COURSE GUIDE

CSS 808
ADVANCED CYBERCRIMES AND CYBER SECURITY

Course Team

Dr. Usman A. Ojedokun (Course Developer/Writer) - UNIBADAN
(Course Editor)
Prof. Sam Obadiah Smah (Course Coordinator) – NOUN
Dr. Dickson Ogbonnaya Igwe (Programme Leader) – NOUN

NATIONAL OPEN UNIVERSITY OF NIGERIA

© 2021 by NOUN Press
National Open University of Nigeria
Headquarters
University Village
Plot 91, Cadastral Zone
NnamdiAzikiwe Expressway
Jabi, Abuja

Lagos Office
14/16 Ahmadu Bello Way
Victoria Island, Lagos

e-mail: centralinfo@nou.edu.ng
URL: www.nou.edu.ng

First Printed 2021

ISBN: 978-978-058-142-8

CONTENTS **PAGE**

Introduction…………………………………………………….. iv
Course Aim…………………………………………………. iv
Working Through this Course……………………………….. iv
Course Materials…………………………………………….. v
Study Units………………………………………………….. v
References and Further Reading…………………………… v
Assignment File……………………………………………… vii
Presentation Schedule……………………………………….. vii
Assessment………………………………………………….. viii
Tutor -Marked Assignments (TMA)…………………………. viii
Final Examination and Grading……………………………… ix
How to get the Most from this Course………………………… ix
Tutors and Tutorials………………………………………….. x
Summary………………………………………………………x

INTRODUCTION

This is a three-credit unit course for postgraduate students in Criminolgy and Security Studies (CSS) in the Faculty of Social Sciences. The material had been designed and written to meet the reading needs of Nigerian students. It provides an overview of what you would be taught and in addition makes provision for the organization and requirements of the course.

COURSE AIM

This course aims to familiarize you with the current advances in cybercrime and cyber security. Specifically, it would enable you have a clear understanding of how the Internet, Internet networks and Internet information and community tools are being employed to carry out different types of crime on the cyberspace. Equally, it would expose you to the transnational characteristic of cybercrime and the associated jurisdictional challenges that are often embedded in the prosecution of cybercrime and cybercriminals. Furthermore, it would acquaint you with the old and emerging threats that are dominating cyberspace and the major efforts being made by concerned stakeholders, such as Internet operators, cyber security experts, governments, multilateral institutions, and international organizations to combat the menace of cybercrime.

The broad aim of the course will be achieved through the discussion of the following:

i. history and evolution of cybercrime
ii. the major types of cybercrimes and their criminological motivations
iii. law enforcement and prosecutorial responses to cybercrime
iv. transnational issues in cybercrime enforcement and prosecution
v. cyber threats and cyber security
vi. cybercrime investigations and electronic evidence
vii. computer forensics investigations
viii. cybercrime and criminological theories

COURSE OBJECTIVES

To attain the aims set out to achieve, *CSS 808: Advanced Cybercrimes and Cyber Security* has been divided into seven different modules, each with its own peculiar objectives. It is in your best interest to study them before you start working through the unit. You may want to refer to them during your study of this unit to check your progress.

Below are the wider objectives of the course as a whole. When you meet the stipulated objectives of the course, the aims of the course would have been automatically achieved. Specifically, you should be able to adequately discuss the following at the successful completion of the course:

i. the internet and emergence of cybercrime
ii. the meaning of cybercrime
iii. the evolution of cybercrime (pre 1970s-2000)
iv. major techniques and tools deployed for perpetration of cybercrime
v. the black market of cyber criminality
vi. the major categorizations of cybercrime
vii. types of cybercriminals
viii. motives of cybercriminals
ix. cybercrime and the *Yahoo Yahoo* phenomenon in Nigeria
x. measuring the socio-economic costs of cybercrime
xi. cybercrime and transnational legal jurisdictions
xii. international legislative efforts at tackling cybercrime
xiii. challenges associated with cybercrime prosecution
xiv. agencies and organizations monitoring cybercrime
xv. Nigerian government efforts at tackling cybercrime
xvi. cyber threats in the cyberspace
xvii. the necessity for cyber security
xviii. cybercrime, surveillance, and privacy issues
xix. cyber threats and cyber safety tips
xx. what is electronic evidence?
xxi. procedures for generating electronic evidence
xxii. electronic evidence handling in cybercrime investigation
xxiii. sourcing for electronic evidence in cybercrime investigation
xxiv. the place of electronic evidence in criminal trial
xxv. meaning of computer forensics
xxvi. the standard phases in computer forensic investigation
xxvii. computer forensic investigation tools
xxviii. mobile devices in computer forensic investigation
xxix. challenges associated with computer forensic investigation
xxx. anomie-strain theory and differential association theory
xxxi. social learning theory and situational crime prevention perspective
xxxii. routine activity theory and lifestyle exposure theory
xxxiii. space transition theory and digital drift theory

WORKING THOUGH THIS COURSE

To complete this course, you are required to read the study units and other related materials. You will also need to undertake practical exercises for which you need a pen, note-book, and other materials listed below. The exercises are to help you in understanding the concepts found in this study. At the end of each unit, you will be required to submit written assignments for assessment purposes. At the end of the course, you will write a final examination.

COURSE MATERIALS

The major materials you will need for this course are:

i. Course Guide
ii. Study Units
iii. Assignment File
iv. Relevant textbooks including the ones listed under each unit
v. As a criminology student, it will be good for you to read up and familiarize yourself with cases of cybercrimes reported in both electronic and print media. Also, you are expected to be aware of the changing nature, trends and patterns of cybercrime in the world at large and Nigeria in particular.

Study Units

In this course, there are four modules, divided into 18 units. Below are the units covered:

Module 1 History of Cybercrime

Unit 1 The Internet and the Emergence of Cybercrime
Unit 2 The Meaning of Cybercrime
Unit 3 The Evolution of Cybercrime (Pre 1970-2000)
Unit 4 Techniques and Tools Deployed for Cybercrime
Unit 5 The Black Market of Cyber Criminality

Module 2 Cyber Criminals and their Motives

Unit 1 Cybercrime Categorisations
Unit 2 Types of Cybercriminals
Unit 3 Motives of Cybercriminals
Unit 4 Cybercrime and the *Yahoo Yahoo* Phenomenon in Nigeria
Unit 5 Measuring the Socio-Economic Costs of Cybercrime

Module 3 Cybercrime and Law Enforcement

Unit 1 Cybercrime and Transnational Legal Jurisdictions
Unit 2 International Legislative Efforts for Tackling Cybercrime
Unit 3 The Challenges associated with Cybercrime Prosecution

Unit 4	Agencies and Organizations Monitoring Cybercrime

Module 4	**Cyber Threat and Cyber Security**
Unit 1	Cyber Threats and Cyber attacks in the Cyberspace
Unit 2	The Necessity for Cyber Security
Unit 3	Cybercrime, Surveillance, and Privacy Issues
Unit 4	Cyber Threats and Cyber Safety Tips

Module 5	**Cybercrime and Electronic Evidence**
Unit 1:	What is Electronic Evidence?
Unit 2	Procedures for Generating Electronic Evidence
Unit 3	Electronic Evidence Handling in Cybercrime Investigation
Unit 4	Sourcing for Electronic Evidence in Cybercrime Investigation
Unit 5	The Place of Electronic Evidence in Criminal Trial

Module 6	**Computer Forensics and Cyber Crime Investigation**
Unit 1	Meaning of Computer Forensics
Unit 2	The Standard Phases in Computer Forensic Investigation
Unit 3	Computer Forensic Investigation Tools
Unit 4	Mobile Devices in Computer Forensic Investigation
Unit 5	Challenges Associated with Computer Forensic Investigations

Module 7	**Cybercrime and Criminological Theories**
Unit 1	Anomie-Strain Theory and Differential Association Theory
Unit 2	Social Learning Theory and Situational Crime Prevention Perspective
Unit 3	Routine Activity Theory and Lifestyle Exposure Theory
Unit 4	Space Transition Theory and Digital Drift Theory

References and Further Reading

Every study unit contains a list of references for further reading. Do not hesitate to consult them if need be.

THE ASSIGNMENT FILE

The assignment file contains all the tutor-marked assignments including CSS 808. Make sure your assignments are done and submitted to your tutor for marking. The marks you obtain from these assignments will reflect in the final score you will obtain in this course.

THE PRESENTATION SCHEDULE

The Presentation Schedule included in your course material gives you important dates for the completion of tutor-marked assignments and tutorial attendance. Remember, you are required to submit all your assignments by the due date. You should not be lagging behind in your work.

ASSESSMENT

Your assessment will be based on tutor-marked assignments (TMAs) and final examination which you will write at the end of the course.

TUTOR- MARKED ASSIGNMENTS (TMAs)

In addition to working through all the TMAs in your course material, four TMAs would be sent to you in the assignment file. The four TMAs must be answered and submitted for assessment. The four assignments would be marked and the best three would be selected which will constitute the 30% of your final grade.

FINAL EXAMINATION AND GRADING

At the end of the course, you will write a final examination which will constitute 70% of your final grade. In the examination which shall last for two hours, you will be requested to answer three questions out of at least five.

HOW TO GET THE MOST FROM THIS COURSE

In Distance Learning Programme, the study units replace the university lecturers. This is one of the great advantages of distance learning; you can read and work through specially designed study materials at your own pace, and at a time and place that suits you best. Think of it as reading the lecture instead of listening to the lecturer. In the same way a lecturer might give you some reading to do, study units tell you when to read, and which are your text materials or set books. You are provided exercises to do at appropriate points, just as a lecturer might give you an in-class exercise.

Each of the study units follows a common format. The first item is an introduction to the subject matter of the unit, and how a particular unit is integrated with the other units and the course as a whole. Next to this is a set of learning objectives. These objectives let you know what you should be able to do by the time you have completed the unit. These learning objectives are meant to guide your study. The moment a unit is finished, you must go back and check whether you have achieved the objectives. If you make this a habit, then you will significantly improve your chances of passing the course. The main body of the unit guides you through the required reading from other sources. This will usually be either from your set books or from a reading section. The following is a practical strategy for working through this course. If you run into any trouble, telephone your tutor. Remember that your tutor's job is to help you. When you need assistance, do not hesitate to call and ask your tutor to provide it.

Most importantly you are to read this Course Guide thoroughly and automatically becomes your first assignment. Thereafter, organise a Study Schedule. Design a "Course Overview" to guide you through the Course. Note the time you are expected to spend on each unit and how the assignments relate to the units. Important information, e.g. details of your tutorials, and the date of the first day of the semester is available from the study centre. You need to gather all the information into one place, such as your diary or a wall calendar. Decide on a method and write in your own dates and schedule of work for each unit. Once you have created your own study schedule, do everything to stay faithful to it. The most important reason students fail is that they get behind with their course work. If you get into difficulty with your schedule, please, let your tutor know before it is too late for help. Turn to every unit and read the introduction and the objectives for the unit. Assemble the study materials. You will need your set books and the unit you are studying at every point in time. Work through the unit. As you work through it, you will know what sources to consult for further information. In addition, keep in touch with your study centre as up-to-date course information will be continuously available there and before the relevant due dates (about 4 weeks before due dates), keep in mind that you will learn a lot by doing the assignments carefully. They have been designed to help you meet the objectives of the course and therefore will help you pass the examination. Submit all assignments not later than the due date.

It is also compulsory to review the objectives for each study unit to confirm that you have achieved them. If you feel unsure about any of the objectives, review the study materials or consult your tutor. When you are confident that you have achieved a unit's objectives, you can start on the next unit. Proceed unit by unit through the course and try to pace your study so that you keep yourself on schedule. When you have submitted an assignment to your tutor for marking, do not wait for its return before starting on the next unit. Keep to your schedule. When the assignment is returned, pay particular attention to your tutor's comments, both on the tutor-marked assignment form and on the ordinary assignments. After completing the last unit, review the course and prepare yourself for the final examination. Check that you have achieved the unit objectives (listed at the beginning of each unit) and the course objectives (listed in the Course Guide). Lastly, ensure that you practice on the personal computer as prescribed to gain the maximum proficiency required.

TUTOR AND TUTORIALS

The dates, times and locations of these tutorials will be made available to you, together with the name, telephone number and address of your tutor. Each assignment will be marked by your tutor. Pay close attention to the comments your tutor might make on your assignments as these will help in your progress. Make sure that assignments reach your tutor on or before the due date. Your tutorials are important. Therefore, try not to skip any. It is an opportunity to meet your tutor and your fellow students. It is also an opportunity to get the help of your tutor and discuss any difficulties you might encounter when reading

SUMMARY

This course material is written to equip you with vital information and comprehensive details required to make you become well-informed and knowledgeable about the advances in cybercrimes and cyber security.

