and effective environment for the consumer, business and the Government to conduct and use electronic transactions;

(k) promote the development of electronic transactions services which are responsive to the needs of users and consumers;

(l) ensure that, in relation to the provision of electronic transactions services, the special needs of particular communities and, areas and the disabled are duly taken into account;

(m) ensure compliance with accepted International technical standards in the provision and development of electronic communications and transactions:

(n) promote the stability of electronic transactions in the Republic;

(o) promote the development of human resources in the electronic transactions environment;

(p) promote SMMEs within the electronic transactions environment;

(q) ensure efficient use and management of the .za domain name space; and

(r) ensure that the national interest of the Republic is not compromised through the use of electronic communications.

The Act provides for sixteen (16) chapters covering: interpretation, objects and applications; maximizing benefits and policy framework; facilitating electronic transactions; e-government services; cryptography providers; authentication service providers; consumer protection; protection of personal information; protection of critical databases; domain name authority and administration; imitation of liability of service providers; cyber inspectors; cybercrime; and general provisions. Chapter XIII which is titled cybercrime comprise of the following sections:

85. Definition
86. Unauthorized access to, interception of or interference with data
87. Computer-related extortion, fraud and forgery
88. Attempt, and aiding and abetting
89. Penalties

This particular chapter of the Act that focuses on cybercrime is not comprehensive enough because when compared to for example, the Nigerian Cybercrime (Prohibition, Prevention Etc.) Act, 2015, it is obvious that it does not capture many emerging variants of cybercrime. However a comprehensive cybercrime bill is reportedly before the South African parliament and is expected to be passed into law soon.

The Republic of Ghana - Electronic Transactions Act, 2008 (Act No.772)

The Electronic Transactions Act, 2008 (Act No.772) was the first major legislation on cybercrime in Ghana. The Act provides for the regulation of electronic communications and related transactions as well as connected purposes. The Act which is enacted by the President and Parliament of the Republic of Ghana was assented to on 18th December, 2008. Section 1 provides for the object of the Act:

> The object of the Act is to provide for and facilitate electronic communications and related transactions in the public interest, and to
> *(a)* remove and prevent barriers to electronic communications and transactions;
> *(b)* promote legal certainty and confidence in electronic communications and transactions;

(c) promote e-government services and electronic communications and transactions with public and private bodies, institutions and citizens;

(d) develop a safe, secure and effective environment for the consumer, business and the Government to conduct and use electronic transactions;

(e) promote the development of electronic transaction services responsive to the needs of consumers;

(f) ensure that, in relation to the provision of electronic transactions services, the special needs of vulnerable groups and communities and persons with disabilities are duly taken into account;

(g) ensure compliance with accepted international technical standards in the provision and development of electronic communications and transactions;

(h) ensure efficient use and management of the country domain name space; and

(i) ensure that the interest and image of the Republic are not compromised through the use of electronic communications.

Sections 5 to 24 of the Act provides for the following electronic transactions:

5. Recognition of electronic message
6. Original writing
7. Admissibility and evidential weight of electronic records
8. Retention of electronic records
9. Secure electronic records
10. Digital signature
11. Equal treatment of digital signatures
12. Signing of an electronic record

13. Conduct of a person relying on a digital signature

14. Recognition of electronic certificates and digital signatures

15. Notarisation, acknowledgement and certification

16. Other requirements

17. Automated transactions

18. Dispatch of electronic record

19. Receipt of electronic record

20. Expression of intent or other statement

21. Attribution of electronic records to originator

22. Acknowledgement of receipt of electronic record

23. Formation and validity of agreements

24. Variation by agreement between parties

Furthermore, Sections 107 to 140 provide for cyber offences as follows:

107. Stealing

108. Appropriation

109. Representation

110. Charlatanic advertisement

111. Attempt to commit crimes

112. Aiding and abetting

113. Duty to prevent felony

114. Conspiracy

115. Forgery

116. Intent

117. Criminal negligence

118. Access to protected computer

119. Obtaining electronic payment medium falsely

120. Electronic trafficking

121. Possession of electronic counterfeit-making equipment
122. General offence for fraudulent electronic fund transfer
123. General provision for cyber offences
124. Unauthorized access or interception
125. Unauthorized interference with electronic record
126. Unauthorized access to devices
127. Unauthorized circumvention
128. Denial of service
129. Unlawful access to stored communications
130. Unauthorized access to computer programme or electronic record
131. Unauthorized modification of computer programme or electronic record
132. Unauthorized disclosure of access code
133. Offence relating to national interest and security
134. Causing a computer to cease to function
135. Illegal devices
136. Child pornography
137. Confiscation of assets
138. Order for compensation
139. Ownership of programme or electronic record
140. Conviction and civil claims

There are some similarities between the cybercrime offences listed above and those listed in the Nigerian Cybercrime (Prohibition, Prevention Etc.) Act, 2015.

For example, Section 131 of the Ghanaian Electronic Transaction Act, 2008 which criminalized unauthorized modification of computer programme or electronic record, is similar to Section 16 of the Nigerian Cybercrime (Prohibition, Prevention Etc.) Act, 2015 which criminalized unauthorized modification of computer systems, network data and system interference. Also, Section 136 of the Ghanaian Electronic Transaction Act, 2008 which criminalized child pornography is similar to Section 23 of the Nigerian Cybercrime (Prohibition, Prevention Etc.) Act, 2015 which criminalized cyber pornography and related offenses. However, the Nigerian Cybercrime (Prohibition, Prevention Etc.) Act, 2015 seems to be more explicit on cybercrime offenses than the Ghanaian Electronic Transaction Act, 2008. This may be largely because the Nigerian cybercrime law is a more recent legislation than its Ghanaian equivalent.

Republic of Kenya – The Computer Misuse and Cybercrime Act, 2018 (Act No.5)

The Computer Misuse and Cybercrime Act, 2018 (Act No.5) of Kenya provide for offenses that relate to computer systems; to enable timely and effective detection, prohibition, prevention, response, investigation and prosecution of computer and cybercrimes; to facilitate international co-operation in dealing with computer and cybercrime matters; and for related purposes. The Act was assented to on 16th May, 2018 and it became effective from 30th May, 2018.

Sections 14 to 47 of the Act listed the several computer and cybercrime offences criminalized under it. They include:

14. Unauthorized access.
15. Access with intent to commit further offence.
16. Unauthorized interference.
17. Unauthorized interception.
18. Illegal devices and access codes.
19. Unauthorized disclosure of password or access code.
20. Enhanced penalty for offences involving protected computer system.
21. Cyber espionage.
22. False publications.
23. Publication of false information.
24. Child pornography.

25. Computer forgery.
26. Computer fraud.
27. Cyber harassment.
28. Cybersquatting.
29. Identity theft and impersonation.
30. Phishing.
31. Interception of electronic messages or money transfers.
32. Willful misdirection of electronic messages.
33. Cyber terrorism.
34. Inducement to deliver electronic message.
35. Intentionally withholding message delivered erroneously.
36. Unlawful destruction of electronic messages.
37. Wrongful distribution of obscene or intimate images.
38. Fraudulent use of electronic data.
39. Issuance of false e-instructions.
40. Reporting of cyber threat.
41. Employee responsibility to relinquish access codes.
42. Aiding or abetting in the commission of an offence.
43. Offences by a body corporate and limitation of liability.
44. Confiscation or forfeiture of assets.
45. Compensation order.
46. Additional penalty for other offences committed through use of a computer system.

There are several similarities between the cybercrime legislation of Kenya and that of Nigeria. For example, Sections 24, 26, 29, 32 and 33 of the Kenyan Computer Misuse and Cybercrimes Act, 2018 criminalized child pornography, computer fraud, identity theft and impersonation, willful misdirection of electronic messages, and cyber terrorism respectively. Similarly, Sections 23, 14, 22, 11, and 18 of the Nigerian Cybercrime

(Prohibition, Prevention, Etc.) Act, 2015 criminalized child pornography and related offences, computer related fraud, identity theft and impersonation, willful misdirection of electronic messages, and cyber terrorism respectively. Both legislations are relatively current, even though that of Nigeria was enacted three years earlier. They both capture several emerging patterns of cybercrime.

4.0 CONCLUSION

There are several cybercrime and cybercrime related legislations in Nigeria today. With these legislations especially the Cybercrime (Prohibition, Prevention, Etc.) Act, 2015 law enforcement officers and prosecutors are better equipped to more diligently prosecute cybercriminals in Nigeria. However, cybercrime laws need to be periodically amended or reviewed to accommodate some emerging patterns of cybercrime that were not anticipated when the laws were enacted. This also becomes necessary as cybercrime by its nature is always evolving. There is also the need for relevant law enforcement and regulatory agencies in Nigeria to be fully equipped with the technical knowledge required to detect and effectively enforce these laws. Cybercrime legislations in other African countries are either comprehensive or not explicit enough. This may constitute an impediment to the effective extradition and prosecution of transnational cybercriminals. Mutual assistance and cooperation among nation-states in the fight against cybercrime may also be hampered.

5.0 SUMMARY

This unit discussed the existing cybercrime legislations in Nigeria. It specifically examined the Cybercrime (Prohibition, Prevention Etc.) Act, 2015, Advance Fee Fraud and Other Fraud Related Offences Act, 2006, The Money Laundering (Amendment) Act, 2012 and the Evidence Act, 2011. It also examined cybercrime legislations in selected African countries namely: South Africa, Ghana and Kenya.

