NATIONAL OPEN UNIVERSITY OF NIGERIA

SCHOOL OF ARTS AND SOCIAL SCIENCES

COURSE CODE: CSS 852

COURSE TITLE: CYBER CRIMINOLOGY AND VULNERABILTIES

NATIONAL OPEN UNIVERSITY OF NIGERIA

FACULTY OF SOCIAL SCIENCES

CRIMINOLOGY AND SECURITY STUDIES DEPARTMENT

COURSE CODE: CSS 852

COURSE TITLE:

CYBER CRIMINOLOGY AND VULNERABILITIES

Cyber Criminology and Vulnerabilities

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

INTRODUCTION

Welcome to CSS 852: Cyber Criminology and Vulnerabilities

CSS 852 is a second semester 3 Credit Units course that provides students with insights into the issues around deviance, crime and terrorism in the cyberspace. It is prepared for students enrolled in the Doctor of Philosophy Programme of study in Criminology and Security Studies in the National Open University of Nigeria (NOUN).

AIM

a) To introduce students to the fundamental issues around the spate of deviance, crime and terrorism in the cyberspace.

b) To enable students appreciate the role of the relatively young discipline of cyber criminology in interrogating the issues of disorder, crime and criminality in the cyberspace.

c) To guide students to the understanding of how certain twenty-first century social forces shaped the thinking and theorizing of early cyber criminologists.

d) 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 context, concerns, and future directions of the discipline of cyber criminology.

b) To discuss the evolution, classification, cost and other dynamics of cybercrime.

c) To critical review some theories that are relevant in the explanation of deviance, crime and terrorism in the cyberspace.

d) To interrogate some contemporary issues in cybercrime and cyber security and their global implications.

e) To assess the state of cyber crime legislations/cyber security initiatives and the challenges confronting the Nigeria Criminal Justice System in policing and prosecuting cybercrime.

WORKING THROUGH THIS COURSE

To complete this course you are required to read the study units and the recommended books. Each study unit contains a self-assessment exercise, and at some point in the course you will be required to submit your assignment 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

- Course guide
- Study units
- Textbooks, journals and other reference sources
- Assignment file
- Presentation

STUDY UNITS

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

Module 1: Cyber Criminology: Context, History, Concerns, Contribution and Challenges

Unit 1: The Contexts of the Emergence of Cyber Criminology

Unit 2: The History of Cyber Criminology

Unit 3: Definition, Concerns and Current State of Cyber Criminology

Unit 4: Challenges of Cyber Criminological Research

UNIT 1 THE CONTEXT OF THE EMERGENCE OF THE SUB-DISCIPLINE OF CYBERCRIMINOLOGY

CONTENTS

1.0 INTRODUCTION

In order to appreciate the traditional concerns of the sub-discipline of cyber criminology, there is need to first trace its origin. This unit examines the twenty-first century social forces that prepared the grounds for the emergence of cyber criminology.

2.0 OBJECTIVE

This unit is intended to provide you with the knowledge about four critical social forces that had profound impact on the sub-discipline of cyber criminology. At the end of the unit you will specifically understand how globalization, the internet revolution, mediatization and digitization as well as growth of virtual communities influence the thinking and theorizing of early cyber criminologists.

3.0 MAIN CONTENT

3.1 The Context of the Emergence of the Sub-discipline of Cyber Criminology

Cyber criminology is one of the newest sub-disciplines of the discipline of criminology. The term "Cyber Criminology" was academically coined by K. Jaishankar, an Indian Professor of Criminology in 2007 (Ndubueze, 2017).

Ndubueze (2017) identified some twenty-first century global social forces that influenced the development of the discipline of cyber criminology which include globalization, the Internet revolution, mediatization/digitization and the growth of virtual communities.

i.) **Globalization:** Scholars have argued that globalization has redefined political and geographical space thereby creating the sense of a global village that is facilitated by new communication media such as live television coverage of international events and crisis, the Internet as well as e-mail. The net effect of this development is crime as globalization opens up new opportunities for criminality. Consequently, early cyber criminologists were intrigued by the dramatic impact of globalization on people and

governments around the world and specifically how it has facilitated crime and criminality.

ii.) **The Internet Revolution:** The globalization crusade was facilitated by the Internet revolution that climaxed worldwide in the 2000s when the digital divide began closing-up with relatively easy access to broadband across the world and particularly in developing countries, including Nigeria. The establishment of Internet technology left in its wake new patterns of crime and criminality hitherto unknown to humanity. Therefore, early cyber criminologists were interested in interrogating the dynamics as well as dilemmas of crime in the Internet age. Moreover, they were interested in understanding how the social order is disrupted by these developments and more importantly how order can be restore in a seeming chaotic cyberspace.

iii.) **Mediatisation and Digitization:** Mediatisation refers to a situation whereby social communications which occurred on a face-to-face basis are increasingly facilitated by technical intermediation. Digitization refers to the process through which information is converted into a digital format. Social media sites are emerging as platform not only for mediating business and leisure related communications but also as platforms for mediating deviant and criminal terror related communications. Social media use and

abuse has raised profound concern among citizens, corporate entities and governments across the world. Early cyber criminologists wanted to know how traditional modes of communication are largely replaced and sometimes eroded by the new media. They were also interested in investigating how the social media is increasingly being used by deviant, criminal and terrorist elements to facilitate their activities.

iv.) **Growth of Virtual Communities:** Virtual communities have been described as social aggregations with general values and interest on the Internet, and consist of four elements: people, a shared purpose, policies, and computer system. They are created through technologies such as: websites, chartrooms, Internet forums, instant messaging, online game worlds, mobile phones and text/audio/video-massaging. Interestingly, virtual communities have assumed a life of their own as it were, culminating in the massive migration of people from offline, in-person communication patterns to online, virtual communications. Therefore, early cyber criminologists were interested in understanding the various issues surrounding digital communities.

4.0 CONCLUSION

Early cyber criminologists were interested in understanding how the above four social forces affected traditional patterns of social relationships and how they facilitated crime and disorder in the contemporary times. This quest invariably gave rise to cyber criminological thinking and theorizing.

5.0 SUMMARY

The unit exposed us to some twenty-first century social forces that influenced cyber criminological thinking and theorizing namely: globalization, the internet revolution, mediatization and digitization as well as growth of virtual communities.

6.0 TUTOR-MARKED ASSIGNMENT

1. Discuss the 21st century social forces that influenced the emergence of the discipline of cyber criminology as identified by Ndubueze (2017).

7.0 REFERENCES/FURTHER READING

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

UNIT 2 THE HISTORY OF CYBERCRIMINOLOGY

CONTENTS

1.0 INTRODUCTION

Having identified some 21st century social forces that prepared the ground for the emergence of the sub-discipline of cyber criminology in the previous unit, this unit traces the historical development of cyber criminology. It presents the profile of the founding father of the discipline, Karuppannan Jaiskankar.

2.0 OBJECTIVE

This unit will provide you with the knowledge about the historical development the sub-discipline of cyber criminology. At the end of the unit you will be able to trace the history of cyber criminology, identify some early cyber criminologists and know other disciplines that share similar concerns with cyber criminology.

3.0 MAIN CONTENT

3.1 Intellectual Roots

Arguably, the combined forces of globalization, internet revolution, mediatization and digitization as well as growth of virtual communities had profound and far reaching impact on the social structure and triggered a demand for social order. Way before the formal establishment of cyber criminology as a sub-discipline of criminology in 2007, some scholars referred to as early cyber criminologists had

shown concern about the growing spate of crime and disorder in the cyber space. Such scholars include: Bachmann (2007), Brenner (2001), Holt (2003), Jaishankar (2007) Wall (2001), Yar (2005), among others (see Ndubueze, 2016). However, their research efforts found expression within mainstream criminology. But as the cyberspace became more criminogenic and the concerns grew there became a need for a distinct discipline within the social sciences that would focus on the emerging issues. This led to the coining word "Cyber Criminology" by Jaishankar in 2007 (Jaishankar, 2010, Ndubueze, 2017).

3.2 Historical Development

Cyber criminology is one of the newest sub-disciplines in the discipline of criminology. The term "Cyber Criminology" was academically coined by K. Jaishankar, an Indian Professor of Criminology in 2007 (Jaishankar, 2017, Ndubueze, 2017). Jaishankar was concerned about the spate of crime and criminality on the cyberspace. Beyond that he was concerned that in spite of the fact that scholarly inquiry into the emergence of the cyberspace as a hotbed for a novel criminal activity dates back to the 1990s, the discipline of criminology was lagging behind in interrogating the dynamics of the new form of crime - cyber crime. Hence, he established the discipline of cyber criminology to address this research gap. He defined cyber criminology as "the study of the causation of

crimes that occur in the cyberspace and its impact in the physical space" (Jaishankar, 2007a, para. 1). Jaishankar (2018) explained that cyber criminology is multi-disciplinary in nature as it interfaces with criminology, sociology, psychology, victimology, information technology and computer/internet sciences.

Furthermore, the new discipline was given impetus with the introduction of a dedicated open access journal known as *International Journal of Cyber Criminology* (IJCC) in 2007 by Jaishankar. In the maiden edition of the journal, Jaishankar underscored the need for the literature in the area to be documented. He observed that difficulty in collaboration among the disciplines of Internet Science, Computer Science and Criminology pointing out that this is because of the difference in their languages. Jaishankar envisaged that the new journal would provide a veritable platform for the publication of robust interdisciplinary researches among Internet scientists; Computer scientists; Communication specialists and Criminologists (see Jaishankar, 2007). The International Journal of Cyber Criminology has grown over the years to become a Scopus indexed journal and has till date published thirteen issues spanning different aspects of cyber criminology and reflecting by all intent and purposes its interdisciplinary scope. The journal is international in outlook with the editorial board and advisers as well

as contributors coming from across the countries of the global north and the global south.

Moreover, the discipline of Cyber Criminology has become more mainstreamed into the curriculum of many Universities. For example, Jaishankar (2018) noted that University of Alabama, Regis University, Saint Anslem College and Purdue University, USA offer a minor in Cyber Criminology, while Florida State University, USA offers a major in Cyber Criminology. In Nigeria's Federal University of Dutse, students undertaking Masters in Criminology and Security Studies are required to offer a 3 credit course in Cyber Criminology in their second semester.

3.3 Karuppannan Jaishankar

The Founding Father of Cyber Criminology, Professor Karuppannan Jaishankar is the Head, Department of Criminology, Raksha Shakti University, Lavad, Gandhinagar, Gujarat, India. He has been involved in researching and publishing on cybercrime and related subjects. He is also 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 known as Space Transition Theory in 2008.

3.3 Allied Disciplines

The emergence of the cyber space in the 20th century has elicited concerns from various academic disciplines. These disciplines include: Computer science, Criminology, Cyber security Information Technology, Engineering, Law, among others. But, Jaishankar (2018), observed that criminology unlike some allied disciplines did not respond fast enough to emerging new space and the new form of criminality it created.

4.0 CONCLUSION

Cyber criminological thinking and theorizing started in the early days of globalization, internet revolution, mediatization and digitization as well as virtual communities. These forces altered the social dynamics of communication and created some degree of disorder in the society. Therefore, some criminologist were enormously concerned about the disorder, asked pertinent questions and sought for answers. These formed the nucleus for the establishment of the discipline by Jaishankar in 2007.

5.0 SUMMARY

The unit traced the historical development of the discipline of cyber criminology and discuses the contributions of its founding father, Professor Karuppannan

Jaishankar. It underscored the role of some early cyber criminologists in the emergence of the discipline and identified some allied disciplines.

6.0 TUTOR-MARKED ASSIGNMENT

1. Account for the history of Cyber Criminology.

2. Discuss the contributions of Professor K. Jaishankar to the discipline of Cyber Criminology.

7.0 REFERENCES/FURTHER READING

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

Jaiskankar, K. (2010). Editorial – The future of cyber criminology: Challenges and opportunities. *International Journal of Cyber Criminology*, 4 (1 & 2), 26-31.

Jaiskankar, K. (2017). Cyber criminology as an academic discipline: History. contribution, and impact. *International Journal of Cyber Criminology*, 12 (1), 1-8.

Jaiskankar, K. (2018). Commemorating a decade in existence of the International

Journal of Cyber Criminology: a research agenda to advance the scholarship on cyber crime. *International Journal of Cyber Criminology*, 11 (1), 1-9.

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.

UNIT 3: CONCERNS AND CONTRIBUTIONS OF THE DISCIPLINE OF CYBER CRIMINOLOGY

CONTENTS

1.0 INTRODUCTION

There are three traditional concerns of the discipline of cyber criminology. They include: cyber deviance, cyber crime and cyber terrorism. These three distinct but overlapping areas are explained in this unit. The various contributions of the discipline of cyber criminology to the search for social order in the cyberspace are also discussed.

2.0 OBJECTIVE

This unit will equip you with a good appreciation of the fundamental focus of cyber criminological inquiry as well as its contributions. At the end of the unit you will be able to explain the three fundamental concerns of cyber criminology and the various contribution of the discipline to the quest for a senile cyberspace.

3.0 MAIN CONTENT

3.1 Cyber Deviance

Conventionally, behaviours that are contrary to the code of conduct of a society or social group are generally regarded as deviant. In the cyberspace, behaviours that are socially reprehensible or immoral but not criminalized are known as cyber deviance. There are a wide range of behaviours that are exhibited online by

internet users that obviously cross the lines of courtesy and sometimes decency. It is expected that no rational thinking member of society will contemplate or indulge in such behaviour, but such behaviour as abnormal as they may seem are not prohibited by the state and as such those who indulge in them do not face formal criminal sanction. Examples of such behaviour may include: use of vulgar language in social media communications, posting of very personal information on the social media, forwarding of irrelevant posts in social networking groups, use of pseudo names in social media accounts, loitering in the cyberspace etc. Therefore, cyber criminologists are concerned about interrogating the dynamics of the emergence and operations of deviant sub-culture in the digital age (Ndubueze, 2017).

3.1 Cybercrime

Cybercrime fundamentally entails the use of computer systems/allied digital devices and networks for the commission of outlawed conducts. It includes all online behaviours and activities that are prohibited by the criminal law and for which appropriate criminal sanctions are prescribed for defaulters. Nhan and Bachmann (2015) argued that a broad definition of cybercrime will encompass three important components:

(i) Its perpetration through electronic networks;

(ii) The role of technology and

(iii) The relevant laws

The foregoing argument underscores that fact that cybercrimes are usually perpetrated through electronic networks; they are technologically-enabled and are criminalized by extant legislations in certain jurisdictions. In Nigeria, cybercrime is criminalized by the Cybercrime (Prohibition, Prevention, etc.) Act, 2015. The Act which is the first comprehensive legislation on cybercrime in Nigeria provides for a coordinated and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrime in Nigeria.

Offences covered in the Act include:

- Offences against critical national information infrastructure;
- Unlawful access to a computer;
- Registration of cybercafés;
- System interference;
- Interpreting electronic massages, emails, electronic money transfers;
- Tampering with critical infrastructure;

- Willful misdirection of electronic messages;
- Unlawful interruptions;
- Computer related forgery;
- Computer related fraud;
- Theft of electronic devices;
- Unauthorized modification of computer systems, network data and system interference;
- Electronic signature;
- Cyber terrorism;
- Exceptions to financial institutions posting and authorized options;
- Fraudulent issuance of e-instructions;
- Reporting of cyber threats;
- Identity theft and impersonation;
- Child pornography and related offences;

- Cyberstalking;
- Cybersquatting;
- Racist and xenophobic offences;
- Attempt, conspiracy, aiding and abetting;
- Importation and fabrication of e-tools;
- Breach of confidence by service providers;
- Manipulation of ATM/POS Terminals;
- Employees responsibility
- Phishing, spamming, spreading of computer virus;
- Electronic cards related fraud;
- Dealing in card of another;
- Purchase or sale of card of another;
- Use of fraudulent device or attached e-mails and websites.

The penalties for the above listed offences are expressly stated in the relevant sections of the Act.

3.3 Cyber Terrorism

Cyber terrorism refers to the use of the Internet or associated information technology to perpetrate terrorist activities. Caruso (as cited in Sundaran and Jaishankar, 2008, p.596) defined it as "the use of cyber tools to shut down critical national infrastructure (such as energy, transportation, or government operations) for the purpose of coercing or intimidating a government or civilian population".

Terrorist organizations across the world are increasingly utilizing the Internet to raise fund, recruit, indoctrinate, train, deploy and supervise members. Apart from targeting and attacking critical national infrastructure, terrorist organizations also use the internet to coerce the government and intimidate citizens.

Cyber criminologists are interested in studying how the internet is used by terrorist groups to pursue their goals.

3.3 Contributions of the Discipline of Cyber Criminology

The discipline of cyber criminology has contributed immensely to our understanding of the spate of deviance, crime and terrorism in the cyberspace and

societal reaction to them. Below are some of the specific contributions of the discipline of cyber criminology.

i. ***Growth of Multi-disciplinary Researches***: Since the establishment of the discipline of cyber criminology in 2007 several multidisciplinary researches on issues around deviance and crime in the cyber space have been conducted.

ii. ***Emergence of Cyber Dedicated Journals and Textbooks***: In an effort to encourage the dissemination of the scholarly output of cyber criminologists and allied professionals several cyber dedicated journals have been established and textbooks published since the establishment of cyber criminology. Examples include International Journal of Cyber criminology (IJCC) which was established in 2007 by the founding father of cyber criminology, Professor Karuppannan Jaishankar in 2007, Cyber Criminology and Technology Assisted Crime Control: A Reader edited by P.N. Ndubueze (2017) and so on.

iii. ***Hosting of Dedicated Academic Conferences*:** Several cybercrime-related conferences have been organized around the world. These conferences often bring together both cybercrime scholars/researchers and practitioners to enable them brainstorm on emerging deviance and

crime in the cyberspace and how to restore social order. The state and challenges of scholarship in this emerging area is usually discussed. One of such conferences is a United Nations Office on Drug and Crime (UNODC) funded International Conference on Linking Organized Crime with Cyber Crime which held at Hallym University, South Korea on June 7th and 8th 2018.

iv. ***Training of Cyber Specialized Manpower:*** Since the establishment of the discipline of cyber criminology in 2007 many universities now run bachelor programmes in cyber criminology**.**

4.0 CONCLUSION

Early cyber criminologists are interested in three fundamental areas of inquiry. These areas include: cyber deviance, cybercrime and cyber terrorism. Although, deviance, crime and terrorism are not new phenomena, they have become more sophisticated and widespread with the reemergence of internet and digital technologies.