MAIN COURSE

CONTENTS **PAGE**

Module 1 History of Cybercrime…………………. 1

Unit 1 The Internet and Emergence of Cybercrime……………………………… 1
Unit 2 The Meaning of Cybercrime……………. 6
Unit 3 The Evolution of Cybercrime (Pre 1970-2000)…………………………. 11
Unit 4 Techniques and Tools Deployed for Cybercrime ….. 14
Unit 5 The Black Market of Cyber Criminality 17

Module 2 Cybercriminals and their Motives……. 20

Unit 1 Cybercrime Categorizations……………. 20
Unit 2 Types of Cybercriminals……………….. 24
Unit 3 Motives of Cybercriminals…………….. 30
Unit 4 Cybercrime and the *Yahoo Yahoo* Phenomenon in Nigeria………………… 35
Unit 5 Measuring the Socio-Economic Costs of Cybercrime…………………………….. 41

Module 3 Cybercrime and Law Enforcement….. 50

Unit 1 Cybercrime and Transnational Legal Jurisdictions…………………………….. 50
Unit 2 International Legislative Efforts for Tackling Cybercrime…………………… 53
Unit 3 The Challenges associated with Cybercrime Prosecution………………… 53
Unit 4 Agencies and Organizations Monitoring Cybercrime……………………………… 59

Module 4 Cyber Threat and Cyber Security…….. 64

Unit 1 Cyber Threats and Cyber Attacks in the Cyberspace………………………………. 64
Unit 2 The Necessity for Cyber Security……….. 72
Unit 3 Cybercrime, Surveillance, and Privacy Issues 85

Unit 4 Cyber Threats and Cyber Safety Tips 89

Module 5 Cybercrime and Electronic Evidence 96

Unit 1: What is Electronic Evidence? ……….. 96
Unit 2 Procedures for Generating Electronic Evidence………………………………. 103
Unit 3 Electronic Evidence Handling in Cybercrime Investigation………………. 112
Unit 4 Sourcing for Electronic Evidence in Cybercrime Investigation…………… 123
Unit 5 The Place of Electronic Evidence in Criminal Trials…………………………. 133

Module 6 Computer Forensics and Cybercrime Investigation………………………….. 139

Unit 1 Meaning of Computer Forensics……… 139
Unit 2 The Standard Phases in Computer Forensic Investigations………………. 145
Unit 3 Computer Forensic Investigation Tools 150
Unit 4 Mobile Devices in Computer Forensic Investigations……………………………155
Unit 5 Challenges associated with Computer Forensic Investigations………………. 161

Module 7 Cybercrime and Criminological Theories……………………………… 165

Unit 1 Anomie-Strain Theory and Differential Association Theory…………………… 170
Unit 2 Social Learning Theory and Situational Crime Prevention Perspective …………. 172
Unit 3 Routine Activity Theory and Lifestyle Exposure Theory ……………………… 174
Unit 4 Space Transition Theory and Digital Drift Theory……………………………..176

MODULE 1 HISTORY OF CYBERCRIME

Unit 1 The Internet and Emergence of Cybercrime
Unit 2 The Meaning of Cybercrime
Unit 3 Evolution of Cybercrime (Pre 1970-2000)
Unit 4 Techniques and Tools Deployed for Cybercrime Perpetration
Unit 5 The Black Market of Cyber Criminality

UNIT 1 THE INTERNET AND EMERGENCE OF CYBERCRIME

CONTENTS

1.0 Introduction
2.0 Objectives
3.0 Main Content
3.1 The Internet and Emergence of Cybercrime
4.0 Conclusion
5.0 Summary
6.0 Tutor-Marked Assignment
7.0 References/Further Reading

1.0 INTRODUCTION

Internet represents a significant leap in the area of technological innovation and advancement. Its emergence has been beneficial in multiple ways to human population in terms of ease of communication, information exchange, and information dissemination which transcends both space and time. In essence, Internet has positively transformed modes of human interactions, ways of doing business, people’s leisure activities, how work is generally done and organized etc. While this technological innovation has been globally beneficial to human population on many fronts, the anonymity which it offers as well as its global interconnectivity has given birth to a distinct category of criminals – the cybercriminals! Today, crimes being perpetrated on the Internet are national, transnational and international in nature.

2.0 OBJECTIVES

At the end of this Unit, you should be able to:

- trace the origin of the Internet
- explain the relationship between the Internet and cybercrime

3.0. MAIN CONTENT

3.1 The Internet and Emergence of Cybercrime

The emergence of the Internet has tremendously altered the ways through which human population get things done. The Internet has emerged as the fastest-growing communications tool ever-developed in the world. Generally, its emergence has significantly transformed the spheres of business, work, consumption, leisure, and politics (Castells, 2002). As at 2001, more than 700 million people were estimated to be using it (Giddens et al., 2003). By 2007, more than 1 billion people were already using electronic mail (e-mail), with over 240 million using different mobile Internet devices (Siegel, 2007). There are now over 2.8 billion Internet users worldwide, with 641.6 million users living in China and a quarter billion in the US (Internet Live Stats, 2015). These two nations have the highest populations of users of all nations worldwide, though individuals in virtually every nation around the world have some presence online (Internet Live Stats, 2015). By the end of the year 2020, the number of networked devices (the ‘internet of things’) will outnumber people by six to one, transforming current conceptions of the Internet. In the hyper connected world of tomorrow, it will become hard to imagine a ‘computer crime’, and perhaps any crime, that does not involve electronic evidence linked with internet protocol (IP) connectivity (United Nations Office on Drugs and Crime, 2013).

Indeed, the proliferation of computing and networked devices throughout the world, including computers, personal digital assistants (PDAs), and cellular phones is among the most profound technological changes in human history. There is no doubting the fact that the increasing capacity of information technologies (IT) to transform the ways we work and function as a society is unprecedented (McQuade, 2009). Many individuals now have multiple presences online as indicated by several email accounts for both personal and business use and social networking profiles on different sites like Facebook and Instagram. Moreover, consumers are also increasingly discarding the use of print media and opting for e-readers or digital book formats (Wray, 2014). In addition, the cell phone, particularly text messaging, has become the preferred method of communication over other traditional means, including in-person conversations, letters, phone calls, and even email. In fact, individuals under the age of 20 are the age group most likely to send texts rather than to make phone calls (Zickuhr, 2011).

Castells (2002) referred to the Internet as a ‘network of networks’. In essence, a network that links computers together, and enabling communication and information exchange amongst them (Yar, 2006). Many such networks of information and communication technology (ICT) have been in existence for many decades. Some were used in the financial markets, while other big institutions like the military, government departments, business organizations, universities, amongst others have also incorporated them into their operations. Generally, the Internet provides the means to link up the many and diverse networks already in existence, creating from them a single network that enables communication between any and all ‘nodes’ (e.g. individual computers) within it (Yar, 2006). The origin of the Internet has been traced to the development of a network, widely regarded as the ARPANET which was sponsored by the US military in the 1960s with the primary purpose of establishing a means through which secure and resilient communication and coordination of military activities could be made possible. In the political and strategic context of the ‘Cold War’, with the ever-present threat of nuclear confrontations, such a network was seen as a way of ensuring that critical communications could be sustained, even if particular ‘points’ within the computer infrastructure were damaged by an attack (Yar, 2006).

Furthermore, the ARPANET’s technology was also aimed at allowing communications to be broken up into ‘packets’ that could then be sent via a range of different routes to their destinations, where they could be reassembled into their original form. Even if some of the intermediate points within the network failed, they could simply be bypassed in favour of an alternate route, ensuring that messages reached their intended recipients. The creation of the network entailed the development not only of the appropriate computer hardware, but also of ‘protocols’, the codes and rules that would allow different computers to ‘understand’ each other. This development got under way in the late 1960s, and by 1969 the ARPANET was up and running, initially linking together a handful of university research communities with government agencies. From the early 1970s, further innovations appeared, such as electronic mail applications, which expanded the possibilities for communication. Other networks, paralleling the ARPANET such as the UK’s JANET (Joint Academic Network) and the US’s NSFNET (belonging to the American National Science Foundation) were also established. By using common communication protocols, these networks could be connected together, forming an inter-net, a network of networks.

A major impetus for the emergence of the Internet was made possible in 1990 when the US authorities released the ARPANET to civilian control, under the auspices of the National Science Foundation (Yar, 2006). Also, that same year, 1990, saw the development of a web browser by the researchers at the CERN physics laboratory in Switzerland dubbed the ‘world wide web’ (www). This software was subsequently elaborated by other programmers, and this allow for more sophisticated forms of information exchange such as the sharing of images as well as text (Yar, 2006). The first commercial browser, Netscape, was launched in 1994, with Microsoft launching its own Internet Explorer the following year (1995). These browsers made Internet access possible from personal computers (PCs). In the mid-1990s, numerous commercial Internet Service Providers (ISPs) entered the market, offering connection to the Internet for anyone with a computer and access to a conventional telephone line. Since the commercialization of the Internet in the mid-1990s, its growth has been incredibly rapid (Yar, 2006).

Today, the word *cyber* and its relative dot.com are probably the most commonly used terminologies of the modern era (Sadhu, 2009). However, despite the numerous advantages embedded in this technological innovation, criminally-minded individuals are also capitalizing on the interconnectivity and network opportunities offered by the Internet to perpetrate different forms of crimes on the cyberspace. Internet technologies are facilitators for many kinds of infringements: theft; sabotage of information; copyright infringements; breach of professional secrecy, digital privacy, or intellectual property; dissemination of illegal contents; competing attacks; industrial espionage; breach of trademark laws; dissemination of false information; denial of service; various frauds; money laundering amongst others (Ghernaouti, 2013). Indeed, information technology resources have become the potential hostages of cybercriminals.

The Internet and cyberspace can both be considered criminalized zones. Individuals and private or public institutions, due to their presence on the Internet, contribute to the extension of cyber criminality because they increase the number of potential attractive targets for cybercriminals. Cyberspace, due to its characteristics, offers a favourable environment for the expression of criminality, be it classical or related to exploiting the possibilities generated by information technologies (Ghernaouti, 2013). Additionally, it allows users to operate remotely, via networks and hidden behind a screen. In fact, some individuals may stray across the boundary into criminal action without ever being fully aware of the criminal nature of their acts. The computer world offers cybercriminals the possibility of automating their activities. The rise in criminal actions, undertaken at distance through networks, against numerous targets and on a large scale, means that criminals can be ubiquitous in time and space. The dematerialization of transactions, communication facilities, and encoding and anonymity solutions provides connections between criminals without any physical contact, in a secure and flexible way. Therefore, they can organize themselves into teams and plan illicit actions to be performed either in a traditional way or through ICT (Ghernaouti, 2013).

With the emergence of the World Wide Web in 1993, along with a myriad of software applications, online content, and the beginning of high-speed/broadband Internet connections, computer crime evolved into computer-related crime and then what we know today as cybercrime (Yar, 2006). Therefore, any discussion on cybercrime would be incomplete without making reference to the Internet simply because without the latter, the former could and would not exist. It is the Internet that provides the crucial electronically generated environment in which cybercrime takes place (Yar, 2006). Moreover, the Internet cannot be viewed as simply a piece of technology, a kind of 'blank slate' that exists apart from the people who use it. Rather, it needs to be seen as a set of social practices – the Internet takes the form that it does because people use it in particular ways and for particular purposes (Snyder, 2001). 'What' people do with the Net, and 'how' they typically go about it, are crucial for understanding what kind of phenomenon the Internet actually is. Indeed, it is the kinds of social uses to which we put the Internet that create the possibilities of criminal and deviant activity (Yar, 2006).

Ghernaouti (2013) identified the following as the principal characteristics of computing technologies and of the Internet that are exploited for criminal ends:

- digitalisation of information: due to the fragility of digital information, it can be infinitely copied without one being able to distinguish the copies from the originals.
- attack or cybercrime has the capacity to pass unnoticed by its victims.
- virtual aspect of the people involved: there is no physical contact between people (victims and attackers). So, it is easier to harm people and to impersonate them without facing them.
- technologies (tools, services, hardware, software) have vulnerabilities that are exploited by the wrongdoers. The technologies are so complex that there are always vulnerabilities.
- network allows the putting into contact of people, systems and data: resources through the Internet are open to everyone and are accessible from all around the world. They constitute attractive targets, exposed to the criminal world that considers them as items of value and a source of direct (or indirect) enrichment.
- ever-increasing number of users: as the number of people and systems increases, the potential targets for cyberattacks rises, and the more cybercrime is fruitful. The number of users and interconnected systems creates a huge market for crime.
- existence of digital paradises: some countries have no laws relative to computing crime. In some countries, some malicious cyber-actions are not considered criminal. The criminals can therefore attack distant systems and commit computing offences

without fear of the consequences. The feeling of impunity is a driving force for criminals.