6.0 TUTOR-MARKED ASSIGNMENT

Discuss the relevance of the Money Laundering (Amendment) Act, 2012 to cybercrime prosecution in Nigeria.

7.0 REFERENCES/FURTHER READING

Advance Fee Fraud and Other Fraud Related Offences Act, 2006

Cybercrime (Prohibition, Prevention Etc.) Act, 2015

Electronic Communications and Transactions Act 25 of 2002

Electronic Transactions Act, 2008 (Act No.772)

Evidence Act, 2011

Money Laundering (Amendment) Act, 2012

The Computer Misuse and Cybercrime Act, 2018 (Act No.5)

UNIT 2 REGIONAL AND INTERNATIONAL CYBERCRIME LEGISLATIONS/REGULATIONS

1.0 INTRODUCTION

There are several efforts at the regional and international levels to provide legal framework for combating and regulating cybercrime. The Council of Europe Convention of Cybercrime, 2001 was the earliest international efforts at providing a comprehensive legal framework for the control of cybercrime. The African Union Convention on Cyber Security and Personal Data Protection, 2014 also seeks to strengthen the fight against cybercrime at the regional level. The United Nations is also concerned about the spate of cybercrime and has demonstrated this concern by passing several resolutions aimed at promoting international cooperation against cybercrime. The United Nations has also organized international academic conferences aimed at seeking ways to effectively tackle cybercrime and promote cybercrime education.

2.0 **OBJECTIVE**

This unit focuses on regional and international legislations and regulations on cybercrime. It covers the Council of Europe Convention on Cybercrime, 2001, African Union Convention on Cyber Security and Personal Data Protection, 2014 and the various efforts of the United Nations towards Combating Cybercrime.

3.0 **MAIN CONTENT**

3.1 Council of Europe Convention on Cybercrime, 2001

The Council of Europe Convention of Cybercrime, 2001 is generally believed to be the first significant international legislation of cybercrime. It is also referred to as the "Budapest Convention on Cybercrime" and was adopted by the Committee of Ministers of the Council of Europe during its 108th Session which held on 23rd November, 2001. The Convention however became effective 1st July 2004 and has been ratified by 64 states as at September, 2019.

The Council of Europe Convention on Cybercrime is an international treaty that is aimed at combating cybercrime by adopting relevant registrations and facilitating international cooperation. The Convention covers the followings articles:

1. Definitions
2. Illegal access
3. Illegal interception
4. Data interference
5. System interference

6. Misuse of devices
7. Computer-related forgery
8. Misuse of devices
9. Offences related to child pornography
10. Offences related to infringement of copyrights and related rights
11. Attempt and aiding or abetting
12. Corporate liability
13. Sanctions and measures
14. Scope of procedural provisions
15. Conditions and safeguards
16. Expedited preservation of stored computer data
17. Expedited preservation and partial disclosure of trafficked data
18. Production order
19. Search and seizure of stored computer data
20. Real-time collection of traffic data
21. Interception of content data
22. Jurisdiction
23. General principles relating to international co-operation
24. Extradition
25. General principle relating to mutual assistance

26. Spontaneous information
27. Procedures pertaining to mutual assistance requests in the absence of applicable international agreement
28. Confidentiality and limitation on use
29. Expedited preservation of stored computer data
30. Expedited disclosure of preserved traffic data
31. Mutual assistance regarding accessing of stored computer data
32. Trans-border access to stored computer data with consent or where publicly available
33. Mutual assistance regarding the real-time collection of traffic data
34. Mutual assistance regarding the interception of content data
35. 24/7 Network
36. Signature and entry into force
37. Accession to the Convention
38. Territorial application
39. Effects of the Convention
40. Declarations
41. Federal clause
42. Reservations
43. Status and withdrawal of reservations

44. Amendments

45. Settlement of disputes

46. Consolations of the Parties

47. Denunciation

48. Notification

The Council of Europe Convention on Cybercrime which was drafted by the Council of Europe in Strasbourg, France, with the observer states of Council of Europe: Canada, Japan, Philippines, South Africa and the United States participating actively laid the foundation for the cybercrime legislations of many countries across the world. Though adopted nearly two decades ago, it has remained relevant to several issues surrounding international cooperation in the fight against cybercrime. As can be seen from its articles listed above, some of the offences covered in the Convention are provided for in the Nigerian, Ghanaian, Kenyan and South African cybercrime legislations discussed in unit 1 of this module.

3.2 **African Union Convention on Cyber Security and Personal Data Protection, 2014**

The Convention on Cyber Security and Personal Data Protection, 2014 was adopted by the twenty-third ordinary session of the Assembly of the African Union which held in Malabo, Equatorial Guinea on June 27, 2014. The Convention stipulates among other things that member states of the African Union are aware that it is meant to regulate a particularly evolving technological domain, and with a view to meeting the high expectations of many actions with often divergent interest, the convention sets forth the security rules essential for establishing a credible digital space for electronic transactions, personal data protection and combating cybercrime.

The Convention covers the following thirty-eight (38) articles:

1. Definitions

2. Scope of application of electronic commerce
3. Contractual liability of the provider of goods and services by electronic means
4. Advertising by electronic means
5. Electronic contracts
6. Writing in electronic form
7. Ensuring the security of electronic transactions
8. Objective of the Convention with respect to personal data
9. Scope of application of the Convention
10. Preliminary personal data processing formalities
11. Status, composition and organization of National Personal Data Authorities
12. Duties and powers of National Protection Authorities
13. Basic principles governing the processing of personal data
14. Specific principle for the processing of personal data
15. Interconnection of personal data files
16. Right to information
17. Right to access
18. Right to object
19. Right of rectification and erasure
20. Confidentiality obligations
21. Security obligations

22. Storage oblations
23. Sustainability obligations
24. National cyber security framework
25. Legal measures
26. National cyber security system
27. National cyber security monitoring structure
28. International cooperation
29. Offences specific to Information and Communication Technologies
30. Adapting certain offenses to Information and Communication Technologies
31. Adapting certain sanctions to Information and Communication Technologies
32. Measure to be taken at the level of the African Union
33. Safeguard provisions
34. Settlement of disputes
35. Signature, Ratification or Accession
36. Entry into Force
37. Amendment
38. Depository

The Convention which is relatively recent seeks to foster regional cooperation in the fight against cybercrime. However, not all African states have signed the convention. Only 11 countries have signed it as at 5th February, 2019. This slow response to this regional initiative towards cyber security will affect the efforts of respective African states in combating cybercrime.

3.3 United Nations Efforts towards Combating Cybercrime

The United Nations (UN) with headquarters in New York, United States is committed to combating cybercrime. The UN has over the years established expert groups and sponsored conferences related to Information and Communication Technology (ICT) and cyber threats. In, 2012, the then UN Secretary-General, Ban Ki-moon appointed the group of 15 experts from the five permanent members of the UN Security Council as well as Argentina, Australia (the chair), Belarus, Canada, Egypt, Estonia, Germany, India, Indonesia, and Japan to execute a mandate from the UN General Assembly to study possible cooperative measures that will assist in addressing existing and potential threats related to the use of information and communication technologies (ICTs) (see, Wolter, 2020).

Furthermore, in 2013, the United Nations through its Resolution 22/7 provided a framework for strengthening international cooperation to combat cybercrime. In the same vein, its Resolution 22/8 provided a framework for technical assistance and capacity building to strengthen national measures and international cooperation against cybercrime.

Another example of the demonstration of the United Nations commitment to ensuring global cybersecurity is that in 2018, the United Nations Office of Drug and Crime (UNODC) organized an International Academic Conference on Linking Organized Crime and Cyber Crime, Chuncheon, Republic of Korea. Academics and practitioners were invited across the globe to the two day conference which was organized in partnership with Hallim University, Chuncheon, Republic of Korea. Another initiative is the launching of the Global Cybersecurity Index (GCI) to measure the status of cybersecurity worldwide by UN International Telecommunications Union (ITU).

4.0 CONCLUSION

Given its transnational nature, cybercrime can only be effectively combated through international cooperation and partnerships. Technical assistance and capacity-building are critical in the fight against cybercrime. There are legislations/regulations at the regional and international levels aimed at tackling cybercrime. The rectification and enforcement of such legislations is critical to fight against cybercrime.

5.0 SUMMARY

This unit discussed the regional and international legislations as well as regulations on cybercrime. It covers the Council of Europe Convention on Cybercrime, 2001, African Union Convention on Cyber Security and Personal Data Protection, 2014 and the various efforts of the United Nations towards combating cybercrime.

6.0 TUTOR-MARKED ASSIGNMENT

Discuss the various efforts of the United Nations towards combating cybercrime.

7.0 REFERENCES/FURTHER READING

United Nations, Commission on Crime Prevention and Criminal Justice. (2013). *Resolution 22/7: Strengthening international cooperation to combat cybercrime*.

United Nations, Commission on Crime Prevention and Criminal Justice. (2013). *Resolution 22/8: Promoting technical assistance and capacity-building to strengthen national measures and international cooperation against cybercrime.*

Wolter, D. (2020). The UN Takes s Big Step Forward on Cybersecurity. Available at: https://www.armscontrol.org/act/2013-09/un-takes-big-step-forward-cybersecurity

UNIT 3 CHALLENGES OF CYBERCRIME LEGISLATIONS IN AFRICA AND STRATEGIES FOR IMPROVEMENT

1.0 INTRODUCTION

The global rise in the rates of cybercrime underscores the need for more regulation of the cyberspace. The cyberspace is regulated through appropriate legislations and collaboration among nation-states at the regional and international levels. The quest for the establishment and enforcement of effective cybercrime legislations is hampered by several challenges. For example, in some African states there are still no comprehensive legislations on cybercrime.