5.0 SUMMARY

The unit discussed the traditional concerns of the discipline of cyber criminology: cyber deviance, cyber crime and cyber terrorism. It also examined the various contributions of the relatively young discipline of cyber criminology.

6.0 TUTOR-MARKED ASSIGNMENT

What are the concerns and contributions of the discipline of cyber criminology?

7.0 REFERENCES/FURTHER READING

Cybercrime (Prohibition, Prevention, etc.) Act, 2015.

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.

Sundaram, P.M.S. & Jaishankar, K. (2008). Cyber terrorism: problems, perspectives, and prescription. In F. Schmallager & M. Pittaro (eds.), *Crimes of the Internet* (pp. 593 – 611). Upper Saddle River, NJ: Prentice Hall.

UNIT 4: CHALLENGES OF THE DISCIPLINE OF CYBER CRIMINOLOGY

CONTENTS

1.0 INTRODUCTION

The discipline of Cyber Criminology is confronted with several challenges since its establishment in 2007. These challenges include definitional, methodological and theoretical issues; lack of adequate attention from mainstream criminology; multidisciplinary nature of the discipline; dearth of dedicated researchers, research centres and standardized data and so on (Ndubueze, 2016). They are discussed in this unit.

2.0 OBJECTIVE

This unit will expose you to some of the fundamental challenges that confront the discipline of cyber criminology. At the end of the unit you will be able to discuss the various challenges that confront the relatively young discipline of cyber criminology.

3.0 MAIN CONTENT

3.1 Definitional, Methodological and Theoretical Issues

The discipline of cyber criminology is faced with the challenge of framing a generally acceptable definition of its concepts, arriving at uniformed methods and widely embraced theories. There is no generally accepted definition of cyber crime and several other concepts that are often used in cyber criminological studies. This is partly because of the interdisciplinary nature of cyber criminology. This factor

also explains why there is lack of uniformed methods. For example, the methods of Computer Science, a discipline that is housed in the Faculty of Computing in some Nigerian universities is obviously different from those of Criminology which is housed in the Faculty of Social Sciences in Nigerian universities. More so, many criminological theories were established before the emergence of cybercrime as an area of criminological research. By implication, those theories do not sufficiently capture the spate of crime and criminality in the cyberspace. So far there is only one theory: The Space Transition Theory of Cybercrime by Jaishankar (2008) that is cybercrime-specific. This, obviously, constitutes a challenge for cyber criminological studies.

3.2Lack of Adequate Attention from Mainstream Criminology

Cyber Criminology is one of the latest sub-fields of criminology. Unfortunately, most criminology textbooks do not appreciate the place of this new field in twenty-first century criminology as they do not have dedicated chapters on cyber criminology. The few that discuss cybercrimes barely make explicit reference to cyber criminology. An Indian Criminologist, Professor Karuppannan Jaishankar, was one of the early scholars who made serious efforts to promote the new field. He launched an open access journal dedicated to cyber criminology known as: "International Journal of Cyber Criminology" in 2007 and published a book

entitled: “Cyber Criminology: Exploring Internet Crimes and Criminal Behaviour” in 2011. These publications brought to fore the increasing state of crime and disorder in the cyberspace and the need for social order which is the focus of the discipline of cyber criminology.

3.3 *Multi-disciplinary Nature of the Discipline*

Cyber criminology is multi-disciplinary in nature. This is because it draws the interests and inputs of researchers from Criminology, Victimology, Sociology, Internet science and Computer science (Jaishankar, 2007). This makes the issue of common definition of concepts problematic. Internet science and Computer science in their study of cybercrime often use technical terms that are not common in the social sciences. Even where concepts are common, they are defined from strictly discipline-tinted lenses that leave little room for appreciation by allied disciplines. Sometimes publications on cybercrime emanating from non-social science disciplines are rather loaded with jargons that the average social scientist may not understand.

3.4 Dearth of Dedicated Researchers, Research Centers and Reliable/Standardized Data

There has been an unprecedented growth in the internet usage population across the world, including Nigeria in the past one decade or so. More so, there has been a

corresponding spike in the growth of digital technologies. Through the Internet-of-Things (IoT) technology, many devices are remotely connected to the internet. These developments have profound implications for social order in the cyberspace. However, there is dearth of dedicated cyber criminologists in developing countries of Africa including Nigeria. Similarly, there is dearth of cybercrime dedicated research centres in Africa. Most of the centres are found in the developed countries and this explains why most of the path-breaking cybercrime studies emanate from there. In addition, there is also dearth of reliable and standardized data. This is partly because of the gaps in reporting and measuring practices of cybercrime.

4.0 CONCLUSION

The advancement of the frontiers of the discipline of Cyber Criminology has been fraught with some challenges. However, with the growing interest in cyber criminological studies it is expected that these challenges will be addressed. More so, there are high prospects that Cyber Criminology will become more mainstreamed within the discipline of Criminology.

5.0 SUMMARY

The unit discussed some of the critical challenges confronting the discipline of cyber criminology identified by Ndubueze (2016). These challenges revolve

around definitional, methodological and theoretical issues; neglect from mainstream criminology; multidisciplinary posture; and dearth of dedicated researchers, research centres, reliable/standardized data.

6.0 TUTOR-MARKED ASSIGNMENT

What are the challenges confronting the discipline of Cyber Criminology?

7.0 REFERENCES/FURTHER READING

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

Jaishankar, K. (2011) Introduction: Expanding cyber criminology with an avant-garde Anthology. In K. Jaishnakar (ed.). *Cyber criminology: Exploring internet crimes and criminal behaviour,* Boca Raton: CRC Press. xxvii-xxxv.

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: Evolution, Typologies and Dynamics of Cybercrime

Unit 1: Evolution of Cybercrime

Unit 2: Typologies of Cybercrime

Unit 3: Measuring Cybercrime

Unit 4: Cyberspace as Fifth Domain of Warfare

UNIT 1 EVOLUTION OF CYBERCRIME

CONTENTS

1.0 INTRODUCTION

Before the advent of the internet and digital technologies, law enforcement agencies were preoccupied with law and order in the physical space. The internet revolution has changed that landscape. This unit traces the historical evolution of cybercrime and explains how cybercrime emerged over a period of three generation.

2.0OBJECTIVE

At the end of this unit, you will be able to trace the historical development of cybercrime. You will specifically learn Marcum (2014) account of how cybercrime emerged over three generations.

3.0MAIN CONTENT

3.1 First Generation of Cybercrime

Marcum (2014) traced the evolution of cybercrime to a continuum of development that involved 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.

3.2 Second Generation of Cybercrime

The second generation of cybercrime is those that use networks. Hacking and cracking are 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 phone 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 steal money from telecommunications 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.

3.1 Third Generation of Cybercrime

The Third generation of cybercrime came into being as a result of the broadband ability of the internet and is identified by the nature of the distribution. The third generation of cybercrime would not exist if the Internet was not developed as they only occur in the cyberspace. They are therefore considered the true cybercrime. Examples include spam mails, viruses, malwares etc.

4.0 CONCLUSION

In its early days, cybercrime basically focused on the illegal exploitation of mainframe computers and their operating systems and it was not financially motivated. Today, cybercrime has evolved into a highly complex criminal activity involving organized crime networks for the most part.

5.0 SUMMARY

The unit discussed the emergence of cybercrime from its first generation to the third. From a relatively not too complex malicious act to a sophisticated organized criminal behaviour.

6.0 TUTOR-MARKED ASSIGNMENT

Discuss Marcum's (2014) evolution of cybercrime across three generations.

7.0 REFERENCES/FURTHER READING

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

UNIT 2 TYPOLOGIES OF CYBERCRIME

CONTENTS

1.0 INTRODUCTION

Scholars have offered different typologies of cybercrime. These typologies are based on certain considerations such as the role played by technology and based on

the equivalent of the crimes in the existing criminal law. It is important to note that the typologies are not exhaustive and may not be mutually exclusive in all cases. However, they provide a framework for understanding of the taxonomy of cybercrime.

2.0OBJECTIVE

This unit covers Wall's (2001) four classifications, Furnell (2002) two classifications and Gordon and Ford (2006) three classification of cybercrime. At the end of this unit you will learn about the components of the aforementioned cybercrime classifications and know where the various types of cybercrime fit in.

3.0MAIN CONTENT

3.1 Wall (2001) Typology of Cybercrime

There are several classifications of cybercrime in the extant cyber criminological literature. However, Wall's classification is perhaps the most frequently cited in the literature. Wall (2001) identified four categories of cybercrime namely: cyber trespass, cyber deceptions/theft, cyber pornography and cyber violence.

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, web defacement etc.

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

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

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.

It is important to note that whereas Wall's typology of cybercrime is neither exhaustive nor mutually exclusive, for example an offender can trespass into the victim's computer with the intention of stealing the manuscript of his/her unpublished dissertation. However, the classification provides us with a baseline for the understanding of the different variants of crimes on the internet.

3.2 Furnell (2002) Typology of Cybercrime

Cybercrime has been classified based on the role technology plan in their commission. Cybercrime is fundamentally a high-technology crime. This is because of the central role of technology in its commission.

Furnell (2002) classified cybercrime into the following two broad categories:

i. **Computer-Assisted Crimes**: This refers to the offences in which the computer plays a supporting role in their commission. These offences either existed before the emergence of computer technology or can be committed without the use of computers. Examples include fraud, theft, stalking, etc.

ii. **Computer-Focused Crimes:** This refers to offences that emerge as a direct result of the invention of computers. These offences have no direct parallel in other sectors. Examples include hacking, virus attack, web defacing, etc.

The above classification shows clearly that some cybercrimes that are prevalent in Nigeria today, such as advance fee fraud existed way before computers were invented. The reason why they are more prevalent in the digital age is perhaps

because, unlike in the past, criminal can operate anonymously and can target millions of potential victims at the same time with less risk and efforts.

3.2 Gordon and Ford (2006) Typology of Cybercrime

Gordon and Ford (2006) classified cybercrime into three, namely:

i. **Cybercrime that involve computer and hardware devices**: this type of cybercrime is more technical in nature. Example is hacking.

ii. **Cybercrime that is more human than technology based**: This type of cybercrime has more pronounced human element. Example is online gambling.

iii. **The "crimeware"**: This refers to the malicious software that is used for the commission of crime.

The above classification like the preceding ones are not exhaustive, but as mentioned early they are meant to provide us with a fair idea on how the various kinds of cybercrime can be categorized.

4.0 CONCLUSION

There is no universally accepted taxonomy of cybercrime. Cybercrime scholars have attempted to classify cybercrime based on different indices. Among the three

typologies discussed in this unit, Wall (2001) typology remains the most widely cited in the extant literature of cybercrime.

5.0 SUMMARY

The unit discussed three typologies of cybercrime. They include: Wall (2001), Furnell (2002) and Gordon and Ford (2006) classifications of cybercrime.

6.0 TUTOR-MARKED ASSIGNMENT

Enumerate and explain with vivid examples, Wall's (2001) four categories of cybercrime.

7.0 REFERENCES/FURTHER READING

Furnell, S. (2002). *Cybercrime: Vandalizing the information society*. London: United Kingdom.

Gordon, S. & Ford, R. (2006). On the definition and classification of cybercrime. *Journal of Computer Virology*, 2, 13-20.

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

UNIT 3 MEASUREMENT OF CYBERCRIME

CONTENTS

1.0 INTRODUCTION

Crime measurement is a controversial issue and there are different perspectives on how best to measure crime. Undoubtedly crime measurement is fraught with several challenges. Some of the challenges may arise from people reporting practices and how crime is recorded. There are many crimes that happen behind the scene that are neither reported to the people nor recorded. Arguably, such cases will not reflect in the official crime statistics, therefore the victim survey and self-report offender survey serve to account for the crimes that are not reflected in the official crime statistics. Crime can be measured using the following three indicators: Prevalence (number or proportion of victims within the population). b.) Concentration (number of crimes per victim) and c) Incidence (the number of crime that has occurred in a given area).

4.0 **OBJECTIVE**

This unit focuses on the nature of official crime statistics, victim surveys, self-report surveys and the challenges associated with measuring cybercrime.

5.0MAIN CONTENT

3.1 Official Crime Statistics

Official crimes statistics are information about the nature and extent of crime that are collected from the administrative or agency records or data (Skogan, as cited in Jennigs and Reingle, 2014). The Uniform Crime Report (UCR) is a popular example of an official source of crime statistics.

In Nigeria, the sources of official crime statistics primarily include: the police, courts and correctional service, etc. However, it is important to note that national crime statistics are derived from two major sources:

- **Administrative data**: These include data from the police, courts and correctional service.
- **Surveys**: These include crime victimization surveys and self-report surveys.

3.2 Victim Survey

Victim surveys became necessary given that official crime statistics do not reflect the crimes that are not reported the police. These crimes are referred to as the "dark figure of crime". Victimization surveys are alternatives to measure crime in the community using questionnaires or interviews that ask members of the public

about the crimes which have been committed against them over a people of time and whether or not they have been reported to the police. In Nigeria for example, the Centre for Law Enforcement Education of Nigeria (CLEEN) has conducted several national crime victimization survey.

3.3 Self-Report Survey

Self-report survey is a measure of crime that makes use of anonymous questionnaires or interviews to ask respondents about their own criminal activity. Respondents are given confidential questionnaires that request them to record voluntarily whether or not they have committed any of the listed offenses. According to Igbo (2007:78) "The self-report survey is an attempt to get at the "dark-figures of crime which are not reflected in the official crime statistics. It is targeted at offenders whose offences were not known to the police and who were therefore not arrested at the time of the crime".

3.4 Challenges with Measuring Cybercrime

Crime measurement is generally problematic. This is fundamentally because official measures of crime do not reflect the full picture of crime in society. This is basically because of the 'dark figures of crime' – crimes that are not reflected in the official statistics of crime.

The problem of measuring crime is exacerbated with cybercrime for several reasons. First, cybercrime is a relatively new kind of crime. Law enforcement agencies have been used to traditional policing which takes place in the physical space. Hence, grappling with an abstract space might just be a nightmare for the non-internet savvy law enforcement officer.

Second, many internet users are not skilled. This lack of internet skills exposes them to victimization online. Again, because they are not familiar with the workings of the internet they may be victimized without their knowledge. For example, cyber criminals may install spyware when they download free softwares on their system without them knowing. Hence because they are oblivious of such victimization it will not be reported to law enforcement and will not be captured in the official crime statistics.

Third, the data of large corporations and businesses may be breached by cybercriminals. Cybercriminals may send ransomware to such organizations. Sometimes, the affected organizations may choose to quietly pay the ransom rather than report to relevant law enforcement agencies so as to avoid the negative publicity that doing so may cause. In the aforementioned scenario it is unlikely that such a case would be captured in crime statistics. There is also no guarantee that it

will be captured in the self-report and victimization surveys that are carried out to account for the gaps in the official crime statistics.

4.0 CONCLUSION

There is a consensus among scholars on the fact that no single measure of crime can reflect the full extent of crime. Crime cannot be measured through a single statistical instrument. Surveys, census and administrative records all play an important and complimentary role for a comprehensive understanding of the extent of crime.

5.0 SUMMARY

The unit examined the various measurement metrics available for the counting of crime. It specifically discussed official crime statistics, victim survey and offender self-report survey. The challenges associated with measuring cybercrime were also discussed.

6.0TUTOR-MARKED ASSIGNMENT

What are the challenges that are associated with measuring cybercrime?

7.0 REFERENCES/FURTHER READING

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

Press.

Jennings, W. G. and Reingle, J.M. (2014). *Criminological and Criminal Justice Research Methods*. New York: Wolters Kluwer Law & Business.

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

UNIT 4 CYBERSPACE AS THE FIFTH DOMAIN OF WARFARE

CONTENTS

1.0 INTRODUCTION

The cyberspace has emerged as a battle-domain in contemporary warfare. Before the emergence of the cyberspace national wars had traditionally been fought on

land, sea, air and there are international treaties to regulate conflicts in space. Today, the landscape of warfare has expanded to include the cyberspace. This obviously has some implications for cybersecurity.

3.1 The Cyber War Debate

The term of 'cyber war' has been contested by some authors. The debate has centred on whether war occurs in the cyberspace or not. Stone (2012) has expressed the view that the question of whether or not cyber war exists is really difficult to determine. This, according to him, is because of strategic theory's uncertain explanation of the concept of force, violence and lethality. He argued that the three concepts as well as their relationships with one another prove that cyber attacks can be construed as acts of war. Furthermore, Junio (2013) observed that several well established explanations for war suggest that cyber weapons are more capable of being used offensively than other kinds of military technologies. Clarke and Knake (2010, pp. 30-31) in their famous book entitled "Cyber War" made five conclusions on cyber war:

i. Cyber war is real.

ii. Cyber war happens at the speed of light.

iii. Cyber war is global.

iv. Cyber war skips the battlefield and,

v. Cyber war has begun.

3.2 Cyberspace as the Fifth Domain of Warfare

There are basically five domains of warfare. They include: **land, sea, air, space and cyberspace.**

The cyberspace is increasingly recognized as the fifth domain of warfare around the world. It is believed that an emerging battle is raging among the super powers of the world and that this battle will be fought in the cyberspace. Clarke and Knake (2010) observed that military and intelligence organizations are preparing the cyber battlefield with logic bombs and trapdoors and launching virtual explosive in other countries in peacetime.

3.3 Cyber War in the 20th and 21st Centuries

There have been several incidences that occurred in the twentieth and twenty-first centuries that were described as cyber war. Carr (2012) mentioned some of such incidences. They are summarized as follows:

- In May, 1998 an estimated 3,000 hackers self-organized into a group known as the China Hacker Emergency Meeting Centre, attacked Indonesian government websites in protest.