- difficulties, and sometime impossibility, of correctly identifying the origins and perpetrators of an attack decrease the risks for the criminal to be identified, immobilised and taken. Moreover, digital traces can be hard to gather, store, and use as evidence in a court of law.

As a group, all criminal activities being perpetrated via the Internet are referred to as cybercrimes. According to Wall (2001:3), the Internet has impacted upon criminal and/or harmful activity in three main ways. First, it has become a vehicle for communications which sustain existing patterns of harmful activity such as drug trafficking, and hate speech, bomb-talk, stalking and so on. Second, the Internet has created a transnational environment that provides new opportunities for harmful activities that are currently the subject of existing criminal or civil law. Third, the nature of the virtual environment, particularly with regard to the way that it distances time and space (Giddens, 1990), has engendered entirely new forms of (unbounded) harmful activity such as the unauthorized appropriation of imagery, software tools and music products, etc. Indeed, at the far extreme of this third category, the trans-jurisdictional, contestable and private nature of one of the harms indicates a scenario where there exists new wine, but with no bottles at all! Wall (2001:3).

In sum, cybercrime forms a continuation of classic criminality wherein the computer, with the programs and data that are inside and the networks it uses, can become both a target of an attack and a means of carrying one out. Cybercrime benefits its sponsors. Organized crime has quickly understood how to take advantage of information and communication technologies to communicate, organize, and identify both victims and opportunities, thereby increasing efficiency in drug and human trafficking, illegal commerce of rare or protected species, money laundering, selling of counterfeit products, or other economic crimes (Ghernaouti, 2013).

SELF-ASSESSMENT EXERCISE
Briefly discuss the emergence of the Internet.

4.0 CONCLUSION

The above discourse is expected to have exposed you to the origin of the Internet. How it was first created for the purpose of gathering military intelligence, and how it is later being employed for different purposes in other spheres of life. Thus, the Internet has significantly transformed human ways of life ranging from business to work, consumption patterns, leisure, health and politics. As a fastest-growing means of communication and information exchange, coupled with its global interconnectedness, the Internet has brought about the emergence of a new category of crime (cybercrime) and new category of criminals (cybercriminals).

5.0 SUMMARY

In this unit, effort has been made to explain the circumstances that led to the emergence of the Internet and how it has now become a veritable tool in the hands of cybercriminals for carrying out different types of crime at local, national, regional, and international levels.

6.0 TUTOR-MARKED ASSIGNMENT

1. Internet can be likened to a double-edged sword. Discuss
2. Critically discuss the relationship between the Internet and cybercrime

7.0 REFERENCES/FURTHER READING

Castells, M. (2002). *The Internet Galaxy: Reflections on the Internet, Business, and Society*.

Ghernaouti, S. (2013). Cyber Power: Crime, Conflict and Security in Cyberspace. EPFL Press.

Giddens, A., Duneier, M., & Applebaum, P. (2003). *Introduction to Sociology*. W.W Norton and Company, New York. London.

McQuade, S. C. (2009). *Encyclopedia of Cybercrime*. Green Wood Publishing Group.

Sadhu, A. 2009. The Menace of Cybercrime. Available at www.legalserviceindia.com

Siegel, L. (2007). *Criminology: Theories, Patterns, and Typologies (10th Edition).* Wadsworth Cengage Learning.

United Nations Office on Drugs and Crime (2013). *Comprehensive Study on Cybercrime.* UNODC, Vienna.

Wray, J. (2014). *Forrester Research World eReader Adoption Forecast, 2014 to 2019.* Cambridge, MA: Forrester Research.

Yar, M. (2006). *Cybercrime and Society*. Sage Publishers Ltd.

Zickuhr, K. (2011). Generations Online in 2010. Pew Internet and American Life Project. Available at www.pewinternet.org/Reports/2010/Generations-2010/Overview.aspx.

UNIT 2 THE MEANING OF CYBERCRIME

CONTENTS

1.0. Introduction
2.0. Objectives
3.0. Main Content
3.1 Cybercrime
4.0. Conclusion
5.0. Summary
6.0. Tutor Marked Assignment
7.0. References/Further Reading

1.0 INTRODUCTION

Cybercrime remains a topical issue at both national and international levels for scholars. It is also a major cause for concern for governments, multilateral organizations, and security experts. Therefore, it is very important to understand what constitutes cybercrime, the activities of cybercriminals on the cyberspace, and the dangers they pose to other Internet users.

2.0 OBJECTIVES

At the end of this Unit, you should be able to:

- define cybercrime
- know the meaning of cybercrime
- discuss the indices of cybercrime
- differentiate between cybercrime and conventional crimes

3.0 MAIN CONTENT

3.1 Cybercrime

Cybercrime is among the most dominant concepts in the 21st century. However, in spite of its popularity, it is a very difficult term to define because it is rapidly evolving, with new schemes and dimensions being created on a daily basis. Wall (2001) observed that the term ‘cybercrime’ is often used in political, criminal justice, media, public and academic discussions. ‘‘Cybercrime’’ is a broad term covering all the ways in which computers and other types of portable electronic devices such as cell phones and PDAs capable of connecting to the Internet are used to break laws and cause harm. A slightly more technical definition would be ‘‘the use of computers or other electronic devices via information systems such as organizational networks or the Internet to facilitate illegal behaviors'' (McQuade, 2006).

Cybercrime has come about and evolved with the Internet and other advances in IT that have afforded people new ways to cause harm in society. Indeed, this form of crime has been given different nomenclatures such as technological crime, high technology crime, high tech crime, economic crime, Internet crime, digital crime, or electronic crime, amongst other labels used by people to describe crimes committed with computers or other IT devices. These wide-ranging labels that are usually used to qualify cybercrime often create confusion for students and other people interested in knowing more about it or for the purpose of developing measures for its prevention. This is especially true given the fact that there are so many types of cybercrime and abuse of information systems. Some of these will be discussed in Module 2.

Gabrosky et al. (2001) defined cybercrime as the use of Internet services and ICT resources to further illegal ends, such as committing fraud, trafficking in child pornography, stealing of identities or violating of privacy etc. On their part, Hill and Marion (2016) viewed cybercrime as acts that involve criminal uses of the Internet or other networked systems to cause harm to others or some form of a disturbance. It can include any criminal activity—not only on computers, networks, or the Internet but also on mobile phones or other personal devices—that is intended to cause harm to others. Furthermore, Karofi and Mwanza (2006) defined it as a new type of white-collar crime facilitated by technological advancement (i.e) a crime actualized through the platform of the internet.

Thomas and Loader (2000) also noted that cybercrimes are computer-mediated activities which are illegal or considered illicit by certain parties and which can be conducted through global electronic networks. Moreover, the Parliament of the Commonwealth of Australia in 2004 contends that cybercrimes are criminal activities which use or take place through communication technology. The Council of Europe described cybercrime as applying to three categories of criminal activities. The first covers traditional forms of crime such as fraud or forgery, though in a cybercrime context relates specifically to crimes committed over electronic communication networks and information systems. The second concerns the publication of illegal content over electronic media (i.e., child sexual abuse material or incitement to racial hatred). The third includes crimes unique to electronic networks, that is, attacks against information systems, denial of service and hacking (Hill and Marion, 2016). These types of attacks can also be directed against crucial critical infrastructures and affect existing rapid alert systems in many areas, with potentially disastrous consequences for the whole society. Common to each category of crime is that they may be committed on a mass scale and with a great geographical distance

between the criminal act and its effects. According to McConnel (2000), cybercrimes differ from other terrestrial crimes in four major ways: they are easy to learn how to commit; they require few resources relative to the potential damage caused; they can be committed in a jurisdiction without being physically present and are often not clearly illegal.
Regardless of the way it is conceived, cybercrime represents a negative throw-up in the use of cyberspace in the new information age. A common denominator peculiar to this form of crime essentially involves the use of the Internet and other ICT resources to perpetrate acts that deviate from the normatively expected cyber behaviours. Similarly, the conceptualization of cybercrime raises also several key questions, like where do the criminal acts take place in the real and digital worlds and with the help of which technologies; why are damaging activities undertaken; and who are the actors perpetrating the deviant acts? The “where” of criminal activities, actors, and victims. When it comes to cybercrime, the location touches upon both the physical and digital domains (Viano, 2017).

However, the fairly clear borderlines and places common in the physical world are not available in the virtual one. Interestingly, there are still some borders that distinguish the physical from the cyber world. The keyboards, the screen, the arrow, the password, all fulfill a mediating role between the physical and the virtual worlds (Viano, 2017). But once within cyberspace, the idea of a border is much more undefined. In the cyber world, there are obviously no clear-cut. geographic boundaries like in the physical world (Johnson and Post 1996: 1379). Finally, Nhan and Bachman (2015) submitted that a broad definition of cybercrime will include three basic elements: (i) its perpetration via electronic networks; (ii) technology’s role; and (iii) the various applicable laws.

SELF-ASSESSMENT EXERCISE
Explain why cybercrime is difficult to understand.

4.0 CONCLUSION

From the discourse above, it is clear that cybercrime is a particularly difficult concept to define because of its changing patterns and fluid nature. However, regardless of the way it is conceived, a common denominator that is peculiar to this form of crime is that it essentially involves the use of the Internet and other ICT resources to perpetrate acts that deviate from the normatively expected cyber behaviour. Also, cybercrimes differ from the conventional crime in four major ways: they are easy to learn how to commit; they require few resources relative to the potential damage caused; they can be committed in a jurisdiction without being physically present and are often not clearly illegal.

5.0 SUMMARY

This unit has carefully discussed the concept of cybercrime. It highlighted some of the various definitions of cybercrimes as put forward by different scholars and international bodies. Equally, the characteristics of cybercrime which distinguish it from the conventional crimes are also explained.

6.0 TUTOR-MARKED ASSIGNMENT

1. With relevant examples, differentiate between cybercrime and conventional crimes
2. Discuss the three categories of cybercrime recognized by the Council of Europe

7.0 REFERENCES/FURTHER READING

Gabrosky, P.N, Smith, R.G, & Dempsey, G.2001. *Electronic Theft: Unlawful Acquisition in Cyberspace*. Cambridge University Press.

Hill, J.B. & Marion, N. E. (2016). *Introduction to Cybercrime, Computer Crimes, Laws, and Policing in the 21st Century*. Praeger Security International Textbook.

Johnson, D. R. & Post, D (1996). *Law and Borders - The Rise of Law in Cyberspace*. *Standford Law Review,* Vol. 48.

Karofi, U.A & Mwanza, J. (2006). Globalisation and Crime. *Bangladesh E-Journal of Sociology,3(1), 70-87.*

McConnell International Survey (2000), Cybercrime and Punishment? Archaic laws Threaten Global Information. Available at www.mcconnellinformation.com.mcconnellinternal

Nhan, J. & Bachman, M. (2015). Developments in Cyber Criminology. In M. Maguire and D. Okada (eds), *Critical Issues in crime and justice: Thought, policy and practice*. Pp. 209-228. Los Angeles: Sage Publications.

Thomas, D & Loader, B. (2000). Introduction – Cybercrime: Law enforcement, security and surveillance in the information age. In D. Thomas and B. Loader (Eds.). *Cybercrime: Law* *enforcement security and surveillance in the information age*. London Routledge.

Wall, D. (2001). *Crime and the Internet*. New York: Taylor and Francis Group.

UNIT 3 EVOLUTION OF CYBERCRIME (PRE 1970-2000)

CONTENTS

1.0 Introduction
2.0 Objectives
3.0 Main Content
3.1 Evolution of Cybercrime (Pre 1970-2000)
4.0 Conclusion
5.0 Summary
6.0 Tutor- Marked Assignment
7.0 References/Further Reading

1.0 INTRODUCTION

The direction, impact and magnitude of cybercrime may not be adequately understood without discussing how it has evolved from the simple hacking that was witnessed some over 50 years ago to the complicated cyber terrorism and cyber espionage that are staring at us in the face today. Cybercrime has now become an integral part of the cyberspace that is threatening the daily functioning and activities of individuals, business, government and organizations. Cybercriminals can now send virus code over the Internet, reach out and con people, destabilize businesses, governments and organizations from a distance.