2.0 **OBJECTIVE**

This unit focuses on the several challenges that militate against the effective establishment and enforcement of cybercrime legislations in Africa. It also discusses some suggested strategies for the improvement of cybercrime legislations in Africa.

3.0 **MAIN CONTENT**

3.1 Challenges of Cybercrime Legislations in Africa

There are several challenges confronting Africa in its quest to effectively establish and enforce of cybercrime legislations. Ndubueze (2019) discussed some of the challenges as follows:

i.) **The Slow Pace of Processing Legislations**: The process of enacting new legislations in some African countries can be very protracted especially in countries with bi-cameral legislature such as Nigeria. Bills are usually presented and passed in both the upper and lower legislative houses; public hearings are conducted on the bills. Where there are different versions of a bill, they are harmonized, passed by the legislative houses and sent to the President for assent. These processes, though statutory and required to ensure that all relevant stakeholders make necessary inputs to the bill, can be time-consuming. This perhaps explains the delay in passing the first comprehensive cybercrime legislation in Nigeria; Cybercrime (Prohibition, Prevention, etc.) Act, 2015.

ii.) **Gaps in Law Enforcement Knowledge/Skills:** Arguably, law enforcement have not been able to keep pace with the growing complexity of cybercrime. Cybercriminals are inventing new ways of bypassing security barriers in networks and systems, but such ingenuity is not replicated by law enforcement. Law enforcement efforts to combat emerging cybercrimes have, for the most part, being reactive. Marcum (2014) underscores this challenge when she asserts that the most challenging aspect of fighting cybercriminals is that they are often one step ahead of law enforcement in the area of knowledge and skills. A working knowledge of the issues around information and communication technology is required for an effective and efficient establishment and enforcement of cyber crime legislations in Africa. For example, criminal justice professionals require an above average Information and Communication Technology-related security knowledge to satisfactorily enforce cybercrime laws.

iii.) **Low Tempo of Enforcement Activities**: Enforcement of cybercrime legislations in many African countries seems relatively low. This may be as a result of several factors. First, the reporting rate of cybercrime when compared to offline crimes is low. Again, this may be because of the low level of awareness of cybercrime in the continent. Many Internet users may fall victim of cybercrime without knowing immediately. For example, a person may not know that his/her identity has been stolen online until the perpetrator uses it to commit a crime. Second, due to its technical nature, not so many law enforcement personnel understand some technical provisions in the extant legislations. Third, the process of search and seizure of digital evidence require forensic expertise, a skill that is not so common among law enforcement personnel.

iv.)**Security versus Privacy Debate**: The dichotomy between security and privacy especially with respect to the use of electronic surveillance remains of the most discussed challenges of policing cybercrime (Nhan and Bachman, 2015). The foregoing holds true for Africa as well. For example in 2015, a draft bill titled "Frivolous Petition Bill" which proposed two years imprisonment, or a fine of $10,000 (N3.6m) or both for anyone who post "abusive statement" via text message, Twitter, WhatsApp or any other form of social media which passed the second reading in the 8th Nigerian Senate was withdrawn following public out-cry against it (Punch Newspaper, 2018).

v.) **Jurisdictional Issue:** It is well acknowledged that jurisdiction is difficult to establish in the cyberspace and this is one of the major challenges of enforcing cybercrime legislation. This is particularly so because African countries, like their counterparts in other continents would normally encounter some difficulty in determining the jurisdiction of cybercrime cases that cut across many countries of the world.

vi.) **Extradition Issues:** The process of extradition may be tortuous and complicated if the offense for which extradition is sought does not meet the requirement of dual criminality (this means that the offense must be a crime in both concerned countries). This explains why there have been some efforts to address this challenge under the auspices of the African Union. For example, Article 28:2 of the African Union Convention on Cyber Security and Data Protection (2014) provides that:

> State parties that do not have agreement on mutual assistance in cybercrime shall undertake to encourage the signing of agreement on mutual legal assistance in conformity with the principle of double criminality, liability, while promoting the exchange of information as well as the efficient sharing of data between the organization of State Parties on a bilateral and multilateral basis.

vii.) **Dearth of Cybercrime Research Centres:** There is a dearth of cybercrime research centres in Africa when compared to the western world (see, Ndubueze, 2016). The academia and practitioners may be required to make their inputs during public hearings on cybercrime bills. Law makers may require evidence-based, domesticated and well documented research on the cybercrime problem to formulate appropriate legislations that will fit into the peculiarity of each nation-state. But where such research is not sufficiently and readily available, they may be somewhat handicapped. Thus, there is need for African governments to establish and fund cybercrime and cyber security research centres.

viii.) **Low Regional Response:** Overall, there seems to be low response across the spectrum to the problem of cybercrime in Africa. When compared to the developed regions of the world such as America, Australia, Europe and so on, there are not so many conversations going on around the problem of cybercrime. There are not so many regional conferences, seminars, debates, on cybercrimes and criminality. There is no doubt that such activities would ultimately create more awareness on the scope of the problem and underscore the need for more regional cooperation in the efforts to combat it. For example, the African Union Convention on Cyber Security and Personal Data Protection was adopted by the Twenty-third Ordinary Session of the Assembly held in Malabo Equatorial Guinea on 27th June 2014. However, only 11 countries have signed it as at 5th February, 2019 (African Union, 2019). This low response will undoubtedly affect the level of cooperation among member states in the establishment and enforcement of cybercrime legislation in Africa.

ix.) **Weak Voices in Global Internet Governance:** The African Union Commission (2016) has decried the weak voices of Africa in global Internet governance. African needs strong voices in global internet governance as this is critical to the effective enforcement of cybercrime legislations in Africa.

3.2 Strategies for the Improvement of Cybercrime Legislations in Africa

Ndubueze (2019) suggested the following strategies for the improvement of cybercrime legislations in Africa:

i.) **Periodic Review of Cybercrime Legislations:** Cybercrime, being a high-tech crime is evolving in nature. Therefore, it will be practically impossible to establish a set of legislation that will effectively capture its future patterns. Thus, law and policy makers in Africa must continue to update their countries legislations on cybercrime to be able to satisfactory tackle the growing sophistication cyber criminality.

ii.) **Need for Cybercrime Research Centres:** For law and policy makers to be able to update cybercrime legislations they need systematic and reliable data on emerging patterns of cybercrime. Therefore, there is need for African government to establish dedicated cybercrime research centres and specially commission/fund cybercrime research projects. This way, they will be able to generate credible statistics/data that will guide the review of cybercrime legislation in their respective countries.

iii.) **Need for Specialized Training for Law Enforcement:** African governments should invest more in the training and re-training of law enforcement personnel on cybercrime investigation and digital forensics. To be able to effectively and efficiently police cybercrime, law enforcement personnel need an above average knowledge of cybercrime issues. Such knowledge when rightfully applied will go a long way in strengthening the enforcement of the extant legislations on cybercrime in African countries.

iv.) **Need for Enforcement of Existing Legislations:** Law enforcement should be more aggressive in enforcing the existing legislations on cybercrime. This will send warning signals not only to cybercriminals but it will also deter potential cybercriminals who may be scared of experiencing the full wrath of the law. For legislations to fully achieve their objectives they have to be enforced.

v.) **Public Enlightenment Campaigns:** There is need for regulatory agencies to increase the tempo of their public enlightenment campaigns on cybercrime and its legislations. These campaigns should also be propagated in the major local languages for wider coverage. This perhaps may assist in improving the reporting practices of cybercrime. It will address the seeming apathy on the part of citizens to report crime to relevant law enforcement agencies.

vi.) **Need for more Regional Cooperation:** Cybercrime is a transnational crime. It therefore, requires international partnerships to tackle it. There is need for African countries to collaborate with one another in the fight against cybercrime. Such collaboration will reduce the technicalities associated with extradition and will make it more or less, a seamless process. There is need for African countries yet to sign the African Union Convention on Cyber Security and Data Protection to consider doing so.

4.0 CONCLUSION

African states need appropriate legislations to be able to effectively tackle the problem of cybercrime. Given that cybercrime is always evolving and cybercriminals are constantly reinventing their modus operandi, cybercrime laws need to be periodically reviewed. Above all, African states need to partner and provide mutual assistance for the effective implementation of cybercrime legislations.

5.0 SUMMARY

This unit discussed the various challenges that militate against the effective establishment and enforcement of cybercrime legislations in Africa. It also discusses some strategies for the improvement of cybercrime legislations in Africa.

6.0 TUTOR-MARKED ASSIGNMENT

What are the challenges militating against the effective establishment and enforcement of cybercrime legislations in Africa?

7.0 REFERENCES/FURTHER READING

African Union (2019). List of countries which have signed, ratified and acceded to African Convention on Cyber Security and Personal data Protection. Available at: Retrieved from *https://au.int/.../29560-sl-african_union_convention_on_cyber_security_and_personal..*

Marcum, C. D. (2014). *Cyber Crime.* New York: Wolters Kluwer law & Business.