- On May, 7, 1999 a North Atlantic Throaty Organization (NATO) jet bombed the Chinese embassy in Belgrade, Yugoslavia in error. In less than 12 hours after the accident, the Chinese Red Hacker Alliance was formed and they launched series of attacks several hundred United States government websites.

- In late December 2008. Israel launched Operation Cast Lead against Palestine. The led to cyber war between Israeli and Arabic hackers.

- During the Second Russian-Chechen War (1997-2001), in which the Russian Military invaded the secessionist region of Chechnya to reinstall a Moscow-friendly regime, both sides used cyberspace to engage in Information Operations to control and influence public perception.

- The Russian-Georgia War of 2008 is the first example of cyber-based attack that coincided directly with land, sea and air invasion by a state against another. Russia invaded Georgia because Georgia attacked separatists in South Ossetia. The well coordinated cyber campaign used vetted target list

of Georgian government websites and other strategically valuable sites including the United States and British embassies.

- On July 4, 2009, a few dozen of United States websites, including US government sites experienced a mild DDoS attack. A few days later, South Korean government and civilian websites were also targeted. Carr noted that even though the Democratic People's Republic of Korea was the main suspect, there was no evidence to support that suspicion.

The above incidences which are some of the 20th and 21st incidences of cyber war Carr (2012) cited in his book "Inside Cyber War" underscore the fact that cyber war is real and collaborates the arguments of Clarke and Knake (2010) which was mentioned earlier.

4.0 CONCLUSION

Although some authors have disputed the existence of a cyber war, there is evidence from literature to support the claim about it existence. The understanding and appreciation of the dynamics of cyber war by states is critical in the effort to build strong cyber defenses for critical national infrastructure.

5.0 SUMMARY

The unit examined the debates around the existence of cyber war. It discussed the state of cyberspace as a fifth domain of warfare and outlined some 20th and 21st centuries cyber war incidents to buttress the existence of cyber war and its threat.

4.0TUTOR-MARKED ASSIGNMENT

Explain the nature of cyberspace as the fifth domain of warfare.

7.0 REFERENCES/FURTHER READING

Carr, J. (2012). *Inside Cyber Warfare* (2nd ed.). Beijing: Oreilly.

Clarke, R.A. & Knake, R.K. (2010) *Cyber war: The next threat to national security and what to do about it.* New York: Harper Collins Publishers.

Junio, T.J. (2013). How probable is cyberwar? Bringing IR theory back into the Cyber Conflict Debate. *Journal of Strategic Studies*, 36 (1), 125-133.

Stone, J. (2013). Cyber war will take place. *Journal of Strategic Studies*, 36 (1), 101-108.

Module 3: Cybercrime Theories and Their Applicability

Unit 1: Social Learning Theory (SLT)

Unit 2: Routine Activity Theory (RAT)

Unit 3: General Strain Theory (GST)

Unit 4: Space Transition Theory of Cybercrime (STT)

UNIT 1 SOCIAL LEARNING THEORY

CONTENTS

1.0 INTRODUCTION

There are several theories that have been used in the explanation of crime in the cyberspace. Most of such theories are traditional criminological theories with sociological background. Criminology has been slow in the development of cybercrime specific theories. The only effort in that direction so far is perhaps that of Professor K. Jaishankar who propounded the Space Transition Theory of Cybercrime in 2008.

2.0 OBJECTIVE

This unit will expose you to the major assumptions of the social learning theory. At the end of this unit, you will be able to understand the major assumptions of the theory and how it has been applied by scholars in the explanation of crime in the cyberspace.

3.0MAIN CONTENT

3.1 Social Learning Theory

The basic assumption of the social learning theory is that social behaviour is not determined by inner personality drives or sociological and environmental factors. Instead, it is a cognitive process that engages personality and environment in a continuous process of mutual interaction (Beirne & Messerschmidt, 2015). The emphasis of this theory is that people learn behaviour by observing and imitating others.

Akers social learning theory is a reformulation and extension of Sutherland's differential association theory. Differential association theory posits that criminal behaviour is learned during interaction with others but it does not specify the mechanisms by which such behaviour is learned. However, Akers and his associates used insights from several theories of learning in behavioural theory and social learning theory in psychology to specifically describe how crime is learned (Cullen, Agnew and Wilcox, 2014).

Burgess and Akers (1966) social behaviour, including criminal behaviour is influenced by a complex network of rewards and punishments. There is the likelihood that a given behaviour will continue or increase if it is followed more by reward than punishment. In the same vein, there is the likelihood of the same behaviour to decrease or end if it is followed by more punishment than rewards.

Beirne & Messerschmidt (2015, p.146) summarized Burgess and Akers assumption that criminal behaviour is learned in the following seven stages:

i. Criminal behaviour is learned through direct conditioning or through imitation.

ii. Criminal behaviour is learned both in non-social reinforcing situations (for example, the physical effects of drug use) or nonsocial discriminative situations and through social interaction in which the behaviour of others is either for or against criminal behaviour.

iii. The principal components of learning criminal behaviour occurs in groups that compose the individual's major source of reinforcements: peer friendship groups, the family, schools, and churches.

iv. Learning criminal behaviour – including specific techniques, attitudes, and avoidance procedures-depends on effective and available reinforcers and the existing reinforcement contingencies.

v. The specific types and the frequency of learned behaviour depend on the reinforcement that are effective and available and on the norms by which these reinforcers are applied.

vi. Criminal behaviour is a function of norms that are discriminative for criminal behaviour, the learning of which occurs when such behaviour is more highly reinforced than noncriminal behaviour.

vii. The strength of criminal behaviour is a direct function of the amount, frequency and probability of its reinforcement.

3.2 Applicability and Criticism of Social Learning Theory

Social learning theory has been used by scholars to explain cybercrime. For example, Skinner and Fream (1997) used the social learning theory to explain the etiology of computer crime. Also, Higgins and Makin (2004) used SLT to explain software piracy.

However, social learning theory has been criticized on the grounds that there has not been sufficient research to prove that social learning is the principal process mediating the relationship of social structure and crime as expected by the theory (Cullen, Agnew and Wilcox, 2014).

4.0 CONCLUSION

The nature versus nurture debates is an age long one. However, the social learning theorists believe that nurture exerts more influence on individuals as long as

criminal behaviour is concerned. In other words, they argue that criminal behaviour is not inherited but learned.

5.0 SUMMARY

The unit discussed the major assumptions of the social learning theories. It focused on the variant of Burgess and Akers (1966). It also noted that the theory has been used to explain different aspects of cybercrime. The applicability and weaknesses of the theory were also discussed.

6.0 TUTOR-MARKED ASSIGNMENT

Discuss the major assumptions of the social learning theory. What is the major criticism of the theory?

7.0 REFERENCES/FURTHER READING

Beirne, P. &Messerschmidt, J.W. (2015). *Criminology: A Sociological Approach* (6^{th} ed.). New York: Oxford University Press.

Burgess, R.L & Akers, R.L. (1966). A differential association-reinforcement theory of criminal behaviour. *Social Problems* 14(2): 128-147.

Higgins, G.E., & Makin, D.A. (2004). Does social learning theory condition the

effects of low self-control on college students' software piracy? *Journal of Crime Management,* 2, (2): 1-22.

Skinner, W.F. & Fream, A.M. (1997). A Social learning Theory Analysis of Computer Crime among College Students. *Journal of Research in Crime and Delinquency*, 34, 495-518.

UNIT 2 ROUTINE ACTIVITY THEORY (RAT)

CONTENTS

1.0 INTRODUCTION

Routine activity theory is a variant of environmental criminology. Unlike traditional theories of crime that lay emphasis on the offenders, environmental criminology is concerned with the crime. The major premise of environmental

criminology is that crime will not occur unless the offender finds the opportunity to commit it.

5.0 OBJECTIVE

This unit discusses the fundamental arguments of the routine activity theory. At the end of this unit, you will be able to understand the three things that must coverage at the same time and place before crime can occur. You will also learn how routine activity theory has been used to explain cybercrime as well as the shortcomings of the theory.

3.0 MAIN CONTENT

3.1 Routine Activity Theory (RAT)

Routine Activity Theory (RAT) is a major theory of environmental criminology. It was developed by Cohen and Felson in 1979. The theory argues that three elements must come together in a given space and time for crime to occur. They are:

i. A suitable target.
ii. The absence of a capable guardian that could intervene.
iii. The presence of a motivated offender.

A suitable target can be a person, an object or a place. A capable guardian may include: security guards, police patrol, Closed Circuit Television (CCTV) cameras, vigilant colleagues, neighbors etc. A motivated offender is a person with the intent to commit crime. There is the likelihood of crime occurring when a suitable target is not protected by a capable guardian, where a motivated offender is present. According to RAT, crime will only occur if a motivated offender thinks that a target is suitable and a capable guardian absent (Clarke & Felson, 1993).

3.2 Applicability and Criticism of Routine Activity Theory

Reyns and Henson (2016) investigated the relationship between victims' online routines and their identity theft victimization in Canada. They found that some routine activities increase the chances of victims experiencing identity theft. Kigerl (2012) attempted to use routine activity theory to explain cybercrime at the national level. He was interested in determining the characteristics that predict whether a nation is high in either spamming activity or phishing activity. Using a sample of 132 countries, the study revealed that wealthier nations with more internet users per capita had higher cybercrime activity.

The theory however, has been criticized for not considering the factor that influences the offender's decision to commit crime (Adler, Muller & Laufer, 1998).

4.0 CONCLUSION

Routine activity theory underscores the essence of the convergence at the same time and place of three elements: suitable target, motivated offender and absence of a capable guardian for crime to occur. However, from the perspective of the theory predatory crime can be controlled if for example, we make targets unsuitable or if we increase guardianship for high-risk targets.

5.0 SUMMARY

The unit discussed the three elements that must meet at the same time and place before predatory crime can occur as proposed by the routine activity theorists. It also examined the applicability and criticism of the theory.

6.0TUTOR-MARKED ASSIGNMENT

Using the Routine Activity Theory of Cohen and Felson (1979) explain the risky online behaviours that may make an internet user in Nigeria a suitable target of cybercrime victimization**.**

7.0 REFERENCES/FURTHER READING

Adler, F., Muller, G.O.W., & Laufer, W.S. (1998).*Criminology* (3rd ed.). Boston:

McGraw Hil.

Beirne, P. &Messerschmidt, J.W. (2015). *Criminology: A Sociological Approach* (6th ed.). New York: Oxford University Press.

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

Clarke, R. V. & Felson, M. (eds.) (1993). *Routine activity and rational choice. Advances in Criminological Theory*, *5*. New Brunswick, NJ: Transaction Books.

Cullen, F.T., Agnew, R. & Wilcox, P. (2014). *Criminological Theory: Past to Present*. New York: Oxford University Press.

Kigerl, A. (2012). Routine Activity Theory and the determinants of high cybercrime countries. *Social Science Computer Review*, 30 (4): 470 – 486.

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

Reyns, B.W., Henson, B. and Fisher, B.S. (2016). Guardians of the cyber galaxy: An empirical and theoretical analysis of the guardianship concept from routine activity theory as it applies to online forms of victimization. *Deviant Behaviour*. *Journal of Contemporary Criminal Justice*, 32 (2), 148 – 168.

UNIT 3 GENERAL STRAIN THEORY (GST)

CONTENTS

1.0 INTRODUCTION

Life is full of challenges. These challenges may come in different forms and at different levels of a person's life. Coping in the midst of the vicissitudes of life

may not be easy for some people. Therefore, such people may resort to crime when stressed up. The foregoing argument forms the basis for the assumptions of the general strain theory.

2.0 OBJECTIVE

This unit discusses the major assumptions of the general strain theory. At the end of this unit, you will be able to know the proponent of this theory and his major arguments. You will also learn how the theory has been applied in the explanation of cybercrime as well as the weaknesses of the theory.

3.0 MAIN CONTENT

3.1 General Strain Theory (GST)

Robert Agnew (1992, 2001) presents a new and more elaborate version of the strain theory in his General Strain Theory (GST). General strain theory argues that people engage in crime because they experience strains or stressors. For example they are in dire need of money. This could upset them and lead to different kinds of negative emotions like: frustration, anger, and depression. To reduce or escape from their strains and negative emotions they may resort to crime. Not every person will respond to strain with crime. Criminal coping is probable when the

costs of crime are low and when people are disposed to crime (see, Cullen, Agnew and Wilcox, 2014).

Agnew identified **three strains** that may lead to deviance:

i. Failure of an individual to achieve his/her immediate or future goals.
ii. Loss of a source of stability such as bereavement of a loved one, or break of a relationship.
iii. Confrontation with a negative stimuli e.g. crime victimization, visa denial etc.

Furthermore, in buttressing Agnew's argument, Cullen, Agnew and Wlicox (2014, p.207) enumerated the specific strains that are most likely to cause crime as follows:

- Parental rejection,
- Supervision/discipline that is erratic, excessive, and or harsh,
- Child abuse and neglect,
- Negative secondary school experiences (e.g., low grades, negative relations with teachers, the experience of school as boring and a waste of time),
- Abusive peer relations (e.g., insults, threats, physical assaults),

- Work in the secondary labour market (i.e., 'bad jobs' that pay little, have few benefits, little opportunity for advancement, and unpleasant working conditions).
- Chronic unemployment,
- Marital problems,
- The failure to achieve selected goals, including thrills/excitements, high levels of autonomy, masculine status, and the desire for much money in a short period of time,
- Criminal victimization,
- Residence in economically deprived communities,
- Homelessness,
- Discrimination based on characteristics such as race/ethnicity and gender.

3.2 Applicability and Criticism of General Strain Theory

General strain theory has been applied in the explanation of online crime and criminality. Hay, Meldrum and Mann (2010) used GST and a sample of 400 adolescents in a Southeastern state of the United States to examine the effects of cyberbullying (or cyber harassment) on externalizing and internalizing forms of deviance and to assess whether the relationships differs across genders. The study found that both measure of traditional and cyber bullying were significantly related

to delinquency. Again, the study found that the effects of bullying on self-harm and suicidal tendency were about 70 percent greater in males.

It should be noted that Cullen, Agnew and Wlicox (2014) observed that although data support the predictions of the theory, the effects of some of these strains such as abusive peer relations and discrimination has not been well interrogated. Reid (2015) also noted that whereas, Agnew's version of strain theory have highlighted the impact of strain on future behavior, it did not quite explain all reactions to strain.

4.0 CONCLUSION

When individuals fail to achieve their desired goals or when they experience some relative deprivation or fall victim of a crime, they will experience some level of stress. Arguably, whether they cope or not and how they are able to cope will largely depend on the support systems they have such as family and friends. There is the likelihood that individuals with weak support systems may resort to crime and criminality. Crime may just be their way of ventilating their anger and frustration with the system that they perceive has failed them.

5.0 SUMMARY

The unit discussed the major argument of the general strain theory that is centered on the premise that some individuals who experience strain may be inclined to commit crime. It explained how the theory has been applied in the explanation of cybercrime and the weakness of the theory.

6.0 **TUTOR-MARKED ASSIGNMENT**

Discuss the major arguments of the general strain theory**.** How relevant is the theory in the explanation of cybercrime?

7.0 REFERENCES/FURTHER READING

Hay, C., Meldrum, R., & Mann, K. (2010). Traditional bullying, cyber bulling, and deviance: A general strain theory approach. *Journal of Contemporary Criminal Justice* XX (X) 1-18.

Cullen, F.T., Agnew, R. & Wilcox, P. (2014). *Criminological Theory: Past to Present*. New York: Oxford University Press.

UNIT 4 SPACE TRANSITION THEORY OF CYBERCRIME (STT)

CONTENTS

1.0 INTRODUCTION

The internet revolution is sweeping across the globe and altering traditional work and leisure culture of people. Today people are increasingly adapting to the digital culture where digital tools and devices are now integral part of their daily

activities. As exciting as this development is; it has some deep-seated implications for criminal victimization. The space transition theory addresses how the movement from the physical space to the cyberspace and vice versa impacts crime and criminality in the 21st century.

2.0 OBJECTIVE

This unit discusses the seven assumptions of the space transition theory of cybercrime, which is perhaps one of the most recent theories of criminology. The relevance of this theory in the explanation of crime in the cyberspace and its criticism will be examined.

3.0 MAIN CONTENT

3.1 Space Transition Theory of Cybercrime

The Space Transition Theory was developed by Jaishankar (2008) to explain the causation of crime in the cyber space. Space transition involves the movement of persons from one space to another (e.g., from physical space to cyberspace and vice versa). According to the theory people behave differently when they move from one space to another. The propositions of the theory are as follows:

i. Persons with repressed criminal behavior (in the physical space) are inclined to commit crime in cyberspace, which, otherwise they would not commit in physical space, due to their status and position.

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

iii. Criminal behavior of offenders in cyberspace is likely to be imported to physical space and criminal behavior in the physical space may be exported to cyberspace as well.

iv. Intermittent ventures of offenders into the cyberspace and the dynamic spatio-temporal nature of cyberspace provide the chance to escape.

v. (a) Strangers are likely to unite together in cyberspace to commit crime in the physical space.

a. (b) Associates of physical space are likely to unite to commit crime in cyberspace.

vi. Persons from closed society are more likely to commit crimes in cyberspace 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 (Jaishankar, 2008, pp. 292-296).

3.2 Applicability and Criticism of the Space Transition Theory of Cybercrime

Despite its novelty, many scholars have applied the space transition theory of cybercrime in the explanation of crime and deviance in the cyberspace. For example, Tade (2013) used STT to explain the spiritual dimension of cybercrime otherwise known as 'Yahoo Plus phenomenon'. Also, Ndubueze (2016) used STT to explain the spate of deviance, crime and terrorism in the cyberspace.

The Space Transition Theory is the first attempt to use a cybercrime-specific theory in the explanation of crime and deviance in the cyber space. However, Danquah and Longe (2011) in their study conducted in Ghana found that the Space Transition Theory is not applicable to all categories of cybercrime.