2.0 OBJECTIVES

At the end of this Unit, you should able to:

- track the five epochs in the evolution of cybercrime
- discuss the forms of cybercrimes peculiar to each of the five epochs
- narrate the major cybercrime incidents that have been recorded over time

3.0 MAIN CONTENT

3.1 Evolution of Cybercrime (Pre 1970-2000)

The increasing rise in the incidence of cybercrime has placed it on a high pedestal globally. Cybercrime occupies a significant position in the criminological discourse of the 21st century. However, despite it is relatively recent ubiquity, the emergence of cybercrime predates the contemporary time. Indeed, the origin of cybercrime has been traced to the early 1950s. In fact, McQuade (2009) asserts that the abuse and misuse of computer systems has existed since mainframe computers were first invented during the 1940s and 1950s as a means to improve military munitions and then rocket guidance systems. As computers became more necessary for research and communications within academic institutions, military organizations, and financial institutions, pranks and pranksters inevitably came onto the scene. Originally these pranksters were mainly university students who possessed tremendous curiosity about computers and the ways in which they could be used to solve problems. Eventually, during the 1960s, with the invention of ARPANET and then the Internet, and as computers located in colleges and universities throughout the United States interconnected with those located in government agencies and businesses, pranks and the abusive use of computers and computer networks became more common and harmful (McQuade, 2009). The timeline as provided by Hill and Marion (2016) on the history of computer crime aptly captured how cybercrime has evolved over the past few decades.

3.2 Pre-1970 Era

The Internet can be traced back to the events in the 1950s when the United States of America was preoccupied with the Cold War and the Soviet Union. In 1957, the Soviets launched the satellite *Sputnik* into space, thereby winning the space race. As a way to advance American technology and prevent the Soviets from getting any further ahead, in 1958 the U.S. government created a new agency, the Advanced Research Projects Agency (ARPA), with the responsibility of developing new technologies to be used for military purposes.

In 1962, a new division of ARPA was formed, the Information Processing Techniques Office, and a scientist from MIT, J. C. R. Licklider, was appointed to lead the new agency. He proposed a network of interconnected computers that scientists could use to share research and work jointly on projects. The idea lay dormant for a time as few people had the expertise to carry out the plans. The next director of the agency picked up the idea again and formed the Advanced Research Projects Agency Network (ARPANet), an early precursor of the Internet.

Ray Tomlinson, an engineer, was the first person to send an email over the ARPANet. He was also the first person to use the @ symbol in one of those communications. In the 1960s and 1970s, there was little computer crime as the technology was neither widely available nor used by the general population. At that time, computer use was largely restricted to the military and to researchers at universities and other scientific labs. Most unauthorized hacking events were simply pranks carried out on computer systems at universities by inquisitive students who did not intend to cause any harm. The viruses they left behind were easily identified and removed. These hackers sought to discover kinks in the system and then use that information to make improvements. The events generally caused minimal damage to computers or data, if any at all.

The entire purpose of hacking in those days was simply for fun—to prove that a person had the technological savvy and skills to break into a supposedly secure system. At the time, there were few laws that criminalized these activities, so they were not considered to be crimes, and few people were prosecuted for these acts. In fact, offenders often signed their names to a virus. Some may argue that the first person to recognize and study computer crime and security issues was Donn B. Parker. During the early 1970s, as the Internet was evolving, Parker researched computer crime and security issues. He became a senior computer security consultant at the Stanford Research Institute and, in that position, wrote the first federal manual on computer crime, Computer Crime—Criminal Justice Resource Manual, in 1970. This was a manual for law enforcement officials, who were beginning to see more complaints of computer crimes.

3.3 The 1970s Era

During the 1970s, technology was rapidly advancing. Cybercriminals were likewise learning more about computer systems and their vulnerabilities, all the while honing their hacking skills. Throughout the decade, hackers' intentions and purposes were quickly changing. No longer were hackers finding ways into systems for fun; now they intended to cause harm. One of the first computer viruses designed to damage systems appeared in 1971. At this time, a virus known as Creeper was released in the ARPANet. A computer infected with the virus displayed a message on the screen indicating that the system was infected and the identity of those responsible for creating the virus. The first computer crimes also appeared during the 1970s. The first types of computer crimes to be recognized were computer intrusions and fraud.

Also, one of the first identified cybercrimes occurred in 1973, when a chief teller at a Union Dime Savings Bank embezzled money from the company by manipulating account data in the bank's computer system. In the 1970s the use of computer hacking expanded and computerized phone systems became a prime target of "phreakers." These technologically savvy people could break into a system, discover the correct codes and tones, and get free long-distance service. One of those phreakers, John Draper (also known as Cap'n Crunch), discovered that a toy whistle he found in a box of Cap'n Crunch cereal was the same frequency as the AT&T phone network. Using the free whistle, he was able to configure the system so that thousands of people got free phone calls from AT&T. While computer crimes like Draper’s were slowly emerging, the majority of the population remained largely unaware of crimes committed via computers and the Internet. Consequently, the impact of these events went mostly unnoticed by the general public. However, to those who were more aware of computers and their increased vulnerabilities, it was clear that there was a potential for similar crimes to be committed at any organization that relied on computers. In response, state legislators began to respond to the newly emerging crimes. They proposed and debated new legislation that sought to define specific computer operations as illegal. The first computer crime law that focused on cybercrime was the Florida Computer Crimes Act of 1978. The law was passed after it was discovered that employees at the Flagler Dog Track had used a computer to print fraudulent winning tickets. The new law defined all unauthorized access of a computer as a crime, even if the person committing the crime had no malicious intent. New laws also meant that offenders could be, and were actually, arrested and prosecuted for computer crimes, but because of the novelty of these crimes (and partly because criminal justice personnel were unfamiliar with the technology), there were few actual prosecutions for computer crimes.

3.4 The 1980s Era

By the 1980s, computers and technology had become more mainstreamed. The Internet was rapidly expanding, and computers were being used in more businesses, government offices, and homes. Companies were beginning to use the Internet so they could reach out to users not only in the United States but also internationally to expand their markets. Because computers were becoming more widely used, computer crimes were becoming more frequent. Moreover, offenders were also changing. Their intent was no longer to break into a computer system just for the fun of it. Many viruses and hacking attacks were now meant to cause critical harm to computer systems or result in theft of data. The crimes quickly became serious threats to businesses, financial institutions, and government offices. As crimes grew in intensity, courts began to recognize the dangers of computer crime and punished offenders with harsher sentences in terms of lengthier prison terms and higher fines. As a result, the Federal Bureau of Investigation (FBI) was assigned the task of overseeing credit card and computer fraud. During this period, some significant trends became apparent, such as the growth of new viruses, more convictions for those guilty of computer crimes, the emergence of hacking groups, and the use of cybercrime as entertainment, the publication of hacking magazines, and an international perspective.

The first widely known viruses circulated in 1981. The Apple I, II, and III viruses, for example, targeted the Apple II operating system. They first appeared at the computer system of Texas A&M University and spread to other users when they downloaded pirated computer games. This action involved two crimes: the release of the computer virus and the pirating (or theft) of the software. Similarly, the 1980s era also witnessed the prosecution of Ian Murphy, the first person ever convicted of a felony for a computer crime. In 1981, Murphy and three of his friends broke into the AT&T computer system and changed the internal clocks. At that time, phone rates varied depending on the time of day. Phone calls made in the evening were cheaper than those made during the day. By changing the clocks at the company, users were charged incorrect rates for phone usage. Some callers using the phone during peak day times were charged late-night, discounted rates. Some who made phone calls in the evenings to take advantage of lower rates were charged higher rates. Clearly, this cost the company money and frustrated users. Murphy was eventually convicted of computer crimes and sentenced to 1,000 hours of community service and 30 months on probation.

Equally, one of the first arrests for computer hacking also occurred around this time. In 1983, a group of teenagers who called themselves the 414s (after their area code in Milwaukee, Wisconsin) hacked into the computer systems of the Memorial Sloan Kettering Cancer Center in Manhattan, New York, and the Los Alamos National Laboratory in New Mexico. They were quickly arrested by FBI agents and charged with multiple counts of breaking into computer systems. One teen was granted immunity from prosecution in exchange for cooperating with authorities. The others were each given five years of probation. This was a landmark case because it was one of the earliest incidents of an arrest resulting from hacking. At the time, there were few laws regarding cybercrime, and most law enforcement agents did not have the knowledge to investigate allegations of computer crimes. Moreover, until this case, most businesses did not give much credence to the need for security measures. Since cybercrime was not fully understood by business community, and many in the information technology community did not recognize the potential for harm from hacking. Throughout the 1980s, computer crime continued to advance, as did the punishments for it. In 1986, Herbert Zinn (aka Shadow Hawk) was a teenager who lived in New Jersey. He hacked into the computer systems of AT&T to steal computer data. Zinn was eventually convicted and sentenced to nine months in jail.

Furthermore, during this era, people who enjoyed hacking into computer systems, either for fun or for other reasons, began to join groups as a way of advancing their knowledge of the art of hacking. In 1981, a group of German computer enthusiasts who had a strong radical political orientation formed the Chaos Computer Club in Hamburg, Germany. They were able to hack into the German post office and, through the exploitation of security flaws, transfer a sizable amount of money into their own bank accounts. They soon returned the money to the bank but used the opportunity to make a political statement regarding ineffective government action regarding cybersecurity. The group held meetings called the Chaos Communication Congress. Similarly, two groups of hackers, the Legion of Doom (LOD) and the Masters of Deception formed in the United States (4).

The LOD hacking group, founded by Vincent Louis Gelormine under the alias “Lex Luthor,” got its name from popular DC comics; members were a group of phone phreakers who later became hackers. The members of LOD enjoyed the process of hacking, supported others who wanted to get involved, and were eager to share their knowledge of hacking. They even published the Legion of Doom Technical Journal, which contained guiding principles, code, and programming examples as well as other information of interest to hackers around the world. In the late 1980s, LOD actually helped law enforcement by restraining malicious hackers. Gelormine had a reputation for attracting the best hackers to his group. The members of LOD were flagrant and enjoyed the publicity they sometimes received for their actions. However, a spat between two members, Mark Abene (aka Phiber Optik) and Chris Goggans (aka Erik Bloodaxe), an editor of Phrak magazine, led to significant change. Abene left LOD and, along with some friends, formed a new group they called the Masters of Deception (MOD). Also helping to form the group was Eli Ladopoulos (aka Acid Phreak) and Paul Stira (aka Scorpion). MOD often disagreed with the members of LOD, resulting in a two-year dispute known as the “hacker war. Throughout the dispute, hackers from both groups attacked each other using the Internet and telephone networks. They were jamming each other’s phone lines and monitoring each other’s computer calls. Allegedly, members of LOD went so far as to establish an Internet security consultancy group that was available to assist corporations who had been victims of MOD. Members of the groups sometimes switched their allegiance.

Later, a third group appeared on the hacking scene. The Cult of Dead Cow (cDc) was originally founded in Lubbock, Texas, in 1984 by Swamp Ratte (“Grandmaster Ratte”), Franken Gibe, and Sid Vicious. The members of cDc encouraged others to hack. Over time, the group’s members established a secret elite group, the Ninja Strike Force. While the other groups fought with each other, cDc continued to grow its membership and increase interest in hacking. The cDc was known for its use of humor, and members would sometimes wear clothing with amusing cartoons such as that of a crucified cow. In its later years, the cDc became an important proponent of hacktivism, or using hacking techniques for political purposes. The group also released numerous hacking tools, of which Back Orifice (BO) and especially Back Orifice 2000 (BO2K) were notorious examples. BO2K was a Trojan horse that allowed remote control of infected machines. In the early 1990s, members of LOD and MOD were indicted for their illegal hacking activities. Abene was sent to prison for one year after pleading guilty in federal court to conspiracy and unauthorized access to federal interest computers. Many members of the hacking community protested Abene’s punishment, and upon his release, he was named one of New York City’s 100 smartest people. Most cDc members remained free from punishment (Hill and Marion, 2016).

3.5 The 1990s Era

The 1990s was a period of significant transition in the evolution of cybercrime. By this time, the use of the Internet continued to grow, and it was now commonly used in schools and homes. More businesses continued to put their information online because they now had the ability to conduct business in the global economy, 24 hours a day, seven days a week. Geographic boundaries were no longer prohibitive for businesses, and they took advantage of their extended reach. Consequently, the online economy expanded.

According to the Digital Research Initiative, e-commerce first began on August 11, 1994, when NetMarket made the first online transaction. The first item purchased through a website protected by commercially available data encryption technology was the CD Ten Summoner’s Tales by Sting. The buyer used a credit card and paid $12.48, plus shipping costs. Since the Internet was more accessible to a wider band of people during the 1990s, there were more attempts to commit crimes. The term “cybercrime” became more commonly used as people became more aware of hacking, viruses, and other forms of computer crime. Cybercriminals took advantage of vulnerabilities in computer systems around the globe.