Ndubueze, P.N. (2019). Cybercrime and Legislation in an African Context. In T.J. Holt and A.M. Bossler (eds.) *The Palgrave Handbook on International Cybercrime*. Switzerland AG: Palgrave Macmillan, Cham DOIhttps://doi.org/10.1007/978-3-319-90307-1_74-1

Ndubueze, P.N. (2016). Cyber criminology and the quest for social order in Nigerian Cyberspace. *The Nigerian Journal of Sociology and Anthropology.* 14 (1): 32-48.

Nhan, J. & Bachmann, M. (2015). Developments in Cyber Criminology. In M. Maguire and D. Okada (eds.). *Critical Issues in Crime and Justice: Thought, Policy and Practice*, (2nd ed.), pp. 209 -228. Los Angeles: Sage Publications.

Punch Newspaper (2018, February 3). More attacks on FG over social media monitoring. Retrieved June 2, 2019 from *https://punchng.com/more-attacks-on-fg-over-social-media-monitoring/*

Wall, D.S. (2007/10). Policing cybercrime: Situating the public police in networks of security within cyberspace. *Police Practice and Research: An International Journal*, 8 (2), 182-205.

UNIT 4 CYBERSECURITY: ISSUES AND PERSPECTIVES

1.0 INTRODUCTION

Cyber threats have raised the national security threat levels in many countries of the world and constitute major security threats in those countries. Cybersecurity is primarily concerned with the protection of various kinds of digital assets from attacks that are capable of compromising their confidentiality, integrity and availability. Information systems and critical national infrastructure are usually targeted by cybercriminals. A sound cybersecurity policy is required to ensure that they are not disrupted from their smooth operations. This is of utmost importance given that for example, critical infrastructures are critical to the economy and security of every nation in the 21st century.

2.0 **OBJECTIVE**

This unit focuses on the meaning and scope of cybersecurity, types of cyber incidents and attackers, vulnerability in information systems, vulnerability in critical infrastructure, countermeasures for vulnerabilities and cybersecurity risk management.

3.0 **MAIN CONTENT**

3.1 Meaning and Scope of Cybersecurity

Cybersecurity has to do with the protection of computers, networks, programmes and data from unintended or unauthorized access, change or destruction (see, Pale, 2014). It focuses on the understanding of issues around various cyber attacks and devising defense strategies or countermeasures that safeguard the confidentiality, integrity and availability of digital and information technologies (Jang-Jaccard & Nepal, 2014). The scope of cybersecurity covers the protection of various kinds of digital assets. For example, Klonoff (2015) argued that diabetes medical devices such as blood glucose monitors, continuous glucose monitors, insulin pumps, other wearable sensors, cloud computer systems, and readers like, desktop computers, laptops, pads, smartphones and watches need to be protected from threats that can degrade their function and put the health of the user of the device at risk. He noted that such threats can include unauthorized disclosure, modification or loss of function.

According to Kostopoulos (2018, p.xvi) cybersecurity must safeguard the following four principles that are essential for any trusted cyberspace engagement:

i. **Confidentiality**: Data transmitted or stored are private; to be viewed only by authorized persons.

ii. **Integrity**: Data transmitted or stored are authentic - free of errors made in storage or in transit.

iii. **Availability**: Data transmitted or stored are accessible to all authorized.

iv. **Non-Repudiation**: Data transmitted or stored are of indisputable authenticity, especially when supported by acceptable digital certificates, digital signatures, or other explicit identifiers.

3.2 Types of Cyber Incidents

There are various types of cyber incidents. These incidents constitute a major threat to individual internet users, businesses, private and public organizations. Romanosky (2016) categorized cyber incidents as follows:

i. **Data Breach:** This refers to the unintentional disclosure of personally identifiable information that is as a result of loss or theft of digital or printed information such as a laptop or wallet containing a person's driver's license. Data breach also involves the improper disposal or disclosure such as to a dumpsite or website of personal information. Such information can be used to commit identity, financial or medical fraud.

ii. **Security Incident:** This is an incident that involves the compromise or disruption of corporate information technology systems such as computers or networks or its intellectual property. Examples include a denial of service (DOS) attack, theft of intellectual property, malicious infiltration etc.

iii. **Privacy Violation:** This is the unauthorized collection, use or sharing of the personal information of others. This may involve unauthorized collection from cell phones, Global Positioning System (GPS) devices, cookies, web tracking or physical surveillance. It also includes allegations of violations of information statuses as well as unsolicited communications from spam emails, other mass marketing communication (robocalling, texts, and emails) or debt collection.

iv. **Phishing/Skimming:** This category deals with cyber incidents that are perpetrated by individuals against other individuals or firms. These include phishing attack (whereby criminals seek to harvest account information from users), identity theft (whereby criminals use another person's information for financial gain) or skimming attack (where criminals install a hardware devices over automated teller machines that enables them to copy bank account and bank pin numbers of others without their knowledge).

Although the above categorization of cyber incidents is not exhaustive, it provides useful insights on the patterns of cyber incidents in the digital age. The type of cyber incident an attacker can launch will largely depend on his/her skill set. Ashtiani and Azgomi (2014) classified cyber attackers as follows:

i. **Low-skilled attackers:** This kind of attackers also referred to as script kiddies do not have programming knowledge and knowledge of the steps required to gain access to the targeted systems. They usually rely on the blind use of public exploits and tools which professional hackers provide.

ii. **Medium skilled attackers:** This kind of attackers partially knows professional hacking tools and the steps required for accessing targeted systems. However, they lack the programming skills required to create new exploits based on vulnerabilities that they find in their targets.

iii. **High-skilled attackers:** They are versed in vulnerability detection techniques and creating of new exploits. They are very familiar with professional hacking tools and the steps required for accessing targeted systems. They normally use their private archive of exploit.

The harm caused to the targeted system by the attack is usually a function of how skilled the attacker is. Therefore, high-skilled attackers are the most dangerous of the three as they possess the required skill-set to perpetrate highly malicious attacks.

3.3 Vulnerabilities in Information Systems

According to Kostopoulos (2018, p.1) “vulnerability in any system is the result of an intentional or unintentional omission or of an inadvertent design mistake that directly or indirectly leads to a compromise in the system’s availability, integrity, or confidentiality” .The United States National Institute of Standard and Technology (NIST) (as cited in Kostopoulos, 2018, pp. 5-7) protocol for standardizing the identification and cataloging of security vulnerability and configuration is made up of the following six components:

i. **Common Vulnerabilities and Exposures (CVE):** This is a depository of registered known information security vulnerabilities containing unique identification number for each occurrence. An occurrence is first defined as candidate vulnerability, entered in the MTRE Common Vulnerabilities and Exposure List and registered in the National Vulnerability Database.

ii. **Common Configuration Enumerator (CCE):** This depository contains security vulnerabilities and interfacing inconsistencies that are in system configurations. This information can facilitate regulatory compliance, proper interoperability and audit checks. It identifies existing problems and recommends solutions.

iii. **Common Platform Enumerator (CPE):** This component deals with the proper naming of the software and provision of hierarchical structure. It explicitly defines the software and facilitates software inventory management.

iv. **Common Vulnerability Scoring System (CVSS):** This is an algorithm that deals with parameters of the development and use of the subject software and provides a score for the level of calculated security. The algorithm is open access based and it highly patronized by system designers and security analysts who are involved in risk analysis and system planning.

v. **Extensible Configuration Checklist Description Format (XCCDF):** This is an XML template that assists in the preparation of standardized security guidance documents. It presents general software vulnerabilities or those of specific configurations or uses of addressed software, in normalized configuration content via automated security tools.

vi. **Open vulnerability and Assessment Language (OVAL):** This runs across the entire spectrum of the information security tools and services and standardizes the three major steps of the assessment process: the representation of system information, the expression of the specific machine states, and the assessment reporting. These are presented in a language that the information system security community understands.

Information system vulnerabilities are basically weaknesses in the hardware or software design from the client or server side that an attacker can exploit to gain an unauthorized access to the system. The role of human factor is also widely recognized. Cybercriminals can create various kinds of malicious software that are capable of disrupting the smooth operations of hardware and software components of information systems.

3.4 **Vulnerabilities in Critical Infrastructure**

According to Radvanovsky and McDougal (2013) critical Infrastructure are assets of physical and computer-based systems that are fundamental to the minimum operations of the economy and government. They include among others telecommunications, energy, banking and finance, transportation, water systems and emergence services.

The US PATRIOT ACT (as cited in Breneau et. al. (2020, p. 22) listed the following categories of critical infrastructure:

i. Transportation Infrastructure

- Trucks, highways, and bridges
- Trains and rail tracks
- Airplanes and airports
- Ships and ports

ii. EI – Energy Infrastructure

- Pipelines (including for green gas) and refineries
- Electrical grids, towers, and power stations
- Large-scale renewable energy generation and supply systems, e.g., offshore parks
- Nuclear reactors
- Dams

iii. WW – Waste Water System

- Water pipes, tanks, and reservoirs
- Sewage conduits and refineries

iv. ES – Emergency Services

- Hospitals
- Fire stations
- Police stations

v. IT – Information Technologies

- Sensors, connectors, and other data acquisition devices (DAQs)
- Interpretation of signals
- Databases and cloud computing
- Security and safety of data
- Artificial intelligence
- Machine and deep learning

As can be seen from the above list, critical infrastructure cuts across various sectors of a nation's economy and is very essential to its smooth operations. Because critical infrastructure increasingly relying on the internet for their operations, they are vulnerable to cyber attacks. Vulnerabilities in the hardware and software can constitute threats to critical infrastructure as they can obstruct the services provided by critical infrastructures.