4.0 CONCLUSION

The space transition theory of cybercrime is the first and perhaps the only effort so far to develop a cybercrime-specific theory. The theories discussed in Units 1 to 3: the social learning theory, the routine activity theory and the general strain theory are not specific to cybercrime, even though they have been used in explaining cybercrime. Those three theories have also been used in explaining various kind of physical space crime.

5.0 SUMMARY

The unit discussed the seven assumptions of the space transition theory of cybercrime as well as the theory's relevance in the explanation of cybercrime which it was designed to explain. The criticism of the theory was also discussed.

6.0 TUTOR-MARKED ASSIGNMENT

Using the Space Transition Theory of Jaishankar (2008), provide the explanation for the upsurge in Online Advance Fee Fraud in contemporary Nigeria.

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*,2 (2) 1:37-48

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.

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

Tade, O. (2013). A spiritual dimension to cybercrime in Nigeria: The 'yahoo plus' phenomenon. *Human Affairs*, 23, 689 – 705.

Module 4: Cyberspace Threats and Vulnerabilities

Unit 1: Definitions and Scope of Cyberspace, Threats and Vulnerabilities

Unit 2: Threats to Critical National Infrastructures and Industrial Control Systems

Unit 3: Threats by Organized Criminal and Terrorist Organizations

Unit 4: Digital Pitfalls in Developing Countries

UNIT 1 DEFINTIONS AND SCOPE OF CYBERSPACE, THREATS AND VULNERABILITIES

CONTENTS

1.0 INTRODUCTION

The growing reliance on the internet/digital technologies and the numerous opportunities that they provide has exposed individual internet users, private organizations and governmental agencies to potential cyber attack. Arguably, everyone who is directly or remotely connected to the internet and its associated technologies is vulnerable. This is because cyber deviants, criminals and terrorists are growing in their mastery of the internet infrastructure and the dynamics of digital technologies.

2.0 OBJECTIVE

This unit focuses on the various threats and vulnerabilities that are associated with the cyberspace. At the end of this unit, it is expected that you will have a good grasp of the definitions and scope of cyberspace, threat and vulnerabilities. You

will also understand the extent of the threats and vulnerabilities in nation-states, including Nigeria.

3.0 **MAIN CONTENT**

3.1 Cyberspace

The term "cyberspace" was coined by Gibson (1984, p.51) who described it as:

> A consensual hallucination experienced daily by billions 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.

Lessig (1999) opined that the cyberspace is not just one type of space but rather comprises of many places with different kinds of norms and values. He further pointed out that these norms and values are expressed by spaces through their architecture, which are basically the practices that they enable or disable within their space. Jarman and Yannakogeorgos (2018) argued that the cyberspace is made up of digitally networked information and information technology such as computer terminals, servers, and mobile devices connected to remote or hard drives/servers through a digital network. The two known types of digital networks include: the internet and the intranets.

3.2 Threats

Threat may involve the ability or communication of an intention to harm or destroy (Ortmeier, 2009). It is the perceived likelihood of harm or a likely perpetrator's intention to cause harm (Meloy & Hoffmann, 2013). Threats are not only common in the physical space, they also constitute a challenge to cybersecurity. Computer and cyber infrastructures are susceptible to security breaches. The financial and social cost of such breaches can be profound. Guitton (2013) observed that cyber threats were raised to the national threat level in Germany -2006, France – 2008 and the United Kindom -2008.

The Cybersecurity Information Sharing Act of 2015 (CISA) of the United States defined "**Cyber Threat Indicator**" as information that is necessary to describe or identify-

a) Malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability;

b) A method of defeating a security control or exploitation of a security vulnerability;

c) A security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;

d) A method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;

e) Malicious cyber command and control;

f) The actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat;

g) Any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or

h) Any combination thereof." (S.754 §102(7)).

Chapter three of the National Security Strategy of Nigeria (2019) identified the security threats that will drive Nigeria's security priorities for the next five years as: terrorism and violent extremism, armed banditry, kidnapping, militancy, and separatist's agitations, pastoralist-farmers conflicts, transnational organized crime, piracy and sea robbery, porous borders, cybercrimes and technology challenges. It further identified other national security threats as: socio-political threats, fake news and hate speeches, environmental threats, public health challenges, economic challenges, regional and global security challenges. Moreover, the strategy

identified four critical areas of cyber threats that are very capable of causing profound damage to Nigerian security and economy as follows:

- Cybercrime;
- Cyber espionage
- Cyber conflict; and
- Cyber terrorism.

3.3 Vulnerabilities

According to the US National Institute of Standards and Technology (NIST), vulnerability is "a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source" (Information System Audit and Control Association, 2017, p. 4).

Lin (2012) argued that vulnerability is a component of information technology that can be used to compromise it. He further pointed out that vulnerabilities may be inadvertently introduced through a design or implementation error such as a "bug" or deliberately introduced for example, by a hostile programmer, which may be prone to opportunistic use by an adversary.

Criminals and disgruntle employees can exploit the loopholes in a computer system and networks for different reasons. Vulnerability assessment allows organizations to ascertain the extent to which existing security measures can guarantee the confidentiality, integrity and availability of digital information and systems.

A study by Zhao and Zhao (2015) assessed the security and vulnerability of 50 social media sites and found that most sites:

- Posted privacy and security polices but only few of them clearly stated their execution of the key security measures;
- Had network information that was publicly available via internet search, which was vulnerable to cyber intrusion; and
- Were secured with firewalls, filters, or port closures, with only few ports detected as open, which need more improvement.

3.4 Overview of Cyberspace Threats and Vulnerabilities

It has been observed that "every minute, we are seeing about half a million attack attempts that are happening in the cyberspace" (Australian Computer Society, 2016, p.13). The foregoing undoubtedly underscores the extent of threat that

characterizes the cyberspace. It is highly probable that this figure would have significantly increased over the years. This is because cyber deviants, criminals and terrorists are becoming more daring and are inventing new ways of launching cyber attacks. More so, because every information or computer system is vulnerable to attack, cyber attack incidences keep increasing worldwide. It is important to note that not all attacks are launched by criminals or terrorists, sometimes, state actors may be involved in certain attacks. For example, governments may illegally collect classified information of other governments online.

Furthermore, the following potential and real cyber attack incidents will buttress the extent of cyber threats and vulnerabilities worldwide:

- In 1998, there was an organized attack by 300 Chinese hackers on Indonesia government sites to protest anti-Chinese riots in the country. Since then, there has been tens of thousands attempts to hack into major computer networks that belongs to defence, ministries, banks, the media etc. and these are occurring daily (O'Connell, 2012).

- In 2003, 21 power plants were attacked. This resulted in a loss of power in the United States and many parts of eastern Canada. The incident affected

several strategic sites such as Edwards's Air Force Base, which housed B-2 and B-1 bombers. The United States government found that the breakdowns were caused by the W32 Lovsan worm (Platt, 2011).

- At the beginning of 2011, Google announced that it and other companies had been targeted by a China-based cyber-attack, known as Aurora, though there was no prove that it had a direct government connection (Bulletin of the Atomic Scientists, 2011).

- In 2013, it was reported that in the United Kingdom, 93% of large corporations and 87% of small corporations have experienced security breaches in the past year. Seventy-eight percent (78%) of large organizations and 63% of small organizations were attacked by outsiders such as hacktivists (Department for Business, Innovation and Skills, as cited in Vashisth & Kumar, 2013).

- In 2015, Ukraine's power grid was attached by hackers who disabled control systems used to coordinate remote electrical substations. This plunged the capital and western parts of the country into power blackout for hours. The Security Service of Ukraine blamed the government of Russia for the cyber

attack. This accusation was eventually supported in malware analysis by a private computer security company (Kostyuk & Zhukov, 2017).

3.0 CONCLUSION

The internet and digital revolution has resulted in an unprecedented spike in threats and vulnerabilities in the cyberspace. Deviants, criminals and terrorists are exploiting the loopholes in information and system security to their advantage. There is therefore need for the threat and vulnerability levels of systems to be periodically assessed and appropriate measures taken to ensure that they are protected from potential cyber attacks.

4.0SUMMARY

The unit defined the concepts of cyberspace, threat and vulnerabilities. It specifically discussed cyberspace threats and vulnerabilities.

5.0 TUTOR-MARKED ASSIGNMENT

With good examples, explain the terms threat and vulnerability.

7.0 REFERENCES/FURTHER READING

Australian Computer Society (2016). Cybersecurity Threats, Challenges, Opportunities. Available at: file:///C:/Users/user/ Downloads/ACS_ Cybersecurity_Guide.pdf

Bulletin of the Atomic Scientists. Ronald Deibert: Tracking the emerging arm race in cyberspace, 67,1-8.

Cybersecurity Information Sharing Act of 2015 (CISA). United States of America.

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

Guitton, C. (2013). Cyber insecurity as a national threat: Overreaction from Germany, France and the UK? *Journal of European Security*, 22 (1), 21-35.

Information System Audit and Control Association (2017). Security Vulnerability Assessment.Available at: https://www.datasqlvisionary.com/wp-content/uploads/2018/06/Security-Vulnerability-Assessment.pdf

Jarman, J.A., & Yannakogeorgros, P. (2018). *The cyber threat and globalization: The Impact of U.S. National and International Security*. Lanham, Maryland: Rowman & Littlefield.

Kostyuk, N. & Zhukov, Y.M. (2017). Invisible digital front: Can cyber attack shape battlefield events? *Journal of Conflict Resolution*, 1-31.

Lessig, L. (1999). *Code and other laws of cyberspace*. New York: NY Basic Books.

Lin, H. (2012). A virtual necessity: Some modest steps towards greater cybersecurity. *Bulletin of the Atomic Scientists*, 88 (5) 75-87.

Meloy, R. & Hoffmann, J. (2013). *International handbook of threat assessment*. Oxford: Oxford University Press.

National Security Strategy (2019). Federal Republic of Nigeria.

O'Connell, M. E. (2012). Cyber security without cyber war. *Journal of Conflict an Security.Law*, 17 (2): 187 – 209.

Ortmeier, P.J. (2009). *Introduction to Security: Operations and Management* (3rd ed.). New Jersey: Pearson Education.

Platt, V. (2011). Still the fire-proof house?: An analysis of Canada's cyber security

strategy. *International Journal*, 12, 155-167.

Vashisth, A. & Kumar, A. (2013). Corporate espionage: The insider threat. *Business Information Review*, 30 (2) 83-90.

Zhao, J. & Zhao, S.Y. (2015). Security and vulnerability assessment of social media sites: An exploratory study. *Journal of Education for Business*, 90 (8) 458-466.

UNIT 2 THREATS TO CRITICAL INFRASTRUCTURES AND INDUSTRIAL CONTROL SYSTEMS

CONTENTS

1.0 INTRODUCTION

Critical infrastructures and industrial control systems are essential to the efficient operation of economic and social activities of a country. Today, these infrastructures and systems are increasingly been connected to the internet. Whereas this development has made them super-efficient, it has also made them susceptible to cyber attacks. Hence securing these important national and organizational assets has been a top priority for states and businesses around the world.

2.0 OBJECTIVE

This unit examines the extent of the threats posed to critical infrastructures and industrial control systems by the activities of cyber deviants, criminals and terrorists.

3.0MAIN CONTENT

3.1 Definition and Scope of Critical Infrastructure

Scholars have variously defined critical infrastructure. According to Alcaraz and Zeadallly (2015, p.1):

> A critical infrastructure (CI) consist a set of systems and assets, whether physical or virtual, so essential to the nation that any disruption of their services could have a serious impact on national security, economic well-being, public health or safety or any combination of these.

Section 58 of the Nigerian Cybercrime (Prohibition, Prevention etc.) Act, 2015 defines critical infrastructure as "systems and assets which are so vital to the country that the destruction of such systems and assets would have an impact on the security, national economic security, national public health and safety of the country".

What is clear in all the definitions you would see on Critical Infrastructure is that the assets are very crucial to the survival and sustenance the economic, security, health and wellbeing of the country. In fact, it could be considered an act of treason when an individual or group attacks the critical infrastructure of a country.

The European Programme for Critical Infrastructure Protection (EPCIP) (as cited in Alcaraz & Zeadallly, 2015, p.2) classified critical infrastructures as follows:

- Energy: energy production sources, storage and distribution (oil, gas, electricity).
- Information, Communication Technology (ICT): information system and network protection (e.g., the Internet); provision of fixed telecommunications; provision of mobile telecommunication; radio communication and navigation; satellite communication; broadcasting.
- Water: Provision of water (e.g., dams); control of quality; stemming and control of water quantity.
- Food and agriculture: Food provision, safety and security.
- Health care and public health: Medical and hospital care; medicines, serums, vaccines, and pharmaceuticals; bio-laboratories and bio-agents.
- Financial systems: banking, payment services and government financial assignment.
- Civil administration: government facilities and functions; armed forces; civil administration services; emergency services; postal and courier services.

- Public, legal order and safety: maintaining public and legal order, safety and security; administration of justice and detention.
- Transportation systems: road transport, rail transport, air traffic; border surveillance; inland waterways transport; ocean and short-sea shipping.
- Chemical industry: production and storage of dangerous substances; pipelines of dangerous goods.
- Nuclear industry: production and storage of nuclear substances.
- Space: Communication and research.
- Research facilities.

3.2 Definition and Scope of Industrial Control Systems (ICSs)

Apart from critical infrastructures (CIs), a wide array of industrial control systems (ICSs) are vulnerable to cyber attack. The vulnerability of ICSs to cyber attack is largely because they are connected to the internet. Therefore, it is important that these industrial control systems are defined. According to Ani, He and Tiwari (2017, p.33):

> ICs are essentially control systems, including supervisory control and data acquisition (SCADA), distributed control systems (DCS), process control systems (PCS), cyber-physical systems (CPS) or programmable

logic controllers (PLC) often found in the industrial sectors and critical infrastructures is typically used in industries such as electrical, water and waste water, oil and natural gas, chemical, transportation, pharmaceutical, pulp and paper, food and beverages, and manufacturing and used to manage industrial processes such as production, handling and distribution crucially control and monitor operations of industrial set ups; enabling functionalities like the use of control loop for sensor-measurement, hardware control for actuators (breakers, switches, monitors, etc.) human-machine interfacing remote diagnostics, and maintenance.

Furthermore, Lu, Guo, Li, Peng, Zang, Xie and Gao (2014) opined that industrial control systems are normally used in industries such as electrical, water and waste water, oil and natural gas, chemical, transportation, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing (e.g., automotive, aerospace, and durable goods). They observed that these control systems which are interconnected and mutually dependent are critical to the operations of those industries. They enumerated the commonest types of industrial control systems as follows:

- Supervisory Control and Data Acquisition (SCDA);

- Data Communication System (DCS) and ;
- Programmable Logic Controller (PLC).

Lu et al (2014) explained that SCADA is used to control dispersed assets that utilize centralized data acquisition and supervisory control. DCS helps to control production systems in a local area e.g. a factory using supervisory and regulatory control. PLC serves the purpose of discrete control for specific applications and provides regulatory control.

3.3 Threats to Critical Infrastructure

Critical infrastructures (CI) are always been targeted by cyber criminals and terrorists across the world. Losavio, Shut and Keeling (2011) pointed out that on March 29, 2009, GhostNet cyber espionage study and analysis report of the Information Warfare Monitor on distributed malware attacks from China. The attacks reportedly used a combination of Trojan Malware-Ghost Remote Access Tool and social engineering through email to infest machines that were vulnerable. They outlined the key findings as follows:

- Compromise of at least 1,295 computers in 103 countries, of which nearly 30 percent might be high-value targets,

- GhostNet penetration of sensitive computer systems of the Dalai Lama and other Tibetan targets, and
- GhostNet is a covert, difficult-to-detect system capable of taking full control of affected systems (p.131).

Losavio, Shut and Keeling (2011) further explained that the systems that were compromised included government offices of Iran, Bangladesh, Latvia, Indonesia, Philippines, Brunei, Barbados, Bhutan, and embassies of India, South Koreia, Indonesia, Romiania, Cyprus, Malta, Thailand, Taiwan, Portugal, Germany and Pakistan.

3.4 Threats to Industrial Control Systems

Arguably, the increasing dependence of industrial control systems on the internet makes them vulnerable to external attacks. These attacks can come from a wide range of sources such as random hackers, disgruntled ex-employees, competitors, organized criminal groups, terrorists groups and foreign state actors.

Industrial control systems (ICSs) have been severally been attacked over the years across the world. Lu et. al (2014, p.5) cited some of the ICS incidents below:

Date	Location	Detail
2013	South Korea and Japan	Icefog is a small yet energetic APT group, who maintain a foothold in corporate and governmental networks to smuggle out sensitive information.
2012	Global incident	Elderwood attack, spear phishing emails, watering hole, and zero-day exploits are always used.
2012	Middle East	Flame is being used for targeted cyber espionage in Middle Eastern countries.
2011	Global incident	Duqu virus was found, a complex attack tool specifically for critical infrastructure.
2011	U.S.	Hackers attacked the control systems of water supply facilities in Illinois.

2011	Japan	Hackers invaded the control and management system of Shinkansen in Japan.
2010	Global incident	Stuxnet virus was found. Iran is the most serious that the generation of its nuclear power plant was delayed.
2008	Poland	Juvenile attacked the suburban railway system in Lodz, Poland
2007	Canada	Attacker invaded one Canada'sWater SCADA control system and destroyed the control computer system.
2006	U.S.	Hackers invaded the systems of the sewage treatment plant in Harrisburg, Pennsylvania.
2005	U.S.	Zotob worm was found in the automobile corporate network and control network.
2003	U.S.	Teenager invaded the computer system of Houston

		Ferry.
2003	U.S.	Worm was found in the control network of Davis-Besse nuclear power plant.
2001	U.S.	Hacker invaded the control system of electricity transmission system in California.
2000	Russia	Hacker had controlled the largest natural gas pipeline network in the world on the part of Gazprom.
1997	U.S.	Teenage boy invaded (New York) NYNES system.
1994	U.S.	Hacker invaded the Salt River Project in Arizona.
1992	U.S.	Former employee of Chevron closed the emergency alarm systems located in 22 states.

Source: Lu et. al. (2014, p. 5).