As cybercrime and malware became more widely recognized and feared by users, antivirus programs were developed that were more capable of detecting harmful malware. In turn, this meant hackers and criminals needed to increase their technical skills in order to carry out their attacks. They started to make malware that was more complex, so that it went undetected by antivirus programs. One method criminals developed to subvert anti-malware programs was polymorphism. In this type of a virus, each new iteration of the malware evolves, so that a new characteristic will appear that does not affect the original code. In 1997, tools that would allow unskilled people to carry out computer crimes were made readily available online. That year a utility called AOLHell was released. The free application allowed virtually anyone to launch attacks on America Online (AOL). For days, AOL chat rooms were clogged with spam, and the email boxes of AOL users were overwhelmed with spam. Since that year, many more such tools have been released on the Internet.

Despite the increased security measures, the number of cybercrimes exploded during the 1990s, and the crimes that took place were far more devastating than previous crimes. The number of financial crimes committed through computer systems increased as many computer hackers shifted their online activities to stealing credit card numbers, passwords, PIN numbers, and other personal data that could then be used to commit crimes like identity theft. Illegitimate applications of email grew rapidly, generating lots of unsolicited commercial and fraudulent email, or spam. Identity theft was rising by the late 1990s, causing great concern for consumers and law enforcement alike. It quickly became apparent that many hackers no longer broke into computer systems for the challenge or a sense of thrill, and they did not seek attention for their crimes as hackers did in the 1980s. The new group of hackers was much more dangerous. They sought to make a profit and cause harm to others. Some key events occurred in the 1990s that pointed to the dangers of cybercrime. These included new viruses, more cases of hacking, cybercrime as entertainment, government action, hacking groups, and international events.

One virus that was transmitted during the 1990s was the Michelangelo virus, which would install itself on a computer but then remain dormant in an infected computer for many weeks before attacking. The virus was written to trigger on Michelangelo’s birthday and attacked the boot sector of the hard drive or floppy drive. For the most part, the virus left data largely untouched, so it did not cause much damage. In 1999, the Melissa virus was released. Created by David Smith, it caused an estimated $500 million in damages. Smith was eventually convicted of writing the virus and given a five-year prison sentence. This case was the first to have caused so much damage, but it is also key because of the sentence the offender received. This showed that courts were beginning to take computer crime more seriously and to sentence perpetrators accordingly.

Also, the practice of hacking into computer systems continued in the 1990s. In 1994, a 16-year-old boy from the United Kingdom known as Data Stream hacked into many government sites, including Griffiss Air Force Base, NASA, and the Korean Atomic Energy Research Institute. Even though his victims were located in North America and Asia (and he was located in Europe), he was identified by Scotland Yard officials.

This case was critical because it clearly identified the need for international cooperation between law enforcement agencies when it came to investigating cybercrime. Clearly, cybercrime was indeed global and no longer bound by geographic borders.

Another case that showed the growing importance of international cooperation in cybercrime occurred in 1995. Vladimir Levin, a graduate of St. Petersburg Tekhnologichesky University, was arrested and charged with being the head of a group of Russian hackers. The group allegedly stole almost $10 million from Citibank. Levin was arrested by Interpol at Heathrow Airport and extradited to the United States where he was convicted of the charges against him. He was sentenced to spend three years in prison and pay Citibank $240,015, the amount he profited from his crime. Hacking in the United States was not only done for profit but also for other reasons during the 1990s. One of those reasons was political. In 1996, a computer hacker associated with a white-supremacist group disabled a Massachusetts Internet service provider (ISP) and damaged data on its system. The ISP attempted to stop the hacker from sending out worldwide racist messages under the ISP's name. The hacker signed off with the threat, "You have yet to see true electronic terrorism. This is a promise." While this attack caused very little damage, it was an example of how some hacking events were ideologically driven and were done to send a message in support of the hacktivist. Hackers also broke into systems as a way of damaging a business.

In 1997, the Network Solutions Internet domain registry was hacked by a business rival, causing the company a great deal of damage and havoc. Eugene Kashpureff, the owner of a competing business called AlterNiC, eventually pleaded guilty to carrying out the offense. This case is of interest because it was a clear example of how hacking could be used in a dispute between rival businesses. One company used hacking to subvert the business practices and success of a competing business. This was clearly a case of corporate warfare that was carried out through the Internet (Hill and Marion, 2016).

3.6 The 2000s Era

By the 2000s, the majority of people in different parts of the world used technology regularly. Many people's lives were influenced by computers in some way on a daily basis. Computers impacted business, education, health care, banking, and research. The nation's critical infrastructure relied on computers to exist. At the same time, cybercrime continued to rise, and large-scale global malware attacks continued by the use of specific targeting of end-user systems. Cybercriminals continued to use email and websites to deploy malware. Advanced persistent threats became a regular concern, because they posed a threat to the intellectual property and financial assets of companies and nations. New threats at this time focused on mobile operating systems, such as cell phones. As these networked devices became common, criminals were actively developing new technology aimed at exploiting them. New laws have been passed at the federal, state, and international levels to deter cybercrime, but they often lag behind emerging technology, and cybercriminals stay one step ahead of the legislation. Businesses and homes need to have security systems installed to prevent becoming the victims of an attack.

In 2003, Microsoft went so far as to announce bounties for anyone who aided in capturing hackers, virus writers, and various other computer criminals. It was an interesting way to combat computer crime. Equally, social networking sites became very popular and widely used methods to communicate with family, friends, and business contacts in the 2000s. This has led to increases in crimes such as cyberbullying and harassment. A particular crime occurred in 2008 in which a mother of a teenage daughter, Lori Drew, created a fake MySpace page as a way to bully another teenage girl who happened to be her daughter's rival. The target of Drew's attention, Megan Meier, committed suicide as a result of the things Drew posted on the account. Law enforcement sought to hold Drew accountable for her actions and for the death of Meier. Drew was charged with crimes under the Federal Computer Fraud and Abuse Statute, even though the law does not address cyberbullying. In September 2009, U.S. District Judge George Wu dismissed the case. This was one of many examples of how people were using social media for criminal purposes. Another example happened in 2009, when Brian Hurt used Craigslist to hire a prostitute to come to his home. When she arrived at his house, he shot and killed her (Hill and Marion, 2017). This particular incident was similar to a case that occurred in Nigeria where a lady named Cynthia Osokogu was allegedly raped, robbed, and murdered by two Nigerian university undergraduates, Nwabufor Okwumo and Ezekiel Odera, for the after luring to Lagos from Abuja under the guise of sealing a business transaction after initially making friend with her on an online social media network, Facebook (Ogbo, 2012; Usman, 2012).

SELF-ASSESSMENT EXERCISE

Write a brief note on the cybercrime events that dominated the pre-1970 era.

4.0 CONCLUSION

The above discourse on the analysis of the evolution of cybercrime clearly demonstrates that it is a form of crime that advances with information and communication technology (ICT) development. The implication of this is that the magnitude and direction of cybercrime, as well as the levels of sophistication of cybercriminals may be difficult to predict and gauge. In essence, cybercrime is a form of crime that is not only fluid and wide-ranging, but also does changes with time.

5.0 SUMMARY

In this unit, attention had been devoted to the trajectory and metamorphosis of cybercrime from its earliest stage to its advanced stage as we have it today. Also, information was provided on some earliest cases of cybercrime attacks. In addition, attention was also devoted to some notable individuals who played important roles in the emergence of cybercrime.

6.0 TUTOR-MARKED ASSIGNMENT

1. The 1990s was a period of significant transition in the evolution of cybercrime. Discuss.

7.0 REFERENCES/FURTHER READING

Hill, J.B. & Marion, N. E. (2016). *Introduction to Cybercrime, Computer Crimes, Laws, and Policing in the 21st Century*. Praeger Security International Textbook.

McQuade, S. C. (2009). *Encyclopedia of Cybercrime*. Green Wood Publishing Group.

Ogbo, P. (2012). Police Parade Killers of General’s Daughter, Daily Times, Aug, 23.

Usman, E. (2012). How ex-General’s daughter, Cynthia, was killed by face book ‘friends’. *Vanguard*, Aug. 21.

UNIT 4 TECHNIQUES AND TOOLS DEPLOYED FOR CYBERCRIME

CONTENTS

1.0 Introduction
2.0 Objectives
3.0 Main Content
3.1 Techniques and Tools Deployed for Cybercrime
4.0 Conclusion
5.0 Summary
6.0 Tutor- Marked Assignment
7.0 References/Further Reading

1.0 INTRODUCTION

Cybercriminals are employing different tools and techniques to facilitate their illegal and clandestine activities on the cyberspace. Internet Service Providers, internet architecture, individual and corporate internet users, as well as government agencies are among the most frequently targeted by cybercriminals. Without certain specialized tools and techniques, cybercrime may be difficult for cybercriminals to perpetrate. Hence, tools and techniques constitute important wares for cybercriminals. Some of the tools and techniques commonly deployed for the perpetration of cybercrime shall be discussed in this unit.

2.0 OBJECTIVES

At the end of this unit, you should be able to:

- explain the basic and advanced tools and techniques for cybercrime
- understand how cybercriminals deploy these tools and techniques on the cyberspace

3.0 MAIN CONTENT

3.1 Techniques and Tools Deployed for Cybercrime

Cybercrime perpetration requires the use of some techniques and cyber-tools. Although to be effective, such techniques and tools need to be sophisticated, at least to overcome basic levels of security measures. However, they do not necessarily need to be highly sophisticated (Akhgar and Brewster, 2016). With a global network of potential targets, attackers can easily look for the weakest link and benefit from poor security in one place or another. But more importantly, tools are available also to would-be criminals who have no technological expertise or skills, through the existence of a large underground marketplace where hacker tools are traded, in much the same way as legal online marketplaces function (along with vendor rating systems and helpdesks) (Akhgar and Brewster, 2016). The existence of such black markets was a primary reason to criminalize the misuse of devices in the Cybercrime Convention and Directive 2013/40/EU1, but the effect of this penalization on the factual easy availability of hacker tools remains to be seen. Here, five major types of techniques and tools commonly deployed for the perpetration of cybercrime are discussed.

3.2 Botnets

‘‘Bot networks,’’ or botnets, are collections of computers that have traditionally been under the control of a single entity, usually without the knowledge or consent of the owners or users of those computers (McQuade, 2009). The attacker exploits security weaknesses, generally in a computer connected to the Internet, to place small programs called daemons which run in the background of the host computer, unknown to the third party (Clough, 2010). Individually affected computers are running software known as a ‘‘bot’’ (from ‘‘robot’’), and these infected computers are often referred to as ‘‘bots’’ or ‘‘zombies.’’ Botnets are used by the controlling entity, sometimes known as a ‘‘botherd’’ or ‘‘botherder,’’ to perform one or more functions on computers owned or used by other people.

Bots have a central role in the cybercriminal world (Ghernaouti, 2013). Botnet owners either launch attacks themselves, or they rent their network of zombie computers to any third party who wants to launch an attack. Bot networks are thus a real threat to all Internet-connected systems. Various attacks can be performed by cybercriminals using bots and botnets, such as: drowning websites and e-mail servers; stealing identities by obtaining information from the victim; proxying network traffic such as SMTP and HTTP; phishing, by helping to identify potential victims and hosting fraudulent websites; advance fee fraud; extortion, by threatening organizations with a DDoS attack if they do not pay a certain amount of money; hosting illegal data and installing malware, such as a backdoor, to maintain access after the exploit (Ghernaouti, 2013).

Expert botherds are able to distribute functions across individual computers running a bot (such as cracking passwords) or have them work in concert (e.g., engaging in a denial of service attack). Both programs were initially created in the early 1990s by Internet Relay Chat (IRC) users to provide automated responses while they were away from their computers, to attack and defend control of IRC channels, as well as to perform other tasks. By 1999, various tools such as Trinoo, Tribal Flood Network, Stacheldraht, and Shaft were developed to engage in distributed denial of service (DDOS) attacks, often against IRC servers (McQuade, 2009).

In 2000, these DDOS tools were merged with worms and rootkits in order to automate the rapid compromise of systems used to launch attacks. By 2002, the IRC control functionality of the original bots was merged with these tools, and bots became a general-purpose platform for compromising systems, taking control of them, and using them for a variety of tasks beyond DDOS (McQuade, 2009). The DDOS capability became less common as bots began to be used by criminals for economic gain. Some botnets have begun to use other communications mechanisms besides IRC, including peer-to-peer (p2p) protocols that eliminate dependence upon a botnet controller at the expense of losing the ability to send commands simultaneously to all bots. Botnets have also become one of the primary tools of criminal activity used on the Internet, and botnet activity is often motivated by the desire of cybercriminals to make money.