Alcaraz and Zeadllly (2015) classified the faults associated with critical infrastructure into two: internal and external faults. An internal fault involves anomalous changes that originated from the system. An external fault has to do with interactions that originate from outside the system like natural phenomena, malicious actions or accidents. They explained that whatever be the cause, any fault within the critical infrastructural system can create an internal effect that can result in the collapse of essential services and activities for the control. For example, an attack on a sensor node can cause hardware and software errors that may eventually affect the operations of essential resources for the control like remote terminal units.

3.5 **Countermeasures for Vulnerabilities**

Cyber infrastructural systems are always threatened with various kinds of vulnerabilities. Kostopoulos (2018, pp.19-20) suggested the following countermeasures that can serve as defenses against external threats.

- Screening the URL of online system access attempts against a list of pre-approved ones. Or, extend them or retreat them as the need calls for.
- Maintaining the instruction risk by reducing access privileges wherever they are not absolutely necessary.
- Minimizing the outline availability of sensitive data, thus reducing the exposure to possible instruction.

- Having passwords that are immune to “dictionary” attack by including letters of foreign languages.
- Using multi-factor authentication, such as receiving additional access parameters via mobile telephony.
- Designing for high volume traffic, so that “flooding” attempts to the interface ports will not succeed.
- Developing the ability to recognize Distributed Denial of Service (DDoS), attacks, through dynamic metrics, that continuously observe the resources utilization.
- Use of firewall, anti-virus software, and upgrading of the software, and updating of the software (updates and patches) of Web-connected devices.
- Log and report instruction attempts and suspicious Web requests.
- Disconnect or deactivate Web-accessible assets not used at the moment.
- Conduct a frequent (daily or weekly) audit. Be aware of the types of applications that reside in your system.

3.6 **Cybersecurity Risk Management**

Musman and Turner (2018) used Cyber Security Game (CSG) to demonstrate the following ways cyber security risk can be addressed.

i. **Quantifying cyber risk**: This focuses on the damage (loss) caused by an unfavourable events and an estimate of how often it may occur within a period of time (likelihood). Mission Oriented Risk and Design Analysis (MORDA) is a security risk analysis methodology that combines threats, attack trees, and mission impact concepts to arrive at unbiased risk metric. Many people also use simplified models that use the definition “Risk = Threat (T) x Vulnerability (V) x Consequence (C)”. Experts usually assess the threat and vulnerability terms as probabilities. Consequence is assessed using various units such as economic replacement cost, or fatalities. The idea being to assess adversary intent as “threat” and consequently use such assessment to strengthen defense.

ii. **Comprehensive assessment of cyber incidents:** There is a wide range of potential attacker exploits and method; some may be opportunistic while others may be targeted. The cyber security game approach focuses on assessing whether good security principles have been applied and whether there were defenses to frustrate the efforts of the attacker. Due to the wide range of attack methods it is difficult for cyber modeling to comprehensively capture all the likely cyber incident instances. In order to address the problem some have used cyber incidents effects instead of the attack instances that can produce those effects. Confidentiality, Integrity and Availability (CIA) cyber incident effects is commonly considered. However, in cyber security game (CSG) cyber effects is defined in the DIMFUI (i.e. deregulation, interruption, modification, fabrication, unauthorized use, and interception) classification as a more comprehensive set of incident effects, where every entry in the common vulnerability and exposure serve as one or more of these effects against one or more of the cyber resources of the system.

iii. **Modeling attack paths:** Cyber security defender must have the capacity to identify and defend against multi-step attacks. This is very necessary because they deal with intelligent adversary. Cyber systems are usually interconnected and therefore attackers can exploit those cyber components that seem non-critical in order to bypass security controls and other defenses, example Stuxnet and targeted data breach. It is common to identify attack path and model attacker behaviour using attack trees. Although it is usually developed manually, it can be computed via automation using system typology model. This approach is generalized by cyber security game using a probabilistic attacker model that factors all the potential impact targets an attacker can possibly hit.

iv. **Modeling attacker behaviour:** Cyber security defense is also complicated by the fact that every action taken by a defender to improve system security is followed by a corresponding adjustment by an attacker to find another potential loophole. Attack trees provide insights about how an attacker will exploit various options to bypass defenses, but do not show how the tree is affected by the defender's action. To deal with this problem, cyber-attacks and the corresponding defense actions that can prevent them can be construed as game playing between two players. Cyber security game generalizes attacker behaviour by applying a game-theoretic approach that is based on the constraints imposed on the attacker by the system structure and defenses.

v. **Identifying the best investments:** There are several cyber risk methods that deals with allocating resources by the risk ranking of critical cyber resources or developing a top10 list of system's risk. But such ranking are not enough for resource allocation. The best defenses and where to employ them vary and largely depend on the defender's level of resource. Cyber security game has a portfolio engine that can best identify investment considering resource investment.

4.0 CONCLUSION

Information systems and critical national infrastructure are threatened by the activities of cyber criminals. The need to secure them becomes very imperative. While the vulnerabilities in these systems cannot be completely eliminated certain countermeasures can make them less prone to attacks that are capable of disrupting their smooth operation. It is important that concerted efforts are made by stakeholders to safeguard the confidentiality, integrity and availability of digital information and technologies as that is the whole essence of cybersecurity.

5.0 SUMMARY

This unit examined the meaning and scope of cybersecurity, types of cyber incidents and attackers, vulnerability in information systems, vulnerability in critical infrastructure, countermeasures for vulnerabilities and cybersecurity risk management.

6.0 TUTOR-MARKED ASSIGNMENT

a. What do you understand by the term "cybersecurity"?

b. Explain the various types of cyber incidents.

7.0 REFERENCES/FURTHER READING

Alcaraz, & S. Zeadally (2015). Critical Infrastructure Protection: Requirements and Challenges for the 21st Century. *International Journal of Critical Infrastructure Protection (IJCIP),* 8, 1-34.

Ashtiani, M. & Azgomi, M.A. (2014). A distributed simulation framework for modeling cyber attack and the evaluation of security measures. Simulation: *Transactions of the Society for Modeling and Simulation International*, (90) 9, 1071-1102.

Bruneau, M. et. al. (2020). Introduction: Challenges and generic research questions for future research on resilience. In Z. Wu, X. Lu, M. Noori (eds.). *Resilience of Critical Infrastructure Systems: Emerging Developments and Future Challenges* (pp. 1-42) Boca Raton: Taylor and Francis – CRC Press.

Jang-Jaccard, J. & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Science,* 80, 973-993.

Klonoff, D.C. (2015). Cybersecurity for connected diabetes devices. *Journal of Diabetes Science and Technology,* 9 (5) 1143-1147.

Kostopoulos, G. (2018). *Cyberspace and Cyber Security* (2nd ed.). Boca Raton: CRC Press, Taylor & Francis Group – CRC Press.

Pale, P. (2014). Education as a long term strategy for cybersecurity. In A.Vaseashta, P.

Susmann & E. Braman (ed.). *Cyber Security and Resiliency Framework* (pp. 127-134). Amsterdam: IOS Press.

Radvanovsky, R. & McDougal, A. (2013). *Critical Infrastructure, Homeland Security and Emergency Preparedness* (3rd ed.). Boca Raton: Taylor and Francis- CRC Press.

Romanosky, S. (2016). Examining the cost and causes of cyber incidents. *Journal of Cybersecurity*, 2 (2), 121-135.

Module 6: Cyber Crime Policing and Prosecution in Nigeria: Issues, Challenges and Prospects

Unit 1: The Challenges of Studying and Investigating Cybercrime
Unit 2: Digital Forensic and Investigation
Unit 3: Third Party Policing Strategies and Cybercrime Investigation
Unit 4: Challenges of the Criminal Justice System in Policing and Prosecuting Cybercrime.

UNIT 1 THE CHALLENGES OF STUDYING AND INVESTIGATING CYBERCRIME

1.0 Introduction

2.0 Objectives

3.0 Main Content

3.1 Defining Cybercrimes

3.2 Rapidly Changing Laws

3.3 Changes in Law Enforcement Practices

3.4 Understanding the Context

3.5 Understanding the “How”s and “Why”s of Cybercrime

4.0 Conclusion

5.0 Summary

6.0 Tutor-Marked Assignment

7.0 References/Further Reading

1.0 INTRODUCTION

Cybercrimes are basically technology-based and technology-enabled crimes. They are often complex in nature and always evolving. Therefore studying and investigating cybercrime is fraught with several challenges.

2.0 **OBJECTIVE**

This unit examines the challenges of studying and investigating cybercrime as discussed by Graham and Smith (2020) namely: defining cybercrime, rapidly changing laws, changing law enforcement practices, understanding the context and understanding the “how”s and “why”s of cybercrime .

3.0 **MAIN CONTENT**

3.1 Defining Cybercrime

The public is confronted with the challenge of developing adequate vocabulary and sets of definitions for the explanation and understanding of cybercrime related phenomena. A certain definition of cybercrime tend to place emphasis on the environment an activity took place rather than the activity itself. From that perspective, any criminal or deviant activity that is mediated with computer technology is cybercrime or cyberdeviance. For example, stalking a person is a traditional crime. However, when stalking is done through social media-in cyberspace- stalking now become cyberstalking and therefore a cybercrime. There are some malicious behaviours online that may not fit into the existing definitions of cybercrime and what is considered cyberdeviance will normally depend on the context.