As can be seen from the above table, industrial control systems have had their share of costly cyber attacks regardless on the side of globe that they are located. These incidents also underscore the earlier argument that attacks would usually come from a wide range of sources. Whether the source is curious juvenile or an organized criminal group, the fact remains that an attack on industrial control systems could be very costly to affected organizations.

4.0 CONCLUSION

Critical infrastructures such as electricity, transportation, oil and gas, emergency services, Information and communication technology and so on are critical to the smooth operation of the economy of a country. So also are industrial control systems. In today's digital world, these systems are connected to the internet and as such are vulnerable to cyber attack.

5.0 SUMMARY

The unit explained the concepts of critical infrastructures and industrial control systems and well as their scope. The level of threat that criminal and terrorist elements pose to these systems were also discussed.

6.0 TUTOR-MARKED ASSIGNMENT

Discuss the level of threat that criminals and terrorists pose to critical infrastructures and industrial control systems in Nigeria.

7.0 REFERENCES/FURTHER READING

Alcaraz, C. & Zeadallly, Z. (2015).Critical infrastructure protection: Requirements and challenges for the 21st century. *International Journal of Critical Infrastructure Protection*, 8, 1-34.

Ani, U.P.D., He, H.M., & Tiwari, A. (2017). Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective. *Journal of Cyber Security Technology*, 1 (1) 32-74.

Losavio, M.M., Shutt, J.E. & Keeling, D. W. (2011). The information polity: Social and legal framework for critical cyber infrastructure protection. . In T.Saadawi & L. Jordan (eds.) *Cyber infrastructure protection*. (pp. 129 - 158).Carlisle, PA: Strategic Studies Institute, U.S. Army War College.

Lu, T., Guo, X., Li, Y., Peng, Y., Zhang, X., Xie, F., & Gao, Y. (2014). Cyberphysical security for industrial control systems based on wireless senor networks. *International Journal of Distrusted Sensor Networks*, 1-17.

UNIT 3 THREATS OF TERRORISM AND TRANSNATIONAL ORGANIZED CRIME NETWORKS

CONTENTS

1.0 INTRODUCTION

Terrorism is a global security challenge that has endured for ages. From time immemorial to the present day, criminals have always crossed national borders. However, with the emergence of internet and digital technologies terrorists and criminals could cross and traverse national borders through technology. These have profound implications for crime and terror control in Nigeria and elsewhere.

2.0 OBJECTIVE

This unit focuses on the threat of terrorism and attributes of classical and cyber terrorism; cyber-enabled radicalization; cyber terrorist attacks and the various threats posed by transnational organized crime networks. At the end of this unit you will be able to understand how terrorists and transnational criminals are obsessed with the use of the internet and associated digital tools.

3.0 MAIN CONTENT

3.1 Threats of Terrorism and Attributes of Classical and Cyber Terrorism

Terrorist activities are more rapidly perpetrated with the development of the internet and digital technologies. Terrorism is a global security problem. It is criminalized in Nigeria by Terrorism Prevention (Amendment) Act, 2013.

However, cyber terrorism is expressly criminalized by Section 18 of the Cybercrime (Prohibition, Prevention Etc.) Act, 2015.

According to Jarman and Yannakogeorgos (2018, p.155-157) the scope of terrorists' misuse of the internet includes:

- **Cyber influence**: this entails the misuse of the internet to influence populations with propaganda. This may be done in order to raise sympathizers to the cause. This also includes the process of recruitment and radicalization through the internet.

- **Cyber planning**: this refers to the digital coordination of an integrated plan that cuts across geographical boundaries that may or may not cause bloodshed. This planning involves intelligence, surveillance and reconnaissance.

- **Real-time operational execution**: this has to do with the misuse of the internet to cause physical disruption. This goes beyond the hypothetical sphere of detonating improvised explosive devices through cellular technologies.

Ndubueze (2016, p. 6) explained the differences between classical terrorism and cyber terrorism in the table below:

Table 2. Attributes of Classical and Cyber Terrorism – A Comparative Snapshot

Attribute	Classical Terrorism	Cyber Terrorism
Motivation/Objective	Political, religious, social, national, ethnic, ideological and hegemonic.	Political, religious, social, national, ethnic, ideological and hegemonic [essentially the same motivation with classical terrorism].
Sphere	Physical, real world, offline, concrete space.	Cyber, virtual, online abstract space.
Primary Target	Humans, property, physical critical infrastructure	Computer systems/networks/computer mediated communication systems, internet architecture/internet of things, virtual critical

		infrastructure
Scope	Limited to a select and relatively small physical targets.	Massive, large scale virtual targets.
Territory	Select countries	Several countries
Execution Speed	Minutes/Hours	Seconds
Modus Operandi	Overt, physical contact with or close proximity to the target (s). Suicide bombing.	Covert, virtual contact with and unlikely close proximity with the target.
Tools	Fire-arms/ammunitions of all sorts, rocket launchers, IED's, grenades, armoured tanks, machine guns and so on.	Malwares of all sorts.

Nature of Warfare	Asymmetric, guerilla warfare	Asymmetric
Detection	Swift	Slow
Economic Loss	Huge	Exponentially massive and high
Investigation	Traditional, regular law enforcement / anti-terrorism personnel could be used.	Technical, requires highly trained/skilled and experienced law enforcement personnel including forensic experts, cyber criminologists and experts in international

Source: Ndubueze (2016, p 6).

There are several ways terrorist activities on the internet can constitute a threat to national governments and citizens across the world. One of those ways is through recruitment and radicalization of individuals.

3.2 Cyber-Enabled Recruitment and Radicalization

Today, terrorist organizations leverage on the internet and digital technologies to recruit and radicalize otherwise law abiding and oftentimes ordinary citizens. Such recruits having been fully radicalized will pursue and execute terrorist agendas and may go at any length to do so.

Jarman and Yannakogeorgos (2018, p.155) attempted to distinguish between cyber-enabled terrorists operations and operations in the cyberspace and operations in the cyberspace that produce physical effect akin to an armed attack as follows:

- Misuse of the internet for logistics of a terrorist network (including such activities as radicalization, recruitment, and financing).
- Cyber-enabled terrorist attacks as observed from improvised explosive devices to complex command and communications in the middle of an operation.
- The emergence of cyber warfare that is meant to intimidate or mobilize populations without a physical presence.

Scholars have decried the increasing sophistication of terrorist organizations and their link to organized crime networks. Howard and Traughber (2009, p. 365) captured the changing dynamics of terrorist organization in the followings words:

> As the global landscape in the twenty-first century has transformed via globalization, the nature of terrorists' organizations is also changing. Unlike terrorists groups of the past, which were primarily substate actors, today's terrorists are transnational groups operating on a global level. Encouraged by state weakness; globalization; increasing technological interconnectedness; and corrupt, permissive government officials, the "new terrorists" take advantage of an overall decline in international security. These factors have not only pawned new generation of terrorists but have also encouraged a similar increase in transnational crime.

The argument in the above quotation that terrorism is encouraged by state weakness is shared by George (2018) when he observed that in failed states terrorist organizations can mobilize young people who feel socially and economically marginalized to become part of a global terrorist movement. It has

been acknowledged that the internet can increase vulnerability to extremism (Beadle, 2017). Radicalization is said to be complete when an individual that has been influenced leaves the realm of option for that of actively supporting a specific terrorist act, or materially facilitating it (Jarman and Yannakogeorgos , 2018).

3.3 Cyber Terrorist Attacks

Apart from using the internet for the purposes of recruitment and radicalization and explained in the preceding section, terrorists use the internet either to facilitate their operations or attack critical national infrastructure and industrial control systems. This is usually done with the intent to embarrass the government and create fears in the minds of the general public.

Alqahtani (2014, p. 138) defined cyber terrorism as "the intentional use of subversive activities, or the threat thereof, against computers and networks related to critical infrastructure and vital services, with the intention to cause massive physical and psychological harm, for any objective whatsoever". Gross, Canetti and Vashdi (2017) compared conventional terrorism to cyberterrorism. They argued that unlike conventional terrorism, cyberterrorism uses malicious computer technology and not kinetic force. However, the observed both conventional terrorism and cyberterrorism share the same objective of quest to further political,

religious or ideological goals by inflicting physical or psychological harm to civilians.

Why do terrorist organizations increasingly use the internet infrastructure? This is question is aptly answered by Bogdanoski and Petreskp (2013, p. 60) thus:

> Considering the fact the terrorists have limited funds, cyber attacks are increasingly attractive, because, their implementation requires a smaller number of people and certainly smaller funds. Another advantage of cyber attacks is that they allow terrorists to remain unknown, because they can be very far from the place where the act of terrorism is committed. Unlike the terrorists that place their camps in countries with weak governance, cyber terrorists can store anywhere and remain anonymous.

3.4 Threat of Transnational Organized Crime Networks

According to Dijk and Spapens (2014) the main distinguishing characteristics of transnational organized crime is that part of their criminal business processes are completed in different countries. The United Nations Office on Drug and Crime (as cited in Dijk and Spapens, 2014, p.214) in 2002, conducted a study using a sample

of 40 countries, which included the United States, Russia and Africa. The study came up with the following typology of networks:

i. **The criminal network**: this is defined by the activities of key members; provenience in the network is a function of position and skills, personal loyalties is essential, coalescence around criminal projects, low public profile, network reforms after exit of key individuals. Examples of groups included in this sample were a Dutch network of drug smugglers and a Nigerian network involved in different types of crime.

ii. **The standard rigid hierarchy**: this is made up of single leader, clearly defined hierarchy, strong system of internal discipline, usually strong social or ethnic identity, violence is essential to activities, influence or control over defined territories. Examples of group under this category are from Italy, China, Columbia and Eastern Europe.

iii. **The regional hierarchy**: this comprise of single leadership structure, line of command from centre, degree of autonomy at regional level, geography/regional distribution, multiple activities, usually strong social or ethnic identity, violence essential to activities. Typical examples include the outlawed motorcycle gangs such as the Hells Angels with branches in different countries.

iv. **The clustered hierarchy**: this include a number of criminal groups, governing arrangements for the groups present, cluster has stronger identity than the constituent groups, degree autonomy for constituent groups, formation strongly linked to social/historical context, relatively rare. Example is the "28s prison gang" of South Africa.

v. **The core group**: this category is surrounded by loosed network, limited number of individuals, tightly organized flats structure, small size maintains internal discipline, rarely has social or ethnic identity. Example include a Dutch group involved in human trafficking.

Furthermore, the UNODC study revealed that most groups engage in trans-border operations. Also, it found that of the group, 70 percent were involved in criminal activities in three or more different countries, while many operated in five or more countries. It also found that most engaged in multiple criminal activities. Moreover, of the 40 groups studied, 30 used corruption and 33 routinely used violence. Also, of the 40 groups, 30 showed evidence of the investment of profits from illegitimate activities in legitimate business activity.

Transnational crime is linked to terrorism in various ways. Rollins and Wyler (as cited in Crank & Jacoby, 2015, p.256) explains this connection in the following three ways.

i.) **Expand skill base**: Through partnerships both can enhance their strengths. Through specialized skills their functionality and success rate can be improved. This kind of partnership for resource expansion may eventually result to a situation whereby the terrorist organization depends on the criminal transactions, which increases the vulnerabilities that international security agents can take advantage of.

ii.) **Shared tactics:** Notwithstanding the ideological difference between transnational organized criminal organizations and terrorist organizations, their operational tactics are usually the same. Some of such tactics are use of violence, profit-oriented criminal activity, money laundering, stealth during border crossing, illegal weapon acquisition, and the corruption of public officials. Therefore, they can mutually reinforce their tactics.

iii.) **Organizational evolution**: Whereas criminal groups may evolve politically; political terrorist groups may be inclined to becoming criminal for-profit enterprises.

Dijk and Spapens (2014) argued that globalization and revolution in information and communication technology among others has provided unprecedented opportunities for transnational organized crime. Indeed

transnational organized criminal networks are using the internet to facilitate the operations of their criminal enterprise. This strategy is obviously cheaper, faster, less risky and perhaps more profitable.

4.0 CONCLUSION

Terrorist organizations and transnational organized crime networks are growing in scope and sophistication. This is largely because like legitimate organizations and businesses they are leveraging of the numerous opportunities that internet and digital technologies creates. Terrorists and transnational criminals therefore constitute a growing threat to countries around the world in the digital age.

5.0 SUMMARY

The unit discussed the threats posed by the clandestine online activities of terrorists and transnational organized crime networks as well as how the cyberspace facilitates radicalization of ordinary citizens.

6.0 TUTOR-MARKED ASSIGNMENT

Discuss how the online activities of terrorists and transnational criminals constitute a threat to cyber security in Nigeria.

7.0 REFERENCES/FURTHER READING

Alqahtani, A. (2014). Awareness of the potential threats of cyberterrorism to the national security. *Journal of Information Security*, 5, 137-146.

Beadle, S. (2017). *How does the internet facilitate radicalization?* London: War Studies department, Kings College.

Bogdanoski, M. & Petreski, D. (2013) *Cyber Terrorism– Global Security Threat.* Contemporary Macedonian Defense. *International Scientific Defense, Security and Peace Journal*, 13 (24). pp. 59-73.

Crank, J.P., & Jacoby, L.S. (2015). *Crime, violence and global warming*. London: Routledge: Taylor and Francis Group.

Cybercrime (Prohibition, Prevention Etc.) Act, 2015

Dijk, J.v., & Spapens, T. (2014). Transational organized crime networks. In P. Reichel & J. Albanese (eds). *Handbook of Transnational Crime and Justice* (2nd ed.). pp. 213-226). Los Angeles: SAGE Publications.

George, J. (2018). State failure and transnational terrorism: an empirical analysis. *Journal of Conflict Resolution*, 62 (3) 471-495.

Gross, M.l., Canetti, D., & Vashdi, D.R. (2017). Cyberterrorism: its effects on phychological well-being, public confidence and political attitudes. *Journal of Cyberseucity*, 3 (1), 49-58.

Howard, R.D. & Traughber, C.M. (2009). The "New Silk Road" of terrorism and organized crime: The key to countering terror-crime nexus. . In J..H. Norwitz (ed.). *Pirates, Terrorists, and Warlords: The History, Influence, and Future of Armed Groups around the World*. (pp.368-384).New York: Skyhorse Publishing.

Jarman, J.A., & Yannakogeorgros, P. (2018). *The cyber threat and globalization: The Impact of U.S. National and International Security*. Lanham, Maryland: Rowman & Littlefield.

Ndubueze, P.N. (2016). Policing Cyber Terrorism in Africa: Perspectives,

Problems and Prospects. In J. Ingram (ed.). *Policing Strategies, Management and Potential Risks*. (pp. 59-84).New York: Nova Publishers.

Terrorism Prevention (Amendment) Act, 2013

UNIT 4 FIVE-LEVEL PROBLEM SOLVING STRATEGY FOR THREAT AND VULNERABILITY

CONTENTS

1.0 INTRODUCTION

Threats and vulnerabilities have become common features of cyber-physical systems. Critical infrastructures and industrial control systems are often exposed to threats and vulnerabilities. The National Strategy to Secure Cyberspace (n.d.) proposed a five-level problem solving strategy for controlling threats and vulnerabilities in the cyberspace.

2.0 OBJECTIVE

This unit discusses the five-level problem solving strategy for the management and control of threats and vulnerabilities in the in the cyberspace. At the end of the unit you will learn how individual home users of the internet/small businesses, large enterprises, critical infrastructure, nation-states and the globe are exposed to cyber attacks.

3.1 Level 1: the Home User/Small Business

The computers that are used by people at home can become part of networks of remotely controlled machines that can be used to attack critical infrastructures. Home and small business computers without defense mechanisms, particularly those using digital subscriber line (DSL) or cable connections, are vulnerable to attackers who can use those machines without the owner's knowledge. Groups of

such “zombie” machines can then be used by third-party actors to launch denial-of-service (DoS) attacks on key Internet nodes and other important enterprises or critical infrastructures. Hence, home personal computers needs to be adequately defended from intrusion.

3.2 Level 2: Large Enterprises

Large-scale enterprises such as corporations, government agencies, and universities etc. are common targets for cyber attacks. Many such enterprises are part of critical infrastructures. Enterprises require clearly articulated, active information security policies and programmes to audit compliance with cybersecurity best practices. The U.S. intelligence community warns that American networks will be increasingly targeted by malicious actors both for the data and the power they possess.

3.3 Level 3: Critical Sectors/Infrastructures

The collaboration of organizations in sectors of the economy, government, or academia to address common cybersecurity problems, will reduce the burden on individual enterprises. Such partnerships often produces shared institutions and mechanisms, which may have cyber vulnerabilities whose exploitation could directly affect the operations of member enterprises and the sector as a whole.

Enterprises can also reduce cyber risks by participating in groups that develop best practices, evaluate technological offerings, certify products and services, and share information. Several sectors have formed Information Sharing and Analysis Centers (ISACs) to monitor for cyber attacks directed against their respective infrastructures. ISACs also share information about attack trends, vulnerabilities, and best practices.

3.4 Level 4: National Issues and Vulnerabilities

There are cybersecurity problems with national implications which cannot be solved by individual enterprises or infrastructure sectors alone. Since all sectors share the Internet, they are therefore all at risk if its mechanisms (e.g., protocols and routers) are not secure. Weaknesses in widely used software and hardware products can also create problems at the national level. This would require coordinated activities for the research and development of improved technologies. More so, the lack of trained and certified cybersecurity professionals deserves national level attention.

3.5 Level 5: Global

The worldwide web is a planetary information grid of systems. Internationally shared standards enable interoperability among the world's computer systems. This

interconnectedness therefore implies that problems on one continent may affect computers on another. Hence, the need for international cooperation to share information related to cyber issues and, the prosecution of cyber criminals. Without such cooperation, the efforts to collectively detect, deter, and mitigate the effects of cyber-based attacks would be hampered.

4.0 CONCLUSION

The threat to and vulnerabilities of cyber security affects each country across all the levels of the internet usage value-chain. Individual internet users, corporations, nation-states and the globe are affected one way or the other by the threat of cyber attacks. Therefore, the response to the challenges of cyber security needs to be a collaborative one that will include all stakeholders for it to be productive.