Botnets provide a technology infrastructure that, in conjunction with a creative division of labor, disperses risks faced by online criminals, allowing them to grow their operations to larger scales with minimal fear of being identified, arrested, and prosecuted. Criminal activity using botnets has been split into multiple roles, where different individuals and groups can participate in separate tasks. This allows specialization both in particular activities and for the dispersal of risk. Some of the common roles include:

- writing the malware used to compromise systems;
- compromising popular Web servers and using them to deploy that malware;
- collecting bots into botnets (the ‘‘botherder’’ role);
- using botnet-provided services to distribute data (such as spam or malware), collecting data (such as financial account information and passwords), or processing information (such as password cracking);
- selling captured account information;
- using captured account information to engage in credit card fraud or to create forged ATM cards;
- using forged ATM cards to empty bank accounts; and
- laundering the proceeds of credit card fraud by reselling purchased items (McQuade, 2009).

3.3 War driving

War driving is a technique involving driving around with a portable Wi-Fi device (laptop, tablet, smartphone, or custom device) searching for insecure wireless networks. War drivers often use specialized antennas to extend their reach. Software is available for download that automates the practice. Combined with global positioning systems, war driving software can automatically generate maps that locate Wi-Fi network sites (Waschke, 2017). War driving is legal in most places, although some local laws outlaw it. The step usually taken after finding available Wi-Fi sites is illegal. Open networks discovered on a war drive that are not encrypted and secured with a password can easily be accessed without authorization from the owners. This is illegal. Criminals war drive, or use maps produced by war drivers, to gain unauthorized access to Wi-Fi networks. They may do this to steal Internet access, gain illicit access to passwords and data by hacking into devices on the Wi-Fi network, or hide their identity by communicating from a location that cannot be traced to them (Waschke, 2017). The obstacles to these searches do not mean that a search is pointless, but they are challenging

3.4 The Onion Router (TOR)

Tor was developed to offer privacy, confidentiality, and anonymity on the Internet. In the mid-1990s, the United States Naval Research Laboratory scientists and engineers generated the Tor concepts and architecture for the protection of online secret communications (Waschke, 2017). The Tor project continues to be developed and maintained through grants from various agencies of the U.S. government, contributions from individuals, and other organizations. The basic principles behind Tor are a network of volunteer servers and repeated encryption of the information associated with the message. Messages are routed and repeatedly encrypted on random paths through the Tor server network. It is called “the onion router” because pealing back one layer of encryption reveals another layer, like pealing an onion.

Although Tor has proven to be penetrable with sufficient resources and effort, the exceptional effort required makes Tor-protected network traffic much more private than normal Internet traffic. The Tor browser is a free download. A moderately savvy computer user can be up and running on Tor in a short time. Tor leads a double life. It preserves privacy and prevents intrusion into both legitimate and illegitimate activities. Tor protects both foreign correspondents and terrorists who threaten them. Individuals use Tor to protect their privacy from intrusive business interests and Tor prevents criminals from spying on law enforcement communications. Tor also protects intellectual property from prying by competitors and foreign nations. At the same time, Tor prevents law enforcement from spying on criminals, terrorists, and antagonistic foreign nations (Waschke, 2017).

Cybercriminals who wish to remain anonymous are using ‘‘the onion router’’ (TOR) method, which is a network of peer computers that will scatter traffic in near real time to routing hosts. Through the use of this tool, a person can set up a computer system to go through TOR capable of routing traffic through another TOR site. By routing traffic through a series of onion router connections being hosted in different countries, cybercriminals can elude law enforcement or other investigators by diverting their real whereabouts and identity. TOR systems can be configured to transmit data very quickly and retain it for only short periods of time, while also changing connection interface requirements. So, the ‘‘state’’ of where an offender is and how they are able to transmit traffic back and forth and all around the world is kept for only a short time and changes constantly (Waschke, 2017). Consequently, a cyberattack launched through TOR may appear to be coming from all over the Internet. If cleverly used by cybercriminals, these tools can be a power source for intelligence gathering about information systems, organizations targeted for economic espionage, or people whose confidential information will then be used to make them victims of identity theft.

3.5 Malware

Malware is a general term for a variety of harmful software specifically designed to attack computer systems, networks, or data (McQuade, 2009). The term was derived by combining the words ‘‘malicious’’ and ‘‘software,’’ and it is used to describe computer viruses, Internet worms, keystroke logging programs, rootkits, spyware, botnets, and the like. Malware can be the cause or the source of other types of attacks, such as denial of service attacks, phishing, and spam. While there are many different kinds of malware, all malware has one thing in common: its existence is unwanted, unknown, or hostile to the end user or owner of the computer system running it. A program that collects data on a personal computer can therefore be considered malware—but only if its existence is unwanted, unknown, or hostile. So, while a spyware program that collects information on Internet activity without the knowledge or consent of the computer’s owner would be considered malware, the ‘‘History’’ folder in the Windows operating system would not (McQuade, 2009). And while keystroke loggers—programs that collect and store all of the keystrokes made on a computer—are commonly considered malware, many legal and legitimate software programs that offer parents the ability to monitor their children’s computer habits would not be considered malware, even though they too may log and store keystrokes.

Most forms of malware become installed on computer systems after an inadvertent action of an unsuspecting computer user. Viruses, spyware, and rootkits can compromise a computer through an infected email or an email attachment being opened, or by an unsuspecting user visiting a phony Web site cleverly disguised as a legitimate site. Worms are the one type of malware that can propagate itself through flaws or holes in a computer's operating system, i.e., without any end user action at all. Most people use the term ''virus'' instead of ''malware,'' and while viruses are a specific type of malware, not all instances of malware are viruses (McQaude, 2009).

Although technically distinct, the line between viruses and worms is increasingly blurred (Clough, 2010). Both are programs that infect a computer by being copied and then performing a programmed function. These functions can vary from the very simple, such as displaying a message on a particular date, to deletion or modification of data or installation of other malware such as Trojans or bots. Some malware, known as 'logic bombs', is programmed to activate on a certain event occurring, such as a specific date or when a particular program is loaded. The distinction between viruses and worms is that a virus must infect another program. Worms are similar to viruses but are self-replicating; that is, they do not need to infect another application (Clough, 2010).

3.6 Social Engineering

Social engineering is the act of manipulating a person or persons into performing some action. In the realm of computer abuse, this most commonly takes the form of, but is not limited to, convincing victims to divulge personal, financial, or security-related information or to grant access to computer systems or physical environments where such information is stored. Use of trickery and fraud is common in such attacks (McQuade, 2009). Attacks can take place in person, over the phone, through the Internet (including email, instant messaging, and the like), through hard copy correspondence, or through any other means of communication. While computer crime is often thought of in terms of purely technical exploits, this mind-set is dangerous and shortsighted.

Social engineering plays a role in many different kinds of computer abuse and crime. It is a popular attack vector, or means of attack, among hackers and others (McQuade, 2009). A common example is the practice of phishing, where an attacker or attackers send out email, instant messages, voice mails, or other communique's disguised to look like they came from a legitimate source, such as a credit card company, bank, or business. The fraudulent message generally requests that victims ‘‘verify’’ personal information such as account numbers or passwords and often direct them to enter such information into equally fraudulent Web sites. The attacker can then use the personal information to commit fraud, identify theft, and other crimes (McQuade, 2009). However, not all social engineering techniques require a technological component.

Another common example of social engineering is pretexting. Pretexting involves the use of an invented identity and/or scenario (the pretext) to persuade a person to provide sensitive information or access to sensitive computer systems and the like. An attacker calling a victim and pretending to be from his bank or calling an employee of the bank and convincing them that he is, in fact, the victim would be two examples of this type of attack. Pretexting is generally conducted over the phone and requires prior research on the part of the perpetrators (FTC, 2006). Pretexting is often used to convince businesses to release customer information and is sometimes used by private investigators to obtain things like banking records, phone records, and other personal information (Bangerman, 2006). Social engineering attacks generally follow a distinct pattern. As a first step, the perpetrator identifies the people, facilities, and or information system that are to be attacked. In the second step, the attacker conducts research and collects intelligence on his or her target in order to discover security weaknesses. In the third step, the attacker develops rapport with persons who control access to the targeted information, computing system, or facility. In the fourth step, the attacker violates the trust of those persons, and in the fifth step, uses the information collected to commit one or more abuses or crimes (McQuade, 2006).

3.7 Sniffer

A sniffer is a device that is used to capture network traffic. Depending on the size and activity of the network, sniffers may collect an enormous amount of data (Maras, 2015). Network traffic can reveal data about the source, destination, and content of communications. Sniffers have been used for both legitimate and illegal purposes. Notably, criminals have used sniffers to steal passwords and personal information. Sniffers have also been used legitimately to capture data and inspect it for any potential attacks or intrusions. Indeed, sniffers can provide a computer forensics investigator information that can identify the suspect (or suspects) in an attack, the modus operandi of the suspect, and the full content of data of incoming and outgoing network traffic (National Institute of Justice, 2007). Wireshark is an example of a sniffer program that captures network traffic in real time and records it (National Institute of Justice, 2007). This tool is not designed to alert authorities of any suspicious activity, so it is not considered a form of intrusion detection. Instead, it is designed to troubleshoot network problems and is used to perform both live and offline analysis of captured network data (Maras, 2015).

SELF-ASSESSMENT EXERCISE
Explain how tools and techniques are indispensable to the perpetration of cybercrime.

4.0 CONCLUSION

Tools and techniques are indispensable for cybercrime perpetration. The recorded advancement in the area of information and communication technology has also presented cybercriminals with the opportunity to continually innovate with new techniques and develop sophisticated tools to perpetuate illegal activities on the cyberspace. Cybercriminals have become sophisticated with the use of internet tools and techniques designed for the purpose of conducting cybercrime ranging from high tech crime against computer hardware and software to cyber enabled crime against real word entities, such financial crimes, crime against children, cyber terrorism, cyber pornography, cyber espionage, amongst others.

5.0 SUMMARY

In this unit, students have been exposed to the importance of tools and techniques for cybercriminals in the perpetration of illegal activities on the cyberspace. Also, different tools and techniques developed by cybercriminals for the purpose of manipulating both computer networks and Internet users are carefully discussed.

6.0 TUTOR-MARKED ASSIGNMENT

1. With relevant examples, write on cybercriminals’ use of social engineering.

7.0 REFERENCES/FURTHER READING

Akhghar, B. & Brewster, B. (2016). *Combatting Cybercrime and Cyberterrorism: Challenges, Trends and Priorities*. Springer International Publishing.

Clough, J. (2010). *Principles of Cybercrime*. Cambridge University Press.

Maras, M. (2015). *Computer Forensics: Cybercriminals, Laws and Evidence (Second Edition)*. Jones & Bartlett Learning.

McQuade, S. C. (2009). *Encyclopedia of Cybercrime*. Green Wood Publishing Group.

Waschke, M. (2017). *Personal Cybersecurity: How to Avoid and Recover from Cybercrime*. Bellingham, Washington, USA.

UNIT 5 THE BLACK MARKET OF CYBER CRIMINALITY

CONTENTS

1.0 Introduction
2.0 Objectives
3.0 Main Content
3.1 The Black Market of Cyber Criminality
4.0 Conclusion
5.0 Summary
6.0 Tutor-Marked Assignment
7.0 References/Further Reading

1.0 INTRODUCTION

Just like the traditional offline criminality, cybercriminals are also operating specialized cyber underground black markets where tools and information needed for easy facilitation of their illegal activities can be conveniently procured on the Internet. Therefore, this unit introduces students to the social organization, general network system and modus operandi of the black market of cyber criminality.

2.0 OBJECTIVES

At the end of this unit, you should be able to:

- describe the social organization of the black market of cyber criminality
- discuss tools and information available for cybercriminals on the black market of cybercriminals
- demonstrate the general workings of cybercrime underground market.

3.0 MAIN CONTENT

3.1 The Black Market of Cyber Criminality

Professional cybercriminals are organized according to the specific roles they play and the input they can have within their different methods of going about their business. The population of cybercriminals is considerably heterogeneous. Exactly as in traditional criminality, there are beginners, small-time crooks, part-timers, and professional, experienced criminals (Ghernaouti, 2013). They do have one thing in common: the possibility of accessing the wide range of tools available on the Net for launching cyberattacks. These tools can be more or less conspicuous and easy to acquire; some are free, others require payment.