3.2 Rapidly Changing Laws

Digital technological developments are moving at a pace that the legal system is struggling to keep up with. Enacting of new laws is a fundamental requirement for keeping pace with changes in technology and social patterns. But the process of enacting new cybercrime laws is not without challenges as the new laws may not actually address the problems they intended to due to lack of understanding about the problems. For example, while some people are advocating for the criminalization of use of fake identity online, others are opposed to the idea as they argue that it may be used with good motive. For example, a whistleblower may want to conceal him/her identity.

3.3 Changes in Law Enforcement Practices

There are studies that suggest that most cybercriminals are from different backgrounds and social context than traditional criminals. The infrastructure and cultural patterns of law enforcement are oriented towards street crimes and potential street criminals. However, to be able to effectively combat the upsurge in cybercrime, law enforcement need to reorient themselves to cybercriminals as their backgrounds are very likely different from those of traditional criminals. Another change in law enforcement is their learning and institutionalizing of cyberspace investigation techniques. This they have demonstrated in three ways: i. Law enforcement authorities have learned how and when to request evidence from intermediaries through court order, subpoena and warrant. ii. They have developed strategies for following a person's digital trail online. iii. Law enforcement personnel trained in digital forensics can extract digital evidence at the binary level on a hard drive. Notwithstanding the development of these new techniques, investigating and solving cybercrime remains more tasking than street crimes, especially because of its transnational nature. For example, law enforcement agencies may encounter difficulty when a suspect is from another country, as security agencies in other countries may not cooperate with investigators.

3.4 Understanding the Context

It is important that cybercrime scholars consider the cultural context in which cybercrime takes place. It is argued that because cybercrime is largely symbolic in nature, there is need to consider how the crime and victimization are socially constructed compared to other types of crimes. For example, cyber bullying or the theft of a person's identity online will be subject to more interpretation than the physical assault of a person. Also, depending upon the context, a negative social media post may be taken lightly as “just words” or taken seriously as capable of causing psychological trauma.

3.5 Understanding the “How”s and “Why”s of Cybercrime

Theoretically informed scholarly researches are needed in order to understand how and why cybercrime occur. The “how”s and “why”s provides understanding to cybercrime problem:

- Effective laws and social policies originate from rigourous, nonpartisan scholarship that accurately defines and describes cybercrime phenomena.
- Knowing root social causes of cybercrime offending and developing accurate profiles of cybercriminals can assist law enforcement in anticipating and investigating cybercrime.
- Scholarship on victimization can assist social workers and other victim assistance professionals in threating those who have been hurt by cybercrime.

4.0 CONCLUSION

Cybercrime researchers and law enforcement need to be familiar with the several challenges that confront them in their efforts to study and investigate cybercrime. Understanding of the challenges is undoubtedly an important step towards making efforts to ameliorate them. Although, Graham and Smith’s perspective on these challenges which are summarized in this unit is not exhaustive, it provides a background for understanding the challenges of cybercrime investigation.

5.0 SUMMARY

This unit discussed the challenges of studying and investigating cybercrime as presented by Graham and Smith (2020) namely: defining cybercrime, rapidly changing laws, changing law enforcement practices, understanding the context and understanding the “how”s and “why”s of cybercrime .

6.0 TUTOR-MARKED ASSIGNMENT

Graham and Smith's (2020) identified some challenges that are associated with studying and investigating cybercrime. Enumerate and explain these challenges.

7.0 REFERENCES/FURTHER READING

Graham, R.S. & Smith, S.K. (2020). *Cybercrime and Digital Evidence*. New York: Routledge: Taylor and Francis Group.

UNIT 2 DIGITAL FORENSICS AND INVESTIGATION

1.0 INTRODUCTION

Digital forensics is a relatively new sub-discipline of forensic science that is increasingly becoming popular. Digital forensics experts are trained to conduct various kind of digital forensic investigation including some aspects of cybercrime investigation. Although, digital evidence can be fragile and large in volume, digital forensic professionals can automate the various phases of investigation for best result.

2.0 **OBJECTIVE**

This unit focuses on the concept of digital forensics, sources of digital evidence, types of digital forensics, principles of digital forensics, processes of digital forensics and challenges of digital forensics.

3.0 **MAIN CONTENT**

3.1 The Concept of Digital Forensics

Digital forensics also referred to as "cyber forensics" and "computer forensics" is a new sub-discipline of forensic science. The first Digital Research Forensic Workshop (as cited in Roussev (2017, p.11) defined digital forensics as:

> The use of scientifically derived and proven methods towards the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.

The above definition explains the nature and goal of digital forensic. Digital forensics is guided by a scientific protocol and it is often conducted to aid investigation or prosecution. Digital evidence can be collected from a wide range of sources such as desktop computers, laptops, tablets, servers, smart phones, Global Positioning Systems (GPS), drones, Close Circuit Television (CCTV) systems, digital video recorders, SIM-cards, digital cameras etc.

3.2 **Sources of Digital Evidence**

Digital evidence can be retrieved from a wide range of sources. Digital evidence are usually collected or retrieved from electronic and digital devices. Some of them include:

- Computers (desktop, laptops, ipads etc.)
- Removable Media (disks, flash drives, memory cards etc)
- Printers/Fax machines
- Photocopying machines
- Scanners
- Digital cameras
- The Internet
- Smartphones etc.

3.3 Types of Digital Forensics

There are several types of digital forensics (see, International College of Security Studies n.d.). Some of them include:

i. **Computer Forensics:** This is a type of digital forensic that deals with the identification, collection, preservation analysis and reporting of evidence found on computers, laptops etc. These items contain vast amount of data that forensic investigators can examine.

ii. **Network Forensics**: This deals with the monitoring, storing and analysis of network traffic and related activities to determine the source of security attacks, intrusions or breaches. Once the source is identified efforts can be made not block the security loophole in order to forestall future attack.

iii. **Database Forensics**: This refers to the identification, collection, preservation analysis and reporting of evidence found on databases and metadata. The goal may be to trace the transactions that occurred in a database system.

iv. **Mobile Device Forensics**: This deals with the recovery of electronic evidence from cell phones, SIM cards, tablets, Global Positioning System (GPS) devices etc. Usage logs and other kinds of data can be retrieved from mobile devices. For example, a GPS-enable device contains file data that can show when and where a photograph was taken.

v. **Digital Video/Audio Forensics**: This refers to the collection, perseveration, and analysis of video and sound recordings. Investigators may want to establish the authenticity or otherwise of a video or an audio recording. The analysis will reveal whether a recording has been tampered with through for example, editing.

vi. **Disk Forensics**: This has to do with the recovery of digital evidence from digital storage media such as hard disk, USB devices, flash drive, CD plates, DVD plates etc. Depending on their storage capacities, disks can contain vast amount of digital evidence that forensic investigators can examine.

3.4 Principles of Digital Forensics

Digital forensics as a sub-field of forensic science is guided by the scientific principles that govern the admissibility of evidence in a court of law. Schowski (2018) discussed the following principles of digital forensics:

- **Evidence Exchange**: Forensic investigation among other things seeks to establish factual conclusions that are informed by credible evidence. The Locard's exchange principle states that contact between entities will result in exchange that will leave a trace. For example, an offender may unknowingly leave finger prints at the crime scene. In the digital world, email correspondence and web browsing history are examples of these exchanges that can serve as digital evidence in digital forensic investigations.
- **Forensic Soundness**: Evidence is fundamental in investigations. Therefore, whether in the physical or digital worlds, evidence should be handled in such a manner that it admissibility in court is not hampered. Forensic soundness means

that digital evidence remains complete and materially unaltered by the use of technology or methodology. This implies that proper forensic techniques and consistent methodologies that are based on established scientific principles were employed in every investigation. However, human error is the major threat to forensic soundness of digital evidence.

- **Authenticity and Integrity**: Authenticity of digital evidence is maintained in order to show that the data is the same as when it was seized. Technically, there are instances when digital evidence cannot be compared to its original state, for example a random access memory (RAM) that is constantly changing. In such a case, a snap shot can be taken to show the state of the technology when it was seized. Legally speaking, authentication entails establishing to the legal system that: (a) content of the record has remained unchanged (b) Information in the record actually originate from its original source (c) Extraneous information about the record is accurate (.i.e. timestamp). In digital forensics, verifying integrity has to do with comparing the finger prints of digital evidence when it is first collected as well as throughout its life cycle.
- **Chain of Custody:** The chain of custody documents the transfer of ownership over digital evidence between entities. It can be used to validate the integrity of evidence that is presented during court trial. The absence of chain of custody can raise arguments that evidence has been compromised, altered, or improperly handled resulting in contamination. Minimum number of custody transfers is preferred as concerned individuals may be required to testify about the how they handled the evidence when it was in their custody.

According to Schowski (2018, pp.11-12) the G8 Subgroup, *the Principles On Transborder Access to Stored Computer Data – Data Principles on Assessing Data Stored in a Foreign State* which were approved by the G8, states several principles which can assist law enforcement agencies in investigating technology enabled crimes in other countries. They are as follows:

- Preservation of stored data in a computer system.