5.0 SUMMARY

The unit covered the five-level problem solving strategy for threat and vulnerability. The strategy cut across the individual home users of the internet/small businesses, large enterprises, critical infrastructure, nation-states and the globe,

6.0 TUTOR-MARKED ASSIGNMENT

Discuss the five-level problem solving strategies for the management and control of threats in the cyberspace.

7.0 REFERENCES/FURTHER READING

The National Strategy to Secure Cyberspace (n.d). Available at:

http://www.iwar.org.uk/cip/resources/pcipb/case_for_action.pdf

Module 5: Cybercrime Offending, Victimization and Prevention Strategies

Unit 1: Profiling Cybercrime Offenders

Unit 2: Types and Patterns of Cyber Victimization

Unit 3: Cybercrime Victimization Risk Factors

Unit 4: Cybercrime Preventive Strategies

UNIT 1 PROFILING CYBER OFFENDERS

CONTENTS

1.0 INTRODUCTION

Criminal profiling also called offender profiling has been used by law enforcement agencies for ages across the world and has remained a useful strategy in criminal investigation. However, some advances have been made in the use of criminal profiling in the digital age.

2.0 OBJECTIVE

This unit covers the following topics: meaning, history and types of criminal profiling; developing a digital criminal profiling; age of criminal responsibility for cybercrime offenders and; digital forensic criminal profiling models and practices in the cyberspace.

3.0 MAIN CONTENT

3.1 Meaning, History and Types of Criminal Profiling

a) Meaning of Criminal Profiling

Criminal profiling is also variously referred to as "offender profiling", "psychological profiling", "behavioural profiling" and "criminal personality profiling "in the literature. According to Turvey (2002, p.1) criminal profiling refers to "the process of inferring the personality characteristics of individuals responsible for committing criminal acts". He listed the professionals that have been typically engaged in the practice of criminal profiling to include: investigators, behavioural scientists, social scientists, and forensic scientists. Kipane (2019) argued that criminal profiling entails making inferences about the physical, habitual, emotional, psychological, and vocation features of criminals.

b) History of Criminal Profiling

Kipane (2019) have traced the history of criminal profiling to the 15th century, but also noted that some account believed that the method was used as far back as 1880 to predict about a serial killer. He further explained that although experts have debated its effectiveness, criminal profiling has been deployed successfully by law enforcement for over a century. It was also successfully applied at the end

of the 20th century and in the 21st century by law enforcement authorities to identify offenders. Kipane explained that the term "offender profiling" was introduced in the 1970s, and that it was linked to the activities of the Federal Bureau of Investigation (FBI) analysis unit in the United States who used it to describe their criminal investigative analysis work. He observed that criminal profiling at first was used for serial murders, but that the scope of research expanded with time to now include various criminal offences such as rape, murder, terrorism, cybercrime and so on.

b) Types of Criminal Profiling

There are two types of criminal profiling, they include: inductive criminal profiling and deductive criminal profiling (Turvey, 2002).

(i) Inductive criminal profiling: this method of criminal profiling is based on the premise that similarities in crime committed by different offenders will suggest the existence of common personality traits among the offenders. Information for this method of profiling can be collected from record of past crimes, past known offenders and open sources such as the media.

(ii) Deductive criminal profiling: The deductive criminal profiling method uses the evidence found at the crime scene to reconstruct the crime scene. The idea being to develop a mental picture of the characteristics of the offender.

Although criminal profiling is not an exact science, it can offer useful leads that can help in investigators to solve the riddles of crime.

3.2 Developing a Digital Criminal Profiling

Kipane (2019) described five elements of a cyber criminal profile as follows:

i) **Personality characteristics/traits**: These are specific to an individual, and may predispose the individual to commit a cybercrime: Cybercriminals are believed to have a high level of legal nihilism. He argued that a cybercriminal has deviations in legal consciousness; which is exemplified by the inability to conform to legal norms. This he said is related to the enhanced pressure to risk the violation of law in order to realize some personal material gain. He also recognized the impact of the micro environment such as the family negatively affecting the individual's personality formation and by implication enhancing the possible drift to cybercrime.

ii.) **Criminal professionalism:** This has been defined as the personality traits that facilitate the safe and effective execution of cybercrime. He noted that it comprise of four features: namely: personal qualities; knowledge and skills; fearlessness, courage and self-confidence; effectiveness and viability of action; commission of a criminal offence and achieving a specific goal. He explained that for example, some financially motivated cybercriminals may have two main goals, i.e. to input data and user identity in order to gain access to finances through the identity they have acquired.

iii.) **Technical knowledge and technical skills** in dealing with complex programs and devices that enable cybercrime**:** A study has shown that technical execution of majority of illegal activities is relatively simple. He observed that most cybercriminals are university students or students of other educational institutions. Since it is generally recognized that the level of education among cybercriminals may be higher than among other categories of criminals, the use of such skills in the commission of cybercrime will result in progressive increase in its prevalence.

iv.) **Social characteristics**: These have been defined to include demographic features, socio-economic status, socio-psychological and moral qualities. The basic elements are gender, age, nationality, socio-economic status. He argued that the features of a typical fraudster are: a middle aged, man with higher education and substantial work experience in his company (almost half had six or more years of experience, almost a third – three to five years of experience). This fourth assumption is debatable when viewed within the context of the Nigerian society where empirical evidence suggest that online fraudsters and usually undergraduate students.

v.) **Characteristics of motivation:** He argued that motives are developed under the influence of human emotions and feelings. The motives are internal - chosen by the person and external – driven by others. He noted that research has demonstrated that human behaviour is driven by a number of motives – different internal and external factors and that motive is the leading and facilitating function of the activity (internal psychic encouragement), which, when creating the subject of the activity, directs the human activity. He argued that cybercriminals can be of any

gender, age, economic status, race, religion or nationality and can be driven by different motives.

3.3 Profiling Hackers

a) Definition of Hackers

Hackers are basically individuals who gain unauthorized access to a computer system usually for the purpose of carrying out an illegal activity. There are several ways hackers can illegally gain access to a computer system.

b.) Motivation of Hackers

Hackers are driven by a wide range of different motives. Marcum (2014, p.116-118) categories hackers' motivations as follows:

i. **Addiction**: Hackers are driven by addiction just like other addictive behaviours like tobacco smoking and alcoholism. An individual after a continued engagement in hacking activities can become addicted to it. The penchant for hacking can result from the sense of power hackers feel when they gain access to hidden computer files and perhaps the knowledge they acquired through that access. In a bid to keep updating

that knowledge they may continue the activity and this would eventually lead to addiction.

ii. **Curiosity**: Hackers are curious about learning about as much information as they can often using illegal methods. Network systems are usually improved through exploration. Such exploration may involve some trial and error. Therefore, hackers may want to explore and understand how operating system of computers works or how a security code can be cracked. The intent being to satisfy their curiosity.

iii. **Excitement and Entertainment**: Hackers are perceived as highly intelligent persons who possess little or no social skills in the physical world. Many hackers have reportedly claimed that they find their lives online more exciting than that of work or home. Therefore, some hackers crack systems and code just to entertain and excite themselves. This category of hackers does not intent to cause extensive damage to their targets.

iv. **Money**: Hackers are also motivated by monetary issues. This financial greed can be expressed in two ways: a) for personal gain and, b) to prevent large corporation from making financial gains. When hacking started there was an ethic among hackers community that prohibited

members from accumulating wealth illegally through hacking. This is no longer the case today as many hackers engage in financial fraud schemes by blackmailing others or stealing credit cards.

v. **Power, Status and Ego**: Hackers are portrayed in the media as highly intelligent beings who can crack the toughest government security codes. This kind of glamorization attracts some people who are not popular in any way. Also in the hacking world, power and ego is gained through a demonstration that a person is having the upper hand on knowledge and skills about hacking.

vi. **Ideologies**: There are several factors that can influence the formation of ideology. These factors may include: cultural norms, political preferences, social pressure and so on. Ideologies can influence behaviour including those of hackers. Hackers can obtain political and religious information from the internet that could change their belief on certain topics. Hackers support the social movement on freedom of information by the general public.

vii. **Peer Recognition**: Hackers are often perceived as social-misfits and unpopular. They feel more at home online where there is usually no face-to-face interaction with others. Therefore hackers form social

communities with online friends and seek acceptance and recognition from them. This can be achieved by demonstrating their high level of knowledge and skills in the hacking world. This kind of feat often endears them to their peers.

viii. **Revenge:** Revenge is the most malicious motivation for hackers. The hacker can perform an act as a payback for an actual or perceived wrong done the hacker. Revenge motivated attacks are effective if the attacked person or organization does not possess enough skill to counteract the attack or promptly prevent it. A naïve victim may not be aware of the attack or be able to prevent it before extensive damage is done.

c) Methods of Hackers

i. **Brute-force attack**: This method involves the guessing of the password of a system in order to gain access to it. The hacker utilizes knowledge of the victim which may include victim's favourite food, sports, best friend's name and so on.

ii. **Shoulder surfing**: This method entails the hacker watching the victim use a pin number during a transaction. Such transactions may take place

in an automated teller machine point (ATM), supermarkets or petrol stations and so on where point of sale (POS) machines are used.

iii. **Social engineering**: This method entails the hacker posing as a professional or a colleague from another unit or department in order to obtain information about the victim's computer system.

3.4 Profiling Identify Thieves

a) Definition of Identity Theft

Identity theft refers to the stealing and use of the personal information of another person without the person's consent for fraudulent purposes. Identity theft existed before the emergence of the internet. In the pre-internet era, identity thieves criminally and discretely obtained other people's personal information, for example from their drivers' license or work identify card in order to impersonate them. Today, however, with the breakthrough in information and communication technology (ICT), the proliferation of digital devices and relatively easy access to high-speed internet connection, identity theft has become easier to perpetrate albeit, online and difficult to detect. Identify thieves have now grown in sophistication as they employ the internet and ICT knowledge and skills to carry out their nefarious activities online.

b.) Motivation of Identity Thieves

Like Hackers, identity thieves are propelled by different kinds of motives. McNally (2012, p. 11-14) explained these movies using the acronym "MGEARS", which means motivational gears as follows:

i. **Money:** Money is of essence in the world of identity thieves. Unlike earlier when it was mainly in paper form, money today can be in plastic, digital or virtual form when it is in the form of credit that can be borrowed when it is not yet earned by the identity's owner. The security of money in all its forms and location is usually a priority to most people. Nevertheless, people's identities are stolen to enable the thief steal their monies.

ii. **Goods**: Money is desirable and can buy almost everything. An offender that has an identity that can be used as cash, the offender will be able to directly purchase the goods he or she desires. These may include basic necessities of life such as food, clothing and shelter or the available pleasures and luxuries of life such as jewelry, cars and travel.

iii. **Employment**: Some identity thieves just want to obtain employment, because for certain reasons they are unable to work under their real names. For example, an identify thief may steal the educational and birth certificates of a person and use same to obtain job.

iv. **Anonymity**: There is a universal desire for anonymity among offenders as it is believed that it decreases the likelihood of their apprehension. Also, an offender may have certain motive for hiding his or her true identity. The offender will then hide behind the identity of someone else. These categories of identity thieves provide false identity information to authorities such as the police on demand.

v. **Revenge**: Identity thieves may target the owner of a particular identity or any other party that can be affected by their activities using someone else's identity for the purpose of revenge.

vi. **Service**: A service refers to any act that can be carried out for money such as healthcare; care repairs; travel by plane, train, taxi etc. or any other social benefit that can be assessed by one's identity such as public assistance, voting right and community memberships. An identity thief may steal a victim's identity just to enjoy a service that is due the victim.

c) Methods of Identity Thieves

According to Tajpour, Ibrahim and Zamani (2013, pp. 52-54) identity thieves employ the following methods to carry out their fraudulent activites:

i. **Dumpster diving:** Looking through a person's garbage for "pre-approved" credit card offers, copies of old bills, loan applications, and documents with the resident's Social Security Number.

ii. **Shoulder surfing:** Overhearing a person give out personal information over a public telephone or cell phone, or looking over a person's shoulder as they use an ATM or fill out forms. To bribe employees to hand over personal customer information, and physically stealing confidential files or computer hard drives in which identity information is stored.

iii. **Skimming:** Attaching a data storage device to an ATM machine or a retail checkout terminal and reading the credit card or PIN numbers that pass through the device.

iv. **Publicly available information:** A search of public and government databases can yield information about driver's licenses, real estate and other

business transactions, vehicle records, certain types of professional certifications, and licensing records. Newspaper classifieds and other private databases also provide a wealth of information.

v. **Mail theft:** Stealing pre-approved credit card applications, insurance statements, tax information, or investment reports from mailboxes.

vi. **Changing your address:** Diverting victim's billing statements to another location by completing a change of address form.

vii. **Old-fashioned stealing:** Stealing wallets and purses; mail, including bank and credit card statements; pre-approved credit offers; and new checks or tax information. Offenders steal personnel records or bribe employees who have access.

viii. **Retail theft:** Stealing files or getting information from partner at retailers or service providers' offices.

ix. **Pharming or Trojan-horse:** E-mails and their related websites have viruses attached. These viruses contain programmes that record keystrokes and obtain crucial information.

x. **Spoofing:** Sending a message to a computer from a source that pretends the message is coming from a trusted computer's IP address. The spoofer could pose as an Internet Service Provider or even an "identity theft prevention" service provider.

xi. **Botnets:** A hacker can control a PC or a network of PCs from a remote location after inserting a control program into an unsuspecting user's computer.

xii. **SQL Injection Attacks:** Personally identifiable information can be read and modified by SQL Injection Attack as one of the most serious threats to the security of database driven application.

xiii. **Social engineering:** in the context of security, is understood to mean the art of manipulating people into performing actions or divulging confidential information. This is a type of confidence trick for the purpose of information gathering, fraud, or computer system access. All social engineering techniques are based on specific attributes of human decision making and are exploited in various combinations to create attack techniques such as:

xiv. **Pretexting:** Creating and using an invented scenario (the pretext) to engage a targeted victim in a manner that increases the chance the victim will divulge information or perform actions that would be unlikely in ordinary circumstances. It can be used to fool a business into disclosing customer information as well as by private investigators to obtain telephone records, utility records, banking records and other information directly from company service representatives. The information can then be used to

establish even greater legitimacy under tougher questioning with a manager, e.g., to make account changes, get specific balances, etc.

xv. **Phishing:** Sending an email message to a targeted individual, asking them to individual to access a web site that mimics a trusted institution and then reveal private identity information. E-mails are sent to unsuspecting victims, asking for information and providing links to false websites.

xvi. **Wi-phishing:** Consumers sometimes unwittingly use wireless networks set up by fraud. This makes it easy for cybercriminals to steal passwords and other information.

xvii. **Vishing:** This technique is called Vishing as it uses both voice and phishing to conduct the attack. The criminals will call, usually with a recorded message, instructing you to call a number and leave bank account or credit card information or the victim receives a typical e-mail, like any other traditional phishing scam. They are then asked to provide information over the phone instead of being directed to an Internet site.

xviii. **Smishing:** This attack manipulates mobile phone operators/carriers' SMS by sending text messages to mobile users trying to trick them into following a malicious mobile Internet link. These types of phishing traps are commonly known as Smishing. Texting has become very popular on cell phones and smartphones. Criminals are taking advantage of SMS technology by sending

a message asking for private bank or credit account information. The message might indicate that your immediate attention is required or your accounts will be closed. The criminal might provide a website address to visit or a phone number to call.

xix. **Typo Squatting:** They are websites with names similar to legitimate websites. When people make typing errors, they land on these false websites. This gives cyber-criminals the opportunity to infect computers or to insert "bots" into them. It is a new way of phishing.

The above methods of identity theft have wide range of complexity, from simple method such as stealing bags and shoulder surfing to complex methods such as internet phishing and skimming. So they can be considered as:

xx. **Low Tech Methods:** Criminals engaging in identity-based offenses can obtain personal information through low tech methods, such as stealing personal information from mailboxes or during the commission of a robbery or burglary.

xxi. **High Tech Methods:** Offenders may also use high tech methods via computers and/or the Internet to obtain personal information that is seemingly unprotected by the victim.

5.0 CONCLUSION

Criminals profiling is one of the veritable tools used by investigators to determine the likely personality characteristics of a criminal offenders. Although it is argued that the process is not scientific, it has proven to be used in criminal investigation overtime. To minimize the error margin it is expected that investigative officers use it in line with the global best practices. There seems to be an upsurge in the activities of hackers and identity thieves in the digital age.

6.0 SUMMARY

The unit focused on: the meaning, history and types of criminal profiling; developing a digital criminal profiling, profiling hackers and profiling identity thieves. It order to explain the personal characteristics of hackers and identity thieves, it specifically discussed their motives and methods.

7.0 TUTOR-MARKED ASSIGNMENT

What are the motives that drive hacking victimization?

8.0 REFERENCES/FURTHER READING

Kipane, A. (2019). Meaning of profiling cybercriminals in the security context. SHS Web of Conference, 68, 01009, 1-15. https://doi.org/10.1051/shsconf/20196801009

Marcum, C.D. (2014). *Cyber Crime*. New York: Walters Kluwer, Law and Business.

McNally, M. (2012). *Identity theft in today's world*. Santa Barbara, California: Praeger.

Tajpour, A., Ibrahim, S. & Zamani, M. (2013). Identity theft methods and fraud types. *International Journal of Information Processing and Management*, 4 (7) 51-56.

Turvey, B. E. (2002). A history of criminal profiling. In B.Turver (ed.*).* *Criminal Profiling: An Introduction to Behavioural Evidence Analysis* (2nd ed.). Amsterdam: Elsevier Academic Press.

UNIT 3 TYPES AND PATTERNS OF CYBERCRIME VICTIMIZATION

CONTENTS

1.0 INTRODUCTION

Crime victims generally refer to persons who suffered harm, whether physical, financial or psychological as a result of criminal activities. Like conventional crime victims, victims of cybercrime experience some physical, financial or psychological harm resulting from their victimization. There may exist some commonalities between the victims and offenders of cybercrime.

2.0 OBJECTIVE

This unit covers the following topics: definition of cybercrime victims, types of cybercrime victims, patterns of cybercrime victims, and the victim-offender overlap in cybercrime.