Thus, there is a genuine black market for cyber criminality on the Internet in which different types of services and tools can be obtained.
Based on the type of the offer, the quality of the tools provided, and the specific nature of the target market (ranging from the seriously professional to the amateur via the young apprentice), these black market sites can be easy or tricky to locate (Ghernaouti, 2013). Some are freely accessible, while others, often those particularly prized for the quality of the tools and information available, operate under restricted access, reserved for regular customers or clients who have been recommended or introduced, in the same way as contacts are made in mafia circles. These sites generally require subscription, with access being managed and user activities scrutinised. These sites thus form a source of income and profit for the criminals who run them: tools and knowledge in the domain of cyber criminality fall squarely into the framework of traditional criminality and the aim for maximum profits. At the same time, as examples of illegal activities, these sites are by necessity closely monitored by their owners in order to avoid infiltration by the police and other elements of the justice system (Maras, 2015).
For the majority of these illegal sites, to which access is granted by introduction, new joiners are expected to provide evidence of their cybercriminal skills and benefit from several introductions from members of the fraternity who could vouch for them. Overall, though, a large range of tools is available to every Internet user, novices are allowed to take their first steps in the domain by giving them the necessary means. For some, this makes the step from theory to practice very straightforward. Commercial sites are not significantly different from legitimate e-commerce sites, and some of these demonstrate a real flair for marketing. Buyers go there, open a secured account, have access to a shopping basket, and manage their purchases. Ghernaouti (2013) identified the underlisted to be among the products that are generally available for purchase on the black market of cyber criminality:

- stolen credit card data, such as names, addresses, card numbers, expiry dates, and security codes;
- email addresses and turnkey spam services11;
- login details, including account numbers, for online banking and for online gaming (often acquired through phishing);
- scans of genuine identity papers, of falsified identity papers (sent by actual couriers if purchased), and of fake diplomas;
- various pieces of malware that are immediately usable, giving rise to the concept of CaaS – Crimeware as a Service); this software can include phishing kits, Trojan horses, ransomware, viruses, spyware, etc.;
- hosting services for illegal content, command & control servers for botnets, and access to bulletproof servers;

- courses on becoming cybercrimnials or in improving skills, such as in creating better frauds or creating botnets.

Exactly as in traditional areas of commerce, there are sites that sell to consumers and sites that sell in bulk to providers (that is to other cybercriminals), taking a margin for doing so. The prices can vary from one site to another depending on the reseller, on the nature of the data in question (for a bank card, for example, it will hinge on the country of issue; and for account numbers it will depend on the amounts available in the account), and on the quantity purchased. Of course, some offers can very well themselves be scams set up specifically to profit from the greed of other crooks, for example by selling fictitious or faulty goods or services.

The rubrics for “job offers and opportunities” on such sites give a good idea of the specialisation of participants in cyber criminality and of the skills required and in demand. In principle, cybercriminals are specialised, and it is not uncommon to find on their fora advertisements looking for partners or accomplices for specific activities that require multiple technical skills and experience (Ghernaouti, 2013). This splitting of skills and responsibilities (creating malware, accessing systems, hosting contents, usurping identity, money laundering) means that the gangs can reduce the time taken to carry out an operation and thereby diminish the risks of being discovered, and also reduce the likely penalties if caught and convicted. The forums make easy the creation and maintenance of contacts at an international level, meaning that gangs can consist of people from different countries who might not even know each other offline but who can act together at a global scale.
Cybercriminals are rational beings who follow the laws of the market and of supply and demand. They are, above all, criminals who have learned to extend their activities, knowledge, and techniques into cyberspace. Just as there exist a black market and a hidden economy in the physical world, the same can be found in cyberspace (Ghernaouti, 2013). These cybercriminal black markets work in the same manner as classical markets, with the objectives of performance and profitability, feeding the whole chain of cyber criminality and relying on the communications tools and opportunities for contacts provided by the Internet. These markets use the same mechanisms, knowledge, and tools as those activities linked to online advertising and legal e-commerce (Ghernaouti, 2013). They can be found at all stages of the performance of cybercrimes, of their preparation, and their monetisation. In addition, the Internet contributes in a major way to realising their profits. Among other things, the black market offered by the following possibilities:

- buy an on-line phishing kit, install it on a bulletproof server (classic hardware and software platforms), operate it (carry out phishing), collect the data gathered, and sell these through forums, on-line shops, and financial transaction services;

- buy and sell exploits, malware, and ransomware, software that allows cyberattacks to be carried out;

- rent zombie machines and create and operate botnets;

- buy and sell, wholesale or in small quantities, personal data, such as banking details.

- knowing the vulnerabilities that can be exploited in carrying out attacks. The first to discover weaknesses and know how to exploit this for gain will always have a competitive advantage;

- possessing tools to exploit these vulnerabilities;

- having access to individuals willing to buy the tools necessary for committing cybercrimes (ICT or security specialists, good social engineers) and who are then prepared to plan and carry out the crimes (accomplices, intermediaries such as mules used for transferring funds, black hat hackers).

Black markets for cybercriminals can also provide information on market fluctuations that are heavily driven by the lifecycle of vulnerabilities (Ghernaouti, 2013). Vulnerabilities that are not yet widely known, and for which no security patches yet exist, are the most difficult to identify but simultaneously the most profitable for those who exploit them. At the same time, the more that these weaknesses are exploited, or the more significant their impacts, the more likely it is that security countermeasures will be developed. The vulnerabilities, and consequently the exploits, become less profitable for the criminals, their value depreciates, and eventually, they become obsolete. The cybercriminal ecosystem will remain in equilibrium for as long as those involved obtain profits significantly greater than the risks they run of being pursued by the forces of justice (Clough, 2010). This depends both on the real risks, which may or may not be well managed and controlled on the basis of the strategies adopted, and on the perception of these risks. Between the maximisation of the wealth created through cyber criminality, the rapidity of the profits, and the risks of being arrested, certain cybercriminals have developed a real system of economic intelligence that is both dynamic and adaptable in the service of criminality (Ghernaouti, 2013).

SELF-ASSESSMENT EXERCISE

Critically discuss the mode of operation of the black market of cyber criminality.

4.0 CONCLUSION

Black market of cyber criminality emerged with the inception of cybercrime to cater for the needs of cybercriminals. This illegal cyber underground black market essentially provides cybercriminals the opportunity to procure tools and clandestine information necessary for the facilitation of their online crimes.

5.0 SUMMARY

In this unit, students were exposed to the social organization, general network system and mode of operation of the black market of cyber criminality. Also, they were also acquainted with the common tools and information which cybercriminals normally procure on the underground cyber black market for crime perpetration.

6.0 TUTOR-MARKED ASSIGNMENT

1. Discuss in details the tools and information sourced on the black market of cyber criminality.
2. Compare and contrast the traditional back market of crime and the cyber underground black market.

7.0 REFERENCES/FURTHER READING

Clough, J. (2010). *Principles of Cybercrime*. Cambridge University Press.

Ghernaouti, S. (2013). Cyber Power: Crime, Conflict and Security in Cyberspace. EPFL Press.

Maras, M. (2015). *Computer Forensics: Cybercriminals, Laws and Evidence (Second Edition)*. Jones & Bartlett Learning.

MODULE 2 CYBERCRIMINALS AND THEIR MOTIVES

Unit 1 Cybercrime Categorisations
Unit 2 Types of Cybercriminals
Unit 3 Motives of Cybercriminals
Unit 4 Cybercrime and the *Yahoo Yahoo* Phenomenon in Nigeria
Unit 5 Measuring the Socio-Economic Costs of Cybercrime

UNIT 1 CYBERCRIME CATEGORISATIONS

CONTENTS

1.0 Introduction
2.0 Objectives
3.0 Main Content
3.1 Cybercrime Categorizations
4.0 Conclusion
5.0 Summary
6.0 Tutor -Marked Assignment
7.0 References/Further Reading

1.0 INTRODUCTION

Generally, cybercrime is a form of crime that is often very difficult to categorise. Nonetheless, the three major categories of cybercrime that have over time been dominant in the literature include: cybercrime against property (i.e. hacking of computer, bank credit card, hacking a company information and so on) cybercrime against individual (i.e. cyber stalking, phishing, scams, distribution of pornography and trafficking) cybercrime against government (i.e. hacking government websites, intercepting military information, terrorism).

2.0 OBJECTIVES

At the end of this Unit, you should be able to:

- distinguish the major categorizations of cybercrime that is dominant in the literature
- classify cybercrime
- discuss the types of cybercrime.

3.0 MAIN CONTENT

3.1 Cybercrime Categorizations

Just like the term '*cybercrime*' seems difficult to conceptualize, so also is its categorization a little cumbersome. This situation is largely due to the fact that new forms of cybercrimes are emerging as technology advances. Indeed, there are many types of cybercrimes today that did not exist just a few years ago. Although some of those crimes are new crimes, whereas others are new versions of traditional crimes (Hill and Marion, 2016). Regardless of the complexity that is often associated with the categorization of cybercrime, attempts shall be made in this Unit to discuss those that are dominant in the literature. The categorization of cybercrime is necessary because it is by breaking down the analysis of cybercrimes into different levels and types of impact they have that criminological debates can clearly engage more with the issues at hand (Wall, 2001).

Schell and Martin (2004) identified the majority of publicized cybercrimes affecting governments, industry officials, and citizens worldwide as including:

a. Cracking: which involves gaining unauthorized access to computer systems to commit a crime, such as digging into the code to make a copy-protected program run without a password or a valid license string, flooding Internet sites and thus denying service to legitimate users, erasing information, corrupting information, and deliberately defacing Web sites

b. Piracy: this involves copying protected software without authorization

c. Phreaking: this means obtaining free telephone calls or having calls charged to a different account by using a computer or another device to manipulate a phone system

d. Cyberstalking: this entails harassing and terrorizing selected human and institutional targets using the computer, causing them to fear injury or harm

e. Cyberpornography: this involves producing and/or distributing pornography using a computer

f. Cyberterrorism: this involves unlawful attacks and threats of attack by terrorists against computers, networks, and the information stored therein to intimidate or coerce a government or its people to further the perpetrator's political or social objectives

Also, the United States Department of Justice categorized cybercrime into three major forms:

(1) the computer as the target (this involves attacking the computers of others by spreading viruses or a denial-of-service [DoS] attack or an attack on a website)

(2) the computer as the weapon (this means using a computer to commit traditional crimes, such as fraud, illegal gambling, or online pornography), or

(3) the computer as an accessory or a device that contains data incidental to the crime (this entails using a computer as a method to maintain records on illegal or stolen information).

Equally, the United Nations recognized five major categories of cybercrime to include:

(1) financial (crimes that disrupt a business's ability to conduct e-commerce, such as viruses, cyberattacks or DoS attacks, or e-forgery),

(2) piracy (copying copyrighted material),

(3) hacking (the act of gaining unauthorized access to a computer system or network and in some cases making unauthorized use of this access),

(4) cyberterrorism, and

(5) online pornography

The Organized Crime Situation Report of 2005 that was published by the Council of Europe divides cybercrime into the following types of offences:

- offences against the confidentiality, integrity and availability of information and communication infrastructures: illegal access to computers (by computer hacking or wiretapping or by deceiving internet users by spoofing, phishing or password fishing), computer espionage, computer sabotage and extortion.
- computer related traditional crimes: frauds, manipulations, abuse of credit cards, forgery, online grooming of children, search for victims, attacks on public safety through manipulation of flight control systems or hospital computers.
- content-related offences: child pornography, racism, xenophobia, soliciting, inciting, providing instructions for and offering to commit crimes, ranging from murder to rape, torture, sabotage and terrorism, cyberstalking, libel and dissemination of false information, Internet gambling.

- offences related to infringement of copyright and related rights: unauthorized production and use of software, data, audio, and video.

One of the widely recognized typologies of cybercrime was put forward by David Wall (2001) in his book titled '*Crime and the Internet*'. Wall (2001) identified four major categories and these include: (1) cyber-trespass; (2) cyber-deception and theft; (3) cyber-porn and obscenity; and (4) cyber-violence. These categories reference the wide range of deviant, criminal, and terrorist behaviors that have emerged using technology, as well as the subcultures supporting offenders throughout the world (Holt, Adam, and Seigfried-Spellar, 2018).

a. Cyber-trespass: this is the unauthorized crossing of boundaries of computer systems into spaces where rights of ownership or title have already been established. Computer hackers played an important role in the early stages of the conceptual development of the Internet, combining high levels of specialized knowledge to test out and develop new ideas with a staunch ethical belief in freedom of access to all information. Initially they were applauded as a celebration of the genius of youth and the pioneering spirit of America, but they have been subsequently become demonized (Chandler, 996). Although a distinction is increasingly being made between the principled trespasser (the hacker) and the unprincipled trespasser (the cracker), their skills and beliefs are now commonly regarded as a major threat to the interests of those who are attempting to effect monopoly control over cyberspace: namely commerce and the state.

b. Cyber-deception/theft: this describes the different types of acquisitive harm that can take place within the cyberspace. At one level lies the more traditional patterns of theft, such as the fraudulent use of credit cards and (cyber)-cash, and a particular current concern is the increasing potential for the raiding of on-line banking accounts as e-banking becomes more popular. Credit card frauds over the Internet arise from the fraudulent use of appropriate credit cards to buy goods over the Internet from the many virtual shopping malls and auction sites. In common with telephoned transactions, the cyber fraudster does not need to have the actual credit card in order to shop over the Internet; only the card number and the expiry date, together with the name on the card and a delivery address, are required.

c. Cyber-porn and obscenity: The third category in Wall's typology of cybercrime is cyber-porn and obscenity. This represents a range of sexually expressive content online. The cyberporn/obscenity debate is very complex because pornography is not necessarily illegal. The relatively legal nature of adult pornography has enabled the development of an extremely lucrative industry, thanks in part to the availability of streaming web content and high-speed connectivity. In addition, amateurs are increasingly active in the porn industry due to the ease with which individuals can produce professional quality images and media through HD digital cameras, web-enabled cameras, and other equipment (Lane, 2000). While viewing pornographic content is not illegal for individuals over the age of 18, accessing certain content, such as violent or animal-related material, may be criminal depending on local laws.

d. Cyber-Violence: this concerns the violent impact of the cyber-activities of another upon an individual or a social or political grouping. Whilst such activities do not have to have a direct physical manifestation, the victim nevertheless feels the violence of the act and can bear long-term psychological scars as a consequence. The activities referred to here range from cyber-stalking to hate-speech to tech-talk. Cyber stalking includes the persistent tracking and harassment of an individual by another – for example, by the persistent sending of e-mails and the sending of obscene messages or even death threats. A worrying development of cyber-violence arises from the convergence of hate-speech and tech-talk. The latter circulates the technologies which can make the former a reality.

Furthermore, some other common forms of cybercrimes include the following:

i. Phishing: this involves sending emails to users in an attempt to steal their private information, which can then be used for other crimes. The victim receives an email that appears to be from a legitimate organization, such as a bank or a credit card company, that claims there is a problem with the victim's account or that the account needs to be verified (Chawki et al. 2015)." The victim is asked to supply personal information or follow a link to a website to provide personal information. The user is prompted to click on a link and log in to his or her account, which requires a user ID and password. Though the link appears to be from a legitimate financial institution, it is operated by an identity thief. When the victim enters his or her information to verify the account, the victim is also providing the offender with a username and password that can be used to log in to the real account and steal funds. The illegitimate websites are crafted so they appear to be legitimate (Chawki et al., 2015). A typical phishing email will appear to come from a legitimate organisation, such as a bank, and will state that the organisation requires the recipient to verify their account information. For example, it may state that the person's account may have been compromised and the bank needs to check their security details. The email will usually have as spoofed header and will be designed to resemble that of the real organization (Ghernaouti, 2013). The recipient is thereby tricked into providing the information, which is then on-sold and/or used in committing identity crime.

Although typically used to gain financial information, phishing may be used to gain access to any account information which may be useful for the offender. In one particularly sinister example, the defendant used phishing emails to obtain minors' passwords to a social networking site and then used the passwords to secretly gain access to the minors' webcam sessions (Clough, 2010) there are a number of ways in which phishing emails may capture personal information. The least sophisticated is simply to ask the recipient to respond via email or fax. A more sophisticated version is to incorporate a link or an attachment in the message which, when clicked, leads to the downloading of malware such as keyloggers or Trojans.

ii. Pharming: this is a technique which utilizes the way in which internet domain names are resolved to direct unsuspecting users to the false website. Such attacks are particularly pernicious in that a person who knows not to click suspicious links in emails, will still type legitimate emails into their browser, not suspecting it may be lead to a phishing site (Clough, 2010). When a text web address is entered into an Internet browser, it must be converted to a numeric IP address. This is achieved by a system of Domain Name Servers (DNS), which process such requests. In a process known as DNS-poisoning, the DNS may be modified so that when a particular IP address is entered, such as a financial institution, the request is automatically directed to the phishing website mimicking that financial institution. A more limited effect can be achieved by poisoning the DNS cache on the user's computer by modifying the local hostfile. When a web address is entered into the browser, the computer will look for the numeric address locally in the hostfile. The hostfile may therefore be modified to the false website address, to which the user will be directed. This will usually be achieved by a Trojan which places a valid address for the false website in the user's host file (Clough, 2010). Even more insidious, Trojans may wait until the user visits a legitimate website before creating a false pop-up asking for identifying information, which is then transmitted to a remote server. Such a Trojan was used in relation to American Express websites in 2006 (Clough, 2010).

iii. Spamming: this involves sending unwanted or unsolicited emails to thousands of users, sometimes anonymously (McQuade, 2009). Spam can be used to promote or advertise products or to trick people into giving up personal information (phishing). They may offer free investment opportunities or sexual enhancement products. They are often carriers for computer worms, viruses, and other malware. A person who is behind this activity is called a “spammer.” For the sender, spam is economically viable. Users have no operating costs beyond the management of the mailing lists. Because of this, the volume of unsolicited emails has grown. But for the recipients, there may be significant costs to spam. If they have malware attached, the costs can be very high. The direct effects of spam include the consumption of computer and network resources as well as the cost in human time and attention of dismissing unwanted messages. In addition, spam has costs stemming from the kinds of spam messages sent, from the ways spammers send them, and from the race between spammers and those who try to stop or control spam. Because most spams are unwanted and can be very harmful, some email users have spam filters that attempt to block or delete the spam messages. The European Union’s Internal Market Commission estimated that in 2001 that “junk email” costs Internet users €10 billion per year worldwide. In addition to direct costs are the indirect costs borne by the victims—both those related to the spamming itself, and to other crimes that usually accompany it (McQuade, 2009). Perhaps the greatest challenge to enforcement is the global nature of spam. The Spamhaus Project lists the ‘Top 5 Countries’ for spam originating on their networks as the United States, China, Russian Federation, South Korea and the United Kingdom (Clough, 2010). On the other hand, spamming has become a much more organised business, centralised in the hands of a relatively small number of spammers. It has been estimated that approximately 80 per cent of spam targeting North America is generated by ten known spammers (Organisation for Economic Co-operation and Development, 2007).

iv. Identity Theft: digital technology has undoubtedly expanded opportunities for offenders to acquire identity information. The portability and storage capacity of digital technology is such that loss or theft of a computer, PDA or storage device may have disastrous consequences (Clough, 2010). Identity theft occurs when an offender steals personal information from a victim, such as a social security number, biometric number, date of birth, home address, passwords, or driver's license number, and then uses that information to access a victim's bank accounts and/or makes charges on the victim's credit cards. The offender can also apply for bank loans or steal Social Security checks. In some cases, an offender applies for a passport or driver's license with his or her picture but the victim's name. If the offender is arrested, the victim is identified as the offender. According to the Berkshire, Massachusetts, District Attorney's Office, one's personal information is stolen to commit four major types of crimes:

- Financial identity theft: this occurs when an offender uses a victim's identity to obtain money, goods, or services. For example, an offender may take the following actions: Open up a bank account in the victim's name Obtain debit and credit cards in the victim's name Take out mortgage loans in the victim's name Buy an automobile by taking out a loan on the victim's name.

- Criminal identity theft: to facilitate this type of identity theft, an offender poses as the victim to commit a crime or claims to be the victim when apprehended for a crime.

- Identity cloning: this form of identity theft occurs when an offender assumes the identity of the victim in his or her daily life. To do so, the offender usually retrieves duplicates of the victim's driver's license, birth certificate, passport, and other personally identifying records. The offender subsequently takes over all of the victim's existing accounts (e.g., bank and phone information).

- Business/commercial identity theft: Using this form of identity theft, offenders use another business' or organization's name to obtain credit, funds, goods, or services.

v. Credit Card Skimming: this is 'the process through which legitimate credit card data is illicitly captured or copied, usually by electronic means' (Clough, 2010). This technique exploits the vulnerabilities of magnetic-strip technology, present on many credit, debit and other transaction cards. While allowing cards to be programmed with data quickly and easily, it also means that the data can easily be copied. Although commonly referred to as 'credit card skimming', the practice can be applied to any form of card which carries data on a magnetic strip. The technology required to engage in this practice, known as a 'credit card skimmer,' may be a modified version of commercially available card readers or a purpose-built device. Such devices are becoming increasingly small and easy to conceal. Skimmers may also be placed inside point-of-sale terminals, which appear to be legitimate, even in some cases producing bogus receipts. PINs may also be obtained by hot-wiring PIN key pads or using pinhole cameras. At a more sophisticated level, the data transfer from merchants may be intercepted or malware placed in ATM and EFTPOS (Aus/NZ) or Switch (UK) terminals (Clough, 2010).

vi. Denial of Service Attacks: this form of cybercrime is primarily targeted at denying users of computers or other types of electronic devices access to an information system or its resources. DOS attacks often involve flooding a computer network with massive amounts of data in a short period of time so that servers cannot keep up with the amount of data being transmitted (McQuade, 2009). The effect is prevention, disruption, and/or minimization of legitimate network traffic. DOS attacks may also inhibit users from accessing network-related applications or services needed. While some attacks simply bombard networks with large amounts of traffic from thousands of compromised or virus-infected systems on the Internet, other attacks may trigger a ''SYN Flood'' in which a high number of connection attempts to consume entire network connection capabilities. In essence, most DOS attacks are aimed at compromising network efficiency or connectivity. A DoS attack replicates this effect intentionally, and can target a single computer, server, website or network (Clough, 2010). Such attacks are common, with one estimate in the UK putting it at approximately 4,000 per week. Some are concerted attacks, as when an ISP which offered a gaming server facility was subjected to DoS attack on forty-three occasions, preventing thousands of users from accessing the servers (Clough, 2010). In other attacks, well-known websites, including Yahoo.com, Amazon.com, eBay.com and Buy.com were temporarily disabled as a result of such attacks (OECD, 2007).

There are a number of ways in which DoS attacks may be achieved. Network routers may be disabled or wireless access points reprogrammed so that others cannot access the network. Another form of DoS attack is known as 'mail bombing' where the attacker uses specialist software to send large volumes of email to a single address in an effort to overwhelm the mail server. Denial of service may also result from a replicating program such as a virus overwhelming the network. The functioning of a computer may also be impaired where it is used for significant processing such as brute-force cracking. More sophisticated DoS attacks utilize Internet protocols to overwhelm the target computer(s). A networked system such as the Internet relies upon protocols to allow computers to communicate with one another and to ensure that the data requested arrives at its destination (Clough, 2010). The client computers ends are quest to the server, which then responds and identifies itself. Once the client computer receives this identification, data can be transferred (Paget, 2007).

vii. Cyber hate speech

The unregulated nature of the Web has aided a proliferation of cyber-hate. Hate speech can take different forms, but in general targets individuals or groups on racial, ethnic, religious, gender or sexual grounds, or based on other characteristics such as physical or mental disabilities (Ghernaouti, 2013). Online hate speech often takes the form of websites and associated chat rooms and bulletin boards established by organized political or ideological groups. Most often these websites are designed to target young people and do not hesitate to use video games to incite or urge the elimination of Black, Jewish or Arab people, and other members of minority groups (Ghernaouti, 2013). Several thousand hate speech sites exist. The Web provides the extremists with an efficient and cost-effective means of communication for reaching a potentially global audience. Acting remotely and in anonymity reduces the risk of identification and prevents the perpetrators from being prosecuted under national anti-hate speech laws. The dissemination of racist and xenophobic material through computer systems, racial and xenophobically motivated threats, racial and xenophobically motivated insults, denialism, gross minimization, approval or justification of genocide or crimes against humanity, and aiding and abetting are criminalized in the Additional Protocol to the Convention on Cybercrime (ETS 189) (Ghernaouti, 2013). Cyber hate speech has also become a major cause for concern on the Nigerian digital space in recent times.

It is clear from these approaches that a number of general features could be used to describe cybercrime acts. One approach is to focus on the material offence object – that is, on the person, thing, or value against which the offence is directed (UNODC, 2013). This approach is seen in the Commonwealth of Independent States Agreement (where the offence object is computer information) and also in Title One of the substantive criminal law chapter of the Council of Europe Cybercrime Convention (where the objects are computer data or computer systems). Another approach is to consider whether computer systems or information systems form an integral part of the modus operandi of the offence (UNODC, 2013) This approach is also seen in Titles Two, Three and Four of the substantive criminal law chapter of the Council of Europe Cybercrime Convention, as well as in the Shanghai Cooperation Organization Agreement, and the Draft African Union Convention. Identifying possible cybercrime offence objects and modus operandi does not describe cybercrime acts in their entirety, but it can provide a number of useful general categories into which acts may be broadly classified. Some international or regional instruments concern cybercrime only in the narrower conception of the computer system or data as the offence object. Others address a broader range of offences, including acts where the offence object is a person or value, rather than a computer system or data – but where a computer system or information system is nonetheless an integral part of the modus operandi of the offence (UNODC, 2