  – Each state shall ensure its ability to secure rapid preservation of data that is stored in a computer in particular data held by third parties such as service providers, and that is subject to short retention practices or is otherwise particularly vulnerable to loss or modification, for the purpose of seeking its access, search, copying, seizure or disclosure, and ensure that preservation is possible even if necessary only to assist another State.

  – A State may request another State to secure rapid preservation of data stored in a computer system located in that other State.

  – Upon receiving a request from another State, the requested State shall take all appropriate means, in accordance with its national law, to preserve such data expeditiously. Such preservation shall be for a reasonable time to permit the making of a formal request for the access, search, copying, seizure or disclosure of such data.

- Expedited mutual legal assistance

  – Upon receiving a formal request for access, search, copying, seizure or disclosure of data, including data that has been preserved, the requested State shall, in accordance with its national law, execute the request as expeditiously as possible, by:

  - Responding pursuant to traditional legal assistance procedure
  - Ratifying or endorsing any judicial or other legal authorization that was granted in the requesting State and, pursuant to traditional legal assistance procedures, disclosing any data seized to the requesting State.
  - Using any other method of assistance permitted by the law of the requested State.

– Each State shall, in appropriate circumstances, accept and respond to legal assistance requests made under these Principles by expedited but reliable means of communications, including voice, fax or e-mail, with written confirmation to follow where required.

- Transborder access to stored data not requiring legal assistance

  – Notwithstanding anything in these Principles, a State need not obtain authorization from another State when it is acting in accordance with its national law for the purpose of:

  - Accessing publicly available (open source) data, regardless of where the data is geographically located.
  - Accessing, searching, copying, or seizing data stored in a computer system located in another State, if acting in accordance with the lawful and voluntary consent of a person who has the lawful authority to disclose to it that data. The searching State should consider notifying the searched State, if such notification is permitted by national law and the data reveals a violation of criminal law or otherwise appears to be of interest to the searched State.

Given that cybercrime is largely transnational, international cooperation among nation-states is required to effectively prosecute cybercriminals. The above G8 principle deals with many critical areas that are involved in transnational cybercrime investigation such as the preservation of stored data in a computer system, expedited mutual legal assistance and transborder access to stored data not requiring legal assistance. The whole essence of these principles and similar ones that are contained in other international treaties is to ensure that cybercriminals are prosecuted as speedily as possible and that they do not find safe havens where they can hide.

3.5 Processes of Digital Evidence

Ashcroft, Daniels and Hart (1994) discussed the followings stages that are followed in the processing of digital evidence:

i. **Assessment:** The first step in the processing of digital evidence entails the thoroughly assessment of digital evidence by digital forensic examiners. The essence of this assessment is to determine the scope of the case and the necessary line of action that needs to be taken.

ii. **Acquisition:** Given the fragile nature of digital evidence and the fact that examination is best conducted on the original copy of the evidence, the original evidence is acquired in a way that preserves and protects its integrity. This is because contaminated evidence will not produce an accurate result and may not be admissible in the court of law.

iii. **Examination:** Digital evidence is examined in order to extract and analyze it. Extraction deals with the recovery of data from the source of the digital evidence such as computers, laptops, tablets, servers, smart phones, drones, Close Circuit Television (CCTV) systems, digital video recorders etc. On the other hand, analysis has to do with the presentation of the recovered data in a logical and useful format that allows for proper interpretation.

iv. **Documentation and Reporting**: This refers to the documentation of actions and observation throughout the forensic processing of evidence. The documentation is vital because it is used for the preparation of a written report of findings. Without proper documentation the report of findings will be fraught with errors.

Although the above five stages can be further broken down into several other stages, they however provide us with useful insights on the various stages that are normally followed when processing digital evidence.

3.6 Challenges in Digital Forensics

According to Frank and Arnes (2018) one of the major challenges confronting digital forensics, is the large amount of unstructured data that are riddled with uncertainties and errors. They noted that each phase of digital forensics process can demand so much time and resources that are way beyond what is available for the investigation. They further pointed out that this has resulted in the inclusion of big data, automation and occupational methods in the forensic process such as:

- The identification phase can be facilitated by detection and identification methods.
- The collection phase be facilitated by automated remote evidence acquisition tools with built-in evidence integrity assurance.
- The examination phase can be facilitated by automated data recovery and data reduction.
- The analysis phase can use computational methods and machine learning to identify patterns and data of interest in evidence.
- The presentation phase makes use of a wide range of visualization tools, and in-built repeat generation.

4.0CONCLUSION

Cybercrime investigation largely requires the collection and analysis of digital evidence. Undoubtedly, the identification, collection, preservation, analysis and reporting of digital evidence is highly time and resources demanding. Investigators that are involved in the aforementioned tasks need to be properly trained and re-trained for them to be able to deliver on their mandate. Digital forensics is the sub-discipline of forensic science that equips investigators with the technical knowledge required to conduct digital investigations. Although this area of specialization is still relatively new in Nigeria, it is gaining popularity.

5.0 SUMMARY

This unit examined the concept of digital forensics, sources of digital evidence, types of digital forensics, principles of digital forensics, processes of digital forensics and challenges of digital forensics.

6.0 TUTOR-MARKED ASSIGNMENT

a. Define Digital Forensics.

b. What are the various types of digital forensics?

7.0 REFERENCES/FURTHER READING

Ashcroft, J., Daniels, D.J. & Hart, S.U. (1994). Forensic Examination of Digital Evidence: A Guide for Law Enforcement. U.S Department of Justice Program. National Institute of Justice Special Report. Available at: https://www.ncjrs.gov/pdffiles1/nij/199408.pdf

Franke, K. & Arnes, A. (2018). Challenges in Digital Forensics. In A. Arnes (ed.). *Digital Forensics* (1st ed.). pp. 313-317. N.J: Hoboken.

International College of Security Studies (n.d.). Digital Forensics: Different Types of Digital Forensics. Available at: https://icssindia.in/digital-forensics-types-digital-forensic/

Roussev, V. (2017). *Digital Forensic Science: Issues, Methods, and Challenges*. San Antonio: Morgan & Claypool Publishers Series.

Sachowski, J. (2018). *Digital forensic and investigations: People, processes, and technologies to defend the enterprise*. Boca Raton: CRC Press-Taylor and Francis Group.

UNIT 3 THIRD PARTY POLICING AND CYBERCRIME PREVENTION

1.0 INTRODUCTION

Criminal activities are usually perpetrated in the presence of, or with the full knowledge a third party. Arguably, such third parties can do something to prevent the crime from happening, or do nothing about it, or even aid and abet it. Regardless of these likely scenarios, certain crime third parties are required by the law to take certain crime prevention responsibilities. Third party policing strategies are employed in many countries of the world including Nigeria.

2.0 **OBJECTIVE**

This unit focuses on the definition of third party policing, types of crime third parties and the relevance of third party policing to cybercrime prevention.

3.0 **MAIN CONTENT**

3.1 Definition of Third Party Policing

Buerger and Mazerolle (1998) defined third party policing as police efforts to persuade or coerce other regulators or non-offending persons, such as health and building inspectors, housing agencies, property owners, parents, and business owners, to take some responsibility for preventing crime or reducing crime problems. For example, in Nigeria banks, hotel managers, cyber café managers etc. all perform some kind of third-party policing activities as they are required by law to know their customers and report some suspicious activities of their customers to law enforcement. They can be punished if they fail to do so.

3.1 Types of Crime Third Parties

According to Ndubueze and Igbo (2014) a crime third party is any person who is privy to a crime, present at the crime scene, aided or abetted the crime. They argued that third parties by their critical role in the crime matrix have the capacity to preempt, obstruct, and report crime, particularly cybercrimes. They identified the following crime third parties.

Type I: Aiding and Abetting Third Parties

These third parties are accomplices to the crime. They may knowingly and willingly participate in the commission of the crime or assist the offender to escape apprehension and prosecution after he or she has committed the crime. It is believed that criminals do not always strike in isolation. Most crimes are planned and executed with the knowledge and support of others who share the criminal tendencies of the offender. These third parties may or may not be physically present at the crime scene. They may, however, benefit from the crime. In online advance fee fraud, popularly known as ‘yahoo-yahoo’ in Nigeria, certain third parties are used to collect the transferred fund. If the offender is a male but used a female’s name when committing the crime, he may draft in a female to collect the crime proceed from the bank for a fee. The female accomplice who gets a share of the fund is an aiding and abetting third party. This scenario is particularly common with romance and dating scams.

Type II: Intervening and Rescuing Third Parties:

These third parties may by coincidence be present at the crime scene. They may or may not be known to the victim but try to prevent him or her from being victimized by the offender. These third parties may also ensure that the offender is apprehended after committing the crime. This kind of third party acts on his or her own discretion and goodwill and not under any obligation or compulsion. This third party plays the ‘good Samaritan’ role and is usually appreciated by society. Sometimes, this category of third parties volunteer or are compelled to testify in court. Example, the cyber-cafe users who out of their own volition report illegal online activities by other users.

Type III: On looking and Indifferent Third Parties

These third parties by chance find themselves in the crime scene and are privileged to witness the crime being committed. However they do not in any way facilitate or obstruct the crime. So many factors may account for this kind of attitude in a crime scene. This may include fear of victimization, unwillingness to serve as a witness in court or sheer insensitivity to the plight of the victim. In many urban cities, the initial reaction of most people to a violent crime scene will perhaps be a scramble for safety or a call to the police. Very few people will summon the courage to come to the rescue of a victim.

Type IV: Obligatory and Proactive Third Parties

These third parties are required by law to prevent, pre-empt, control, or report crime. They could be held liable for failure to do so. Increasingly, many private citizens, like property owners and business operators are co-opted by law enforcement agencies for policing of people whom they have some kind of control over. The idea here is to prevent, rather than prosecute crime. For example, cyber cafe managers are required by law to ensure that their services and facilities are not used for illegal activities.

3.3 Third Party Policing and Cybercrime Prevention in Nigeria

Cybercrime is a growing problem in Nigeria. Online advance fee fraud popularly known as “yahoo-yahoo” is one of the most prevalent type of cybercrime in Nigeria. Until recently, cyber cafes served as the major internet access point for many Nigerians. In the early 2000s, online advance fee fraudsters in Nigeria used cyber cafes to carry out their fraudulent activities. Concerned about the upsurge in advance fee fraud schemes online, the government intervened through the re-enactment of a consolidated Advance Fee Fraud and Other Related Offences Act, 2006. Section 13 of the Act places telecommunication and internet service providers as well internet cafes under obligation to perform some third party policing functions. For example, cyber cafes managers are required to exercise the duty of care to ensure that their services and facilities are not utilized for unlawful activities. Although with the proliferation of broadband internet services today, internet fraudsters no longer frequent cyber cafes. However, third-party policing still remains relevant in the prevention of cybercrime. For example, by virtue of section 37 of Cybercrime (Prohibition, Prevention Etc.) Act, 2015 financial institutions are under obligation to perform some third party policing functions.

4.0CONCLUSION

Third party policing is an effective strategy for the prevention of various types of crime including cybercrime. Given that law enforcement personnel cannot possibly be everywhere at all times, third parties can be of immense help by reporting suspected criminal activities to law enforcement agencies.

5.0 SUMMARY

This unit examined the definition of third party policing, types of crime third parties and the relevance of third party policing to cybercrime prevention.

6.0 TUTOR-MARKED ASSIGNMENT

With relevant examples, explain the various types of crime third parties.

7.0 REFERENCES/FURTHER READING

Buerger, M.E., & Mazerolle, L.G. (1998). Third party policing: A theoretical analysis of an emerging trend. *Criminal Justice; Criminology-Law,* 15 (2), 301 – 337.

Ndubueze, P.N., & Igbo E.U.M. (2014). Third Parties and Cyber Crime Policing in Nigeria: Some Reflections. *Policing: A Journal of Policy and Practice.* 8 (1): 59 – 68.

UNIT 4 CHALLENGES OF THE CRIMINAL JUSTICE SYSTEM IN POLICING AND PROSECUTING OF CYBERCRIME

1.0 INTRODUCTION

The criminal justice system is confronted with several challenges in its effort to prevent cybercrime and prosecute cybercriminals. The policing of cybercrime and prosecution of cybercriminals is complicated by the transnational and evolving nature of cybercrime. The various security agencies that are involved in the policing of cybercrime and prosecution of cybercriminals in Nigeria such as the Nigerian Police Force (NPF) and the Economic and Financial Crimes Commission (EFFC) as well as similar law enforcement agencies of other countries are confronted with several challenges in their effort to combat cybercrime. Some of these challenges cannot be effectively tackled without the cooperation of other nation-states that are involved in the investigation of transnational cybercrime cases.

2.0 **OBJECTIVE**

This unit examines the definition of the criminal justice system, perspectives on criminal justice and the challenges confronting the criminal justice system in the policing of cybercrime and prosecution of cybercriminals.

3.0 **MAIN CONTENT**

3.1 Definition of Criminal Justice System

Siegel (2009, p.4) defined the Criminal Justice System as “the system of law enforcement, adjudication, and correction that is directly involved in the apprehension, prosecution and control of those charged with criminal offenses”. The criminal justice system therefore represents government response to crime and it serves to regulate potential, alleged as well as actual criminal activity.

The criminal justice system is made up of three parts: i) Police (law enforcement); ii) courts (adjudication); and iii) corrections (jails, prisons, probation and parole). These agencies of the criminal justice system work together to process criminal cases from its beginning to its closure.

3.1 Perspectives on Criminal Justice

Criminal justice can be viewed from different perspectives. Fradella, Burke, and Joplin (2015) have identified five perspectives on criminal Justice as follows:

i. **i. Criminal Justice as a System:** This has to do with the ways criminal justice agencies - that is the police, courts and corrections work together in order to process a case from the beginning of the case to its end.

ii. **ii. Criminal Justice as a Profession:** A profession is a career field that meets criteria such as educational background, adoption of an ethical code, performing specialized tasks, having mechanisms for quality control, prestige as a member of the profession and life time membership in the profession. Criminal Justice can be considered as a profession because it fulfills the six criteria of a profession mentioned above.

iii. **iii. Criminal Justice as Bureaucracy:** The Criminal Justice System is built around a bureaucratic model. Max Weber believes that a bureaucratic agency is governed by many rules, polices, and procedures, is organized in a hierarchy with clear lines of supervision of employees; requires substantial amount of paper work to document activates and requires training of employees. These are applicable to the criminal justice agencies.

iv. **iv. Criminal Justice as a Moral Agent:** Criminal justice practitioners make decisions that both influence and are influenced by notions of morality. Morality is basically about behaviours and actions that are considered right or wrong by society. Criminal justice must also address broad moral questions that are of great interest to society.

v. **v. Criminal Justice as an Academic Discipline:** Criminal justice as an academic discipline of study has been traced to the 1920s when a few universities started offering criminal justice courses and programmes.

Despite these five perspectives on criminal justice, the perspective of the criminal justice in many societies seems to be biased towards the first perspective which regards criminal justice as a system.

3.3 Challenges of the Criminal Justice System in Policing and Prosecuting Cybercrime

The criminal justice system is confronted with several challenges in policing and persecuting cybercrime in Nigeria. Ndubueze (2020, Forthcoming) discussed some of the challenges as follows:

i. **Deterritorisation**

It has been noted that it is practically impossible to know the boundaries of the internet and systems on it at any point in time. This poses serious challenge for online policing. Deterritorisation introduces new variables to policing and may not be understood by a not too computer-savvy police officer.

ii. **Jurisdictional Issues**

Cybercrime is trans-national in nature and thus issues of jurisdiction clearly constitute major obstacle in its effective prosecution. For example, a cybercrime syndicate who reside in different countries can coordinate a cyber attack that may potentially affect victims in over a hundred countries.

iii. **Extradition Protocols**

The extradition of transnational offenders is usually a difficult process complicated by legal technicalities. Dual criminality requirements entails that during all material times the act for which eradication is sought must be a criminal offence in both the requesting and responding countries.

iv. **Identity Flexibility**

The nature of virtual communities is such that allow members to remain anonymous if they so desire. It also allows for identity falsification and identity theft. This can frustrate investigation and policing efforts.

v. **Nature of Electronic Evidence**

The increased launching of new digital devices with specialized software and data-handling protocols and the development of advanced data hiding and data protection techniques frustrate the collection of digital evidence. Law enforcement personnel need to be specially trained on digital evidence recognition, seizure, packaging, transportation, and storage.

vi. **User Behaviour and Naivety**

The first line defense for every internet active person is precaution. However precaution can only be taken when the user is well aware of the activities of cyber criminals online. Many internet users in developing countries are oblivious of the tricks and tactics of cybercriminals.

vii. **Proliferation of Encryption Programmes**

There is an upsurge in computer based encryption programs. It is noted that cybercriminals can hide files in slack space of computer hard drive or store them on a remote server located in another geographic jurisdiction. They can also encrypt, misleadingly title, or even mix files with several unrelated files. This can complicate policing and investigation processes.

viii. **Dearth of Cyber Crime Legislations**

Governments have always been reactive to the problem of crime. Many countries do not have enough cybercrime legislations. Even where cybercrime laws exist, they are no universal.

4.0CONCLUSION

High-technology crimes such as cybercrimes are always evolving and cybercriminals are always devising new methods of perpetrating their criminal activities. Policing and prosecuting cybercriminal is a herculean task. One of the major issues of concern is the transnational nature of cybercrime. Whilst there are several international treaties on mutual cooperation in the fight against cybercrime, not all countries have rectified such treaties. The absence of comprehensive cybercrime legislation in some countries is another major setback in the fight against transnational cybercrime.

5.0 SUMMARY

This unit examined the definition of the criminal justice system, perspective on criminal justice and the challenges confronting the criminal justice system in the policing of cybercrime and prosecution of cybercriminals.

6.0 TUTOR-MARKED ASSIGNMENT

Discuss the challenges confronting the criminal justice system in the policing of cybercrime and prosecution of cybercriminals

7.0 REFERENCES/FURTHER READING

Owen, S.S., Fradella, H.F., Burke, T.W. &Joplin, J.W. (2015). *Foundations of Criminal Justice*. New York: Oxford University Press.

Ndubueze, P.N. (2020, Forthcoming). Cybercrime and the Justice System. In A.A. Aderinto (e.d.). *The Criminal Justice System in Nigeria*. University of Ibadan, Oyo State,Nigeria.

Siegel, L.J. (2009). *Essentials of Criminal Justice* (6thed.). Belmont: Wadsworth.