3.0 MAIN CONTENT

3.1 Definition of Cybercrime Victims

Cybercrime victims are individuals, communities, organizations or governments who suffer some kind of physical, financial or psychological harm as a result of the activities of cyber criminals. Cybercrime is driven by a wide range of different motives, hence cyber criminals may target an individual, a corporate organization, a community or the government depending on what their goal is. Arguably, a

successful cyber attack will result in a loss or harm which is suffered by the victim. Sometimes the loss could be purely monetary such as in advance fee fraud scheme or it may be psychological such as in the case of cyberstalking.

3.2 Types of Cybercrime Victimization

According to Angkasa (2018, p.3) cybercrime victims fall under four broad categories as follows:

i. **Individual Victims:** This refers to individuals who are directly affected by the activities of cybercriminals. For example, an individual can be defrauded through online purchasing. Also, an individual can be defrauded by online advance fee fraudsters through romance scam.

ii. **Corporate Victims:** Public and private corporations in various fields are also targeted by cyber criminals. Corporations across the world have fallen victim of various kinds of cybercrime such as business email scam, corporate data breach, ransomware etc.

iii. **Community Victims:** There as some cybercrimes that may be targeted at communities. This can take the form of hoaxes and

provocative reporting aimed at causing anxiety and hostility in a community. This can be orchestrated for political purposes.

iv. **Government Victims:** Governments have also been targeted by cyber criminals. For example. Cyber criminals may deface a government website or may attack a government computer system with ransomware.

3.3 Patterns of Cybercrime Victimization

The Federal Bureau of Investigation (FBI) Internet Crime Complaint Centre (IC3) (2019) Internet Crime Report provides useful insights into the patterns of cybercrime victimization. The IC3 report is released annually. The report indicates that in 2019, IC3 received a total of 467,361 complaints with reported losses exceeding $3.5 billion. The types of cybercrime that were mostly reported were: phishing/vishing/smishing/pharming, non-payment/non-delivery, extortion, and personal data breach. The top three cybercrimes with the highest reported cases were: business email compromise, confidential/romance fraud, and spoofing.

The IC3 report shows the 2019 victims of cybercrime by in the following table:

Victims

Age Range	Total Count	Total Loss
Under 20	10,724	$421,169,232
20 - 29	44,496	$174,673,470
30 - 39	52,820	$332,208,189
40 - 49	51,864	$529,231,267
50 - 59	50,608	$589,624,844
Over 60	68,013	$835,164,766

Source: IC3 (2019) Internet Crime Report

N.B. Not all complaints included an associated age range – those with this information are excluded from the table.

The above table suggests that elderly people are more likely to fall victim of cybercrime. This is understandable for various reasons. First elderly people, unlike

young adults are less likely to be familiar with the workings of the internet and how to navigate their way around the online environment. Second, in view of the first reason, they may rely on the assistance of third parties who would most likely will be younger for their online transactions. This may further expose them to online victimization as such third parties may take undue advantage of them.

Moreover, the IC3 (2019) Internet Crime Report provided the list of 2019 To 20 International Victim Countries (excluding United States) as follows:

i. United Kingdom - 93,796

ii. Canada - 3,721

iii. India - 2,901

iv. Australia - 1,298

v. France - 1,243

vi. Belgium - 1,031

vii. Germany - 850

viii. Brazil - 628

ix. Mexico - 605

x. Argentina - 578

xi. Philippines - 561

xii. Hong Kong - 535

xiii. South Africa - 465

xiv. Georgia - 454

xv. Switzerland - 438

xvi. Italy - 428

xvii. China - 403

xviii. Malaysia - 362

xix. Spain - 35a

xx. Russian Federation - 349

The above data indicates that only one African country (South Africa) ranked among the top 20 international victim countries of cybercrime. This is perhaps because compared to other continents of the world Africa is lagging behind in the development of digital infrastructure. Internet penetration is also relatively low in Africa. Given that online transactions are powered by the internet infrastructure,

the user population will obviously be higher in countries with this infrastructure. However, Ndubueze (2019) observed that with the 36.1% internet penetration rate in Africa in 2018, which represents 11.10% of the world population of internet users the gap created by the digital divide is speedily closing up.

Victim count by crime type from the IC3 report (2019) is shown below:

By Victim Count

Crime Type	**Victims**	**Crime Type**	**Victims**
Phishing/Vishing/ Smishing/Pharming	114,702	Lottery/Sweepstakes/Inheritance	7,767
Non-Payment/Non-Delivery	61,832	Misrepresentation	5,975
Extortion	43,101	Investment	3,999
Personal Data	38,218	IPR/Copyright	3,892

Breach		and Counterfeit	
Spoofing	25,789	Malware/Scareware/Virus	2,373
BEC/EAC	23,775	Ransomware	2,047
Confidence Fraud/Romance	19,473	Corporate Data Breach	1,795
Identity Theft	16,053	Denial of Service/TDoS	1,353
Harassment/Threats of Violence	15,502	Crimes Against Children	1,312
Overpayment	15,395	Re-shipping	929
Advanced Fee	14,607	Civil Matter	908
Employment	14,493	Health Care	657

		Related	
Credit Card Fraud	14,378	Charity	407
Government Impersonation	13,873	Gambling	262
Tech Support	13,633	Terrorism	61
Real Estate/Rental	11,677	Hacktivist	39
Other		10,842	

The above data indicates that victims of phising/vashing/smishing/pharming top the list of victim by count. The report defines phishing/vashing/smishing/pharming as “unsolicited email, text, messages, and telephone calls purportedly from legitimate company requesting personal, financial, and/or login credentials” (IC3 Report, 2019, p.27). This is not surprising as it does not require any technical informational and communication technology skill to execute. Besides, when people are busy with their daily business schedules they may be taken off-guard by these scammers.

The loss suffered by victims by crime type was also provided by the IC3 Report as follows:

By Victim Loss

Crime Type	**Loss**	**Crime Type**	**Loss**
BEC/EAC	$1,776,549,688	Employment	$42,618,705
Confidence Fraud/Romance	$475,014,032	Civil Matter	$20,242,867
Spoofing	$300,478,433	Harassment/Threats of Violence	$19,866,654
Investment	$222,186,195	Misrepresentation	$12,371,573
Real Estate/Rental	$221,365,911	IPR/Copyright and Counterfeit	$10,293,307
Non-Payment/Non-Delivery	$196,563,497	Ransomware	**$8,965,847

Identity Theft	$160,305,789	Denial of Service/TDoS	$7,598,198
Government Impersonation	$124,292,606	Charity	$2,214,383
Personal Data Breach	$120,102,501	Malware/Scareware/ Virus	$2,009,119
Credit Card Fraud	$111,491,163	Re-shipping	$1,772,692
Extortion	$107,498,956	Gambling	$1,458,118
Advanced Fee	$100,602,297	Health Care Related	$1,128,838
Other	$66,223,160	Crimes Against Children	$975,311

Phishing/Vishing/Smishing/Pharming	$57,836,379	Hacktivist	$129,000
Overpayment	$55,820,212	Terrorism	$49,589
Tech Support		$54,041,053	
Corporate Data Breach		$53,398,278	
Lottery/Sweepstakes/Inheritance		$48,642,332	

The above data on loss by victim shows that business email compromise (BEC)/email account compromise (EAC) ranked topmost among the losses suffered by victims. The report defined business email compromise scam as "a scam targeting businesses working with foreign suppliers and/or businesses regularly performing wire transfers" (IC3 Report, 2019, p.25). Furthermore, it defined email account compromise as "a similar scam that targets individuals…" (IC3 Report, 2019, p.25). The report further explained that these scams are perpetrated by fraudsters who compromise email accounts through social engineering or computer intrusion techniques to do unauthorized transfers. The

average business person is looking for opportunities for expansion and profit maximization. In the desperation to achieve such goal it is probable that he or she may play into the hands of fraudsters who may use social engineering techniques to compromise their account. On the other hand individual accounts may be compromised because many individual users do not take necessary steps to protect their personal computers. This perhaps explains why BEC/EAC is top on the list.

3.4 The Victim-Offender Overlap in Cybercrime

The victim-offender overlap suggests that there is a link between victims and offenders. It is argued that the assumption that victims and offenders can be neatly separated into two mutually exclusive groups is problematic. This is because there are likely some commonalities between victims and offenders.

4.0 CONCLUSION

The landscape of victimization has changed with the emergence of the internet and development of digital devices. In the digital age, people can be victimized from any part of the globe. Online victimization does not require face-to-face contact between the victim and the offender. Victims can be individual internet users, organizations, communities or governments.

5.0 SUMMARY

The unit focused on the definition of cybercrime victims, types of cybercrime victims, patterns of cybercrime victims, and the victim-offender overlap in cybercrime.

6.0 TUTOR-MARKED ASSIGNMENT

Discuss the various types of cybercrime victims.

7.0 REFERENCES/FURTHER READING

Angkasak, D. (2018). Local protection for cybercrime victims on victimological perspective. SHS Web of Conference, 54, 08004: Available at: https://doi.org/10.1051/shsconf/20185408004

Internet Crime Complaint Centre (2019). 2018 Internet Crime Report. Available at: https://pdf.ic3.gov/2019_IC3Report.pdf

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

UNIT 4 CYBERCRIME VICTIMIZATION RISK FACTORS

CONTENTS

1.0 INTRODUCTION

There are several factors that can potentially expose a person to the risk of cybercrime victimization. The internet and digital devices are now engrained in the routine activities and life style of individuals. The reliance on these technologies coupled with the fact that people as a matter of necessity have to migrate from the analogue culture to the digital one undoubtedly expose them to victimization online.

2.0 OBJECTIVE

This unit covers the following topics: routine activities, victim precipitation, space transition and risk factors of cyber victimization in Africa. At the end of this unit you will understand why some individuals are more likely to fall victim of cybercrime than others.

3.0 MAIN CONTENT

3.1 Routines Activities

The term “routine activities” is used to describe our normal activities that cover those that have to do with our family, friends, work, recreation and consumption. These activities determine who we often come in contact or interact with whether

online or offline. A person's online routine activity, for example, the habit of downloading free software and can put him or her at great risk of cyber victimization. The person may in the process of downloading a free software unknowingly download a malware and may not have an active anti-virus kit installed in his/her computer. The routine activities theory (RAT) of Cohen and Felson (1979) has severally been used by scholars to explain cybercrime victimization.

3.2 Victim Precipitation

There are instances where individuals initiate the process of their own victimization. The victims themselves may actually initiate, either passively or actively, the criminal act that ultimately leads to the harm they suffer. This principle applies to both online and offline environments. For example, in this age of social media the flaunting of wealth on social media platforms can make an individual a target of online advance fee fraud or romance scam. Wolfgang (1967) victim precipitation theory has also been used to explain cybercrime.

3.3 Space Transition

Space transition refers to the movement from one space to another. It could be movement from the physical space to the cyberspace or vice-versa. The digital

revolution that is sweeping across countries of the world has resulted in a dramatic increase the space transition traffic. While many are compelled by their routine activities to transit from the analogue system to the digital one, others are just joining the bandwagon. The 'bandwagoners' may not be information technology-savvy and as such may be more prone to cyber victimization. Again, the transition from the physical space to the cyber space and vice-versa as demonstrated by Jaishankar (2008) in his space transition theory facilitates cyber victimization.

3.4 Cybercrime Victimization Risk in Africa

Ndubueze (2019, pp. 6-8) discussed several vulnerabilities that offenders can exploit to victimize their targets online in Africa.

i.) ***High Number of Domains/Very Weak Network and Information Security*:** In 2014, the United Nations Economic Commission for Africa identified the high number of domains and very weak network and information security as major drivers of Africa's vulnerability to cyber security threats. The Report noted that cybercriminals regard Africa as a favourable climate for their criminal activities. It also argued that cybersecurity experts believe that about 80 percent of personal computers in Africa are infected by virus and other malicious software. This is hardly surprising as there are several "free" Internet networks in some

public places. But many of such networks are not secure and may, in fact, be a trap set by cybercriminals who want to access users' personal information with a view to using same to victimize them.

ii.) ***Inadequate Protection of Computer System*****:** Computer security experts believe that many computer systems in Africa are not properly protected and that this exposes them to cyber attack. The ordinary computer user care little about Internet security software. Even when they procure one, they may be reluctant to update them. Some have argued that auto-updating the security software will consume much of their network data. Users, especially the low income ones will normally want to maximize their data usage. They may consider browsing and emailing as activities that are worth their data and updating of antivirus software as less important. This attitude is compounded by their low awareness of the kind of risk they expose their computer system and data to by not taking appropriate measure to protect them. Low income internet users may feel that they are not famous or known and cannot be targeted by cybercriminals. This kind of mind-set perhaps accounts for why they are reluctant to take the necessary steps to protect their personal computers.

iii.) ***Digital Skill-Set Gap*****:** Digital literacy is still relatively low in Africa when compared to the developed continents of the world. Ndubueze (2016b) provides a typology of digital skills in Nigeria viz: i) the digital affable – persons with strong digital skill sets. This category of people can easily operate their personal computers, cell-phones and the Internet. Digital tools have also become part of their daily activities, ii) the digital enfeeble - persons that are weak in the use of digital technology/tools. They are not familiar with the basic functions of their cell-phones and ipads. They also hardly use the Internet and carry smartphones not necessarily because they need it, but as a status symbol, iii) the digital dumb – persons who do not have digital skill set at all. They are digitally passive and avoid using digital tools. If they must use digital tools, they rely on the assistance of a third-party, who is familiar with such tools. Arguably, the last two categories of people are more vulnerable to cyber victimization. This is because they would normally rely on third-parties to do their digital transactions such as bank Automated Teller Machine (ATM) withdrawals and other online transactions. This may expose their passwords to criminal elements. However, those heavily attached to digital tools and are Internet-active, who belong to the first category are also vulnerable to cyber victimization.

iv.) ***Absence of African Languages*:** It has been argued that many African computer users may have difficulty in understanding error messages or warnings about cyber fraud not presented in their mother tongue. This may expose them to cyber fraud. Cyber fraudsters will usually exploit any loop-hole that they find in information and communication technology (ICT) tools to victimize their targets. Therefore, the language issue is a major problem.

v.) ***Trust Factor:*** Trust within families plays a key role in many African societies. People may use their trusted relatives who live with them for certain online transactions, not because the principal does not have digital skill, but because they are trusted. Consequently, such relatives are expected to keep the details of such online transactions confidential. But that may not always be the case, as sometimes, these trusted relatives may be compromised through social engineering or other malicious means by cybercriminals to reveal some personal information of their principal, which, such criminals would eventually use to victimize them.

vi.) ***Greed Factor:*** Greed is a major factor in cybercrime victimization in the African context. It is perhaps one of the most exploited weaknesses by cybercriminals. Many people in Africa think of a better and brighter

future. Many people want to make it big in life; they want to amass wealth and live in opulence. But not too many of such people who are within the 'generation y' age bracket realize that wealth do not come so easily. Cyber criminals in Africa, specifically the *yahoo-yahoo boys* (Internet advance fee fraudsters), exploit this insatiable quest for wealth to perpetrate many online advance fee fraud schemes in the continent.

vii.) ***Faith Factor***: There are several faith-based organizations in Africa. Some of these organizations are prayer groups that encourage members to believe in financial 'miracles'. However, online advance fee fraudsters may exploit this kind of scenario by sending some bogus (advance fee fraud) mails to targets who may mistake such communications as evidence of answered prayers and ultimately fall victims.

4.0 CONCLUSIONS

The landscape of victimization has changed with the emergence of the internet and development of digital devices. In the digital age people can be victimized from any part of the globe. Online victimization does not require face-to-face contact between the victim and the offender. Victims can be individual internet users, organizations, communities or governments. There are several vulnerabilities that cybercriminals can exploit to victimize their targets online in Africa.

5.0SUMMARY

The unit focused on the definition of cybercrime victims; types of cyber victimization; patterns of cybercrime victimization and cybercrime victimization risk factors in Africa.

6.0 TUTOR-MARKED ASSIGNMENT

Discuss the various risk factors that expose internet users in Africa to cybercrime victimization.

7.0 REFERENCES/FURTHER READING

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

Module 6: Cyber Crime Legislations and Cyber Security Initiatives

Unit 1: Cyber Crime Legislations in Nigeria

Unit 2: Cyber Security Strategies/Initiatives at National, Regional and International Levels

Unit 3: Artificial Intelligence for Cyber Security

Unit 4: Challenges of Policing and Enforcement

UNIT 1 CYBERCRIME LEGISLATIONS IN NIGERIA

CONTENTS

1.0 INTRODUCTION

The emergence of the internet and eventual growth of crime and criminality in the cyberspace has created some kind of moral panic in the Nigerian society. This has resulted in calls for the effective regulation of the activities internet users. This call led to the enactment of the first cybercrime-specific legislation in Nigeria. Before the enactment of the Cybercrime (Prohibition and Prevention etc.) Act in 2015, the relevant law enforcements agencies relied on the Criminal Code Act, 1990, the Economic and Financial Crimes Commission (Establishment) Act, 2004, the Advance Fee Fraud and Other Related Offences Act, 2006 etc. to prosecute cybercriminals in Nigeria.

3.0 OBJECTIVE

This unit covers the scope of two cybercrime and related offences legislations in Nigeria. They include: The Advance Fee Fraud and Other Fraud Related Offences Act, 2006 and the Cybercrime (Prohibition, Prevention, etc.) Act, 2015. At the end

of this unit, you will learn the aim of these legislations and the areas that are covered in them.

3.0 **MAIN CONTENT**

3.1 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 y 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, and the High Court of the States, with the jurisdiction to try offences and impose penalties provided under it.

3.2 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;

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.

4.0 CONCLUSION

The war against cybercrime by relevant law enforcement agencies in Nigeria cannot be effective unless backed by adequate legislations. The Cybercrime Prohibition, Prevention, Etc.) Act, 2015 undoubtedly has given a major boost to the efforts to control cybercrime and criminality in Nigeria. It is hoped that the severe penalties that the offences attract will deter cyber criminals.

5.0SUMMARY

The unit focused on two existing legislations that are related to cybercrime in Nigeria: The Advance Fee Fraud and Other Fraud Related Offences, Act, 2015 and the Cybercrime (Prohibition, Prevention, Etc.) Act, 2015. The two legislations provide the legislative frame work for the policing of cybercrime and prosecution of offenders in Nigeria.

4.0TUTOR-MARKED ASSIGNMENT

Compare the major; provisions of Advance Fee Fraud and Other Fraud Related Offences, Act, 2015 to those of the Cybercrime (Prohibition, Prevention, Etc.) Act, 2015.

7.0 REFERENCES/FURTHER READING

Advance Fee Fraud and Other Fraud Related Offences, Act, 2015

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

UNIT 2 CYBERSECURITY STRATEGIES/INITIATIVES AT THE NATIONAL, REGIONAL, AND INTERNATIONAL LEVELS

CONTENTS

1.0 INTRODUCTION

Cybersecurity is one of the topmost global security concerns of the digital age. States across the world are concerned about building efficient and effective cyber defenses that will protect them from cyber deviants, criminals, terrorists as well as state-actors. The preeminence of cybersecurity underpins the efforts to formulate cybersecurity strategies at national, regional and global levels.

2.0OBJECTIVE

This unit focuses on the meaning and scope of cybersecurity, the various cybersecurity strategies at the national, regional and global levels. At the end of this unit, you will appreciate why state governments, regional and international organizations are interested in drafting and implementing cyber security strategies.

3.0MAIN CONTENT

3.1 Meaning and Scope of Cybersecurity

According to Orji (2015, p. 107) the term cybersecurity is defined as "the collection of tools, policies, guidelines, risk, management, approaches, actions, training, best practices, assurances and technologies that can be used to protect the cyber-environment and organization, as well as users' assists ". However, for

Ndubueze (2014, p.152), "Cybersecurity generally encompasses all efforts by individuals, organizations or the government towards removing all known and anticipated loopholes in the cyber infrastructure that may be exploited by online deviants, criminals and terrorists ."

The above definitions clearly underscore the fact the cyber architecture is vulnerable to attacks. Hence, the need for all stakeholders to collaborate to build formidable cyber defenses to protect it from such attacks. This is the essence of cybersecurity.

Kostopoulos (2018, p.xvi) pointed out that 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 National Cybersecurity Strategy/Initiatives

The Federal Government of Nigeria (FGN) has taken several measures to secure Nigeria cyber infrastructure form emerging threats. One of such measures is the development of the National Cybersecurity Policy and Strategy (NCPS) 2015. The policy document enumerates how Nigeria can ensure its preparedness for threats in the cyberspace and underpin the willingness to build comprehensive capability to protect Critical National Information Infrastructure (CNII) and mitigate cyber risks. One initiative that helped to strengthen the National Cybersecurity Policy and Strategy (NCPS) 2015 is the Cybercrime (Prohibition, Prevention, etc,) Act, 2015. The Act contains the comprehensive legal framework for cybersecurity as well as the prohibition and punishment for cybercrimes in Nigeria. More so, to meet the requirements for cybersecurity, Section 41 (b) of the Cybercrime (Prohibition, Prevention, etc,) Act, 2015 provides for the formulation and effective implementation of the National Cybersecurity Policy and Strategy (see, the National Security Strategy, 2019).

Arguably, the effective implantation of the National Cybersecurity Policy and Strategy in Nigeria by relevant stakeholders including law enforcement agencies will ensure the smooth operations of Nigeria cyber infrastructure. This will in turn serve to boost citizens and organizations confidence in cyber systems.

3.2 Regional Cybersecurity Strategy/Initiatives

The African Union with headquarters in Addis Ababa, Ethiopia is committed to incorporating emerging technologies in Africa's development plans and ensuring these technologies are used for the benefit of African individuals, institutions and nation states by ensuring data protection and safety online.

On June 27, 2014, the member states of the African Union adopted the African Union Convention on Cyber Security and Personal Data Protection. 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.

On December 10 to 12, 2019, the African Union Expert Group (AUCSEG) inaugural meeting was held in Addis Ababa, Ethiopia. The aim of the gathering of the ten cybersecurity experts representing the five African regions was to discuss cybersecurity issues and challenges in the continent and deliberate on how to address them. The specific objectives of AUCSEG are as follows:

i. Advising the African Union Commission (AUC) on cybersecurity issues and polices;

ii. Proposing solutions to facilitate the ratification and domestication of the Malabo Convention into national laws;

iii. Sharing the best policy on how to mitigate current and new threats and on the protection of critical infrastructure and election systems as well;

iv. Identifying areas of research needed for the formulation of polices, guidelines, etc., which can be general or sector-specific;

v. Identifying ways to support the establishment and development of Computer Security Incident Response Team (CSIRTs);

vi. Developing ways for close collaboration among AU Member States and stakeholders, on cybersecurity;

vii. Proposing ways to build capacities and to increase skills in ICTs security and their proper use;

viii. Supporting AU on building African position within the international process related to cybersecurity including ways of cooperation with international stakeholders.

As part of its objectives, the group will adopt strategies and action plan to address the African cybersecurity needs and gaps in resource and know-how. It will also propose decisions on the promotion of cybersecurity for socio-economic development in Africa.

From the foregoing it is evident that the African Union has set up the needed machinery for the promotion of cybersecurity among members states. However, the success of these strategies and initiatives will largely depend on how well the respective member states fulfill their obligations to the Union in this respect.

3.4 International Cybersecurity Strategies/Initiatives

The United Nations (UN) with headquarters in New York, United States is committed to global cybersecurity. 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 help to address existing and potential threats related to the use of information and communication technologies (ICTs) (see, Wolter, 2020).

Furthermore, another example of the demonstration of the United Nations commitment to ensuring global cybersecurity, 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. Experts across the world including academics and practitioners were invited 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

Cybersecurity is an issue that concerns all countries of the world. Given the borderless nature of the cyberspace and the devastating nature of cyber attacks, nation-states cannot but collaborate and partner in the war against cybercrime and

cyber terrorism. These collaborations and partnerships have been formed under the auspices of the African Union and the United Nations. Nonetheless, the Federal Government of Nigeria have also demonstrated its readiness to combat crime and terror in the cyberspace and ensure cybersecurity have also established necessary policy and legislative frameworks.

5.0SUMMARY

The unit focused on the various cybersecurity strategies/initiatives at the national, regional and international levels. It highlighted the need for collaborations and partnerships among stakeholders in the war against crime and terrorism in the cyberspace.

6.0TUTOR-MARKED ASSIGNMENT

Discuss the efforts of the African Union in the promotion of cybersecurity in Africa.

7.0 REFERENCES/FURTHER READING

African Union Convention on Cyber Security and Personal Data Protection (2014).

Retrieved June 2, 2019 from

https://au.int/.../29560-treaty-0048_-_african_union_convention_on_cyber_security_.

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

National Security Strategy (2019). Federal Republic of Nigeria.

Ndubueze, P.N. (2014). Cyber security and industrial development in digital Nigeria. In D.O. Imbhonopi & U.M. Urim (eds.) *Trajectory to Industrial Development in Nigeria*. (pp. 149-160). Ota: Department of Sociology, Covenant University.

Orji, U.J. (2015). Multilateral legal response to cyber security in Africa: Any hope for effective international cooperation? 2015 7th International Conference on Cyber Conflict Architectures in Cyberspace. In M.Maybum, A. M. Osula, L. Lindstom (eds,) Tallinn: NATO CCD COE Publications.

United Nations Institute for Disarmament Research (UNIDIR) (2017). United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the 21st Century. Available at:

https://www.unidir.org/files/publications/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf

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 ARTIFICIAL INTELLIGENCE FOR CYBERSECURITY

CONTENTS

1.0 INTRODUCTION

Artificial intelligence (AI) is an area of computer science that is fundamentally concerned with how intelligent machines that functions like human beings can be

created. This area is an emerging area that has received great attention in the digital age. Today, cybersecurity experts are interested in learning how artificial intelligence can be deployed to solve cybersecurity issues.

1.0 OBJECTIVE

This unit covers the meaning and scope of artificial intelligence and artificial intelligence techniques for cyber security. At the end of the unit you will learn how artificial intelligence is applied to cybersecurity.

2.0 MAIN CONTENT

3.1 Meaning and Scope of Artificial Intelligence

Artificial intelligence is primarily a machine-based intelligence. With the monumental breakthrough in the Information and Communication Technologies (ICTs) in the 21st century machines are designed and equipped with the capacity to function as humans, as it were. Vahakainu and Lehto (2019, p. 431) defined artificial intelligence as:

> Artificially-formed intelligence that provides tools for solving complex and demanding problems on a computer or machine. Artificial intelligence is a combination of information technology

and physiological intelligence, which can be computationally used to reach goals.

3.2 Artificial Intelligence Techniques for Cybersecurity

The following artificial intelligence techniques have been identified by Panimalar, Giri and Salman (2018, p.122-123):

i. **Expert System:** This is a computer system that copies the decision making ability of humans. A good example of expert system is knowledge-based systems. Knowledge-based systems are made up of two sub-systems: the knowledge base and the inference engine. The knowledge base comprise of the real world illustrations and assertions, while the inference engine is an automatic reasoning system. It evaluates the current situation of the knowledge base and applies the rules relevant to it, and asserts new knowledge into it. The Cybersecurity Artificial Intelligence Export System comprise the following in knowledge base and interference engine:

Components of Expert Systems	
Knowledge Base	Malicious IP Address
	Known Malware
	Known Virus
	Approved Applications
	Approved IP Addresses
	End Point Usage Statistics
Inference Base	IP Address Geographical Location
	Connection Attempts
	Connection Patterns

	Frequency of Programme Use
	Document Usage
	Login Timestamps
	Port Communication
	File/Folder Access Patterns

Source: Arockia, Giri and Salman (2018, p.123).

Arockia, Giri and Salman (2018) further explained that **Security Expert System** follows a set of rules to combat cyber-attacks. It checks the process with the knowledge base and ignores if it is good known processes, otherwise the system terminates the process. Where no such process exist in the knowledge base, then inference engine algorithms (rule sets) is used by the expert system to find out the machine state. The machine state is made up of three states: safe, moderate and severe. Depending on the machine state, the administrator or user is alerted about the status and the inference feed to knowledge base. The advantages of expert

systems include: decision support, instruction detection, knowledge base and inference engine.

ii. **Neural Nets**: This is also called deep learning. It is an advanced component of artificial intelligence that is designed to work and functions like the human brain. The human brain has several neurons, which serve several purpose, are domain-independent and can learn any type of data. In 1957, Frank Rosenblatt created an artificial neuron (Perceptron) which facilitated neural networks. Perceptron can learn and tackle absorbing issues by combining with other nerves (perceptron). Perceptron on their own can identify the entity on which they are trained by learning and processing the high level raw data, as our brain learns its own from the raw data using our sensory organ's input. When this deep learning (trained) is applied to cybersecurity the system can identify whether a file is malicious or legitimate without human interference. This technique produces strong result in detecting the malicious threats, compared to classical machine learning systems. Neural net's speed makes it very useful in cybersecurity. They can allow the exact detection of new malware threats and close the loophole thereby preventing a potential cyber attack. The advantages of neural nets include: intrusion detection

and protection system, high speed operation, denial of service detection and forensic investigation.

iii. **Intelligent Agents**: This is an independent entity which recognizes movement through sensors and follows up on an environment using actuators, which is an agent and direct its activity towards certain objectives. Intelligent agents may use knowledge base to accomplish their objectives. Intelligent agent is created to combat Distributed Denial of Service (DDoS) attack. The advantages of intelligent agents include: proactive, have agent communication language, mobility. They are reactive and can protect against DDoS.

4.0 CONCLUSION

Artificial intelligence is an emerging area in Computer Science that has shown great promise for cybersecurity. Artificial Intelligence-based cybersecurity defense has demonstrated capacity to tackle cyber threats and attacks.

5.0SUMMARY

The unit focused on the meaning and scope of artificial intelligence and examined some artificial intelligence techniques that are deployed for cybersecurity such as expert systems, neural nets and intelligent agents.

6.0 TUTOR-MARKED ASSIGNMENT

What are the various artificial intelligence techniques used for cybersecurity.

7.0 REFERENCES/FURTHER READING

Arockia, P. S., Giri, P.U. and Salman, K.K. (2018). Artificial intelligence techniques for cybersecurity. *International Research Journal of Engineering and Technology* (5), 3, 122-124.

Vahakainu, P., & Lehto, M. (2019). Artificial Intelligence in the Cyber Security Environment. Proceedings of the 14th International Conference on Cyber Warfare and Security ICCW52019. Available: https://www.researchgate.net/publication /338223306_Artificial_intelligence _in_the_cyber _security_environment_Artificial_intelligence_in_the_cyber_security_environment

UNIT 4 CHALLENGES OF POLICING AND ENFORCEMENT

CONTENTS

1.0 INTRODUCTION

Cybercrime is an emerging crime. The modus operandi for committing cybercrime differs from those of physical space crime in various ways. This makes cybercrime policing a somewhat challenging. Aside the nature of cybercrime posing a challenge for its policing, the issue of extant laws on cybercrime is another area of challenge. In some African countries the laws are not comprehensive enough and even when they are, the enforcement of the laws is sometimes marred by some legal technicalities.

2.0 OBJECTIVE

This unit discusses the challenges associated with policing cybercrime. It also examines the impediments to the effective establishment and enforcement of cybercrime legislation in Africa.

3.0 MAIN CONTENT

3.1 The Challenges of Policing Cybercrime

A renowned cybercrime scholar Wall (2007/2010) identified some challenges confronting the public police in their efforts to control cybercrime as follows:

i. ***De Minimism*:** *De minimism* trap means that the law does not deal with trifles (*de minimis non curat lex*).Many cybercrimes are small-impact

bulk victimizations with a large aggregate loss, but spread out across different jurisdictions of the world. However, local policing strategies cascade to decision at the local level over most efficient expenditure and finite resources, therefore, the 'public interest,' which happens to be a major criterion for releasing police resources for an investigation is usually difficult to justify in individual cases of cybercrime victimization.

ii. ***Nullum Crimen Disparities***: There is the challenge of *nullum crimen* legal disparities in inter-jurisdictional cases (*nullum crimen sine lege* – no crime without law). Though recent protocols as well as cybercrime convention and multi-agency collaborations may facilitate inter-force cooperation, they are nonetheless dependent on whether a particular offense is given similar priority in each jurisdiction. Cooperation may be difficult if the deviant behaviour is an offense in one jurisdiction and not in another.

iii. ***Jurisdictional Disparities***: Police or prosecutors use their resourcefulness to forum-shop when faced with jurisdictional or evidential disparity in order to increase the likelihood of obtaining a conviction. However, inter-jurisdictional cooperation may not to be successful when it comes to non-routine types of offending.

iv. ***Non-routine Activity and Police Culture***: The *solitus* or routinisation issue affects the ability of the police to respond to 'non-routine' criminal activity vis-à-vis their possession of relevant skill sets and experience. Most public policing are based upon local and routinized practices that make up occupational cultures, working patterns and professional policing. Therefore, there may be investigative challenges with non-routine events. Such non-routine events include those created by the internet like cross-border investigations or some deviant behaviour that police officers do not normally consider criminal.

v. ***Under*-reporting:** The under-reporting of cybercrime to the police is another challenge that confronts the police. The assumed problem of under-reporting to the police has been a longstanding debate. The little research into reporting practices, police recording procedures, and prosecutions indicates that there are some shortfalls.

There is no doubt that the above problems accounts for some of the challenges that the police encounter in their efforts to control the problem of cybercrime. These problems are not peculiar to Nigeria or Africa, they cut across the globe. It is also important to note that these are not the only problems that the police encounter in their efforts to control cybercrime. However, they provide us with a baseline for

understanding how challenging it is for law enforcement authorities to effectively control cybercrime.

3.2 Impediments to the Effective Establishment and Enforcement of Cybercrime Legislation in Africa

There are several impediments that militate against the effective establishment and enforcement of cybercrime legislation in Africa. Some of these impediments were identified by Ndubueze (2019) below:

i.) **The Slow Pace of Processing Legislations**: The process of enacting new legislations in some African countries can be long, 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 to 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 their 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:** Law enforcement agencies 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 variant of 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 sound 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.

iii.) **Low Tempo of Enforcement Activities**: Enforcement of cybercrime legislations in many African countries seems relatively low. Several factors may be responsible for this. 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. 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, but not all law enforcement personnel possess that skill.

iv.) **Security versus Privacy Debate**: The dichotomy between security and privacy especially with respect to the use of electronic surveillance is one of the most discussed challenges of policing cybercrime (Nhan and Bachman, 2015). This assertion also applies to Africa. 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:** Jurisdiction is difficult to establish in the cyberspace and this is one of the major challenges of enforcing cybercrime legislation. This is because African countries, like their counterparts in other continents would normally encounter some

difficulty in determining the jurisdiction of cybercrime cases that cut across may countries of the world.

vi.) **Extradition Issues:** The process of extradition could be slow 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 is 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 (see, Ndubueze, 2016). The academia and practitioners may be required to make 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 if such research is not sufficiently and readily available, it may be a challenge. African governments need 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 cyber crimes 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.

ix.) **Weak Voices in Global Internet Governance:** The African Union Commission (2016) has expressed concern over 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.

4.0 CONCLUSION

The emergence of cybercrime has changed the dynamics of policing. Policing in the digital age requires some specialized training and development of skill-sets that are not common in traditional police culture and practices. This constitutes a change for cybercrime policing. The fact that cybercrime offences may vary from one country to another makes cross-border cooperation of law enforcement agencies when prosecuting certain cases difficult. Moreover, there are several issues that make the establishment and seamless enforcement of cybercrime legislation problematic.

5.0SUMMARY

The unit discussed the challenges that public police officers encounter in their efforts to control cybercrime. The several impediments to the effective establishment and enforcement of cybercrime legislations in Africa were also discussed.

6.0 TUTOR-MARKED ASSIGNMENT

Discuss the challenges militating against the effective control of cybercrime by the Police.

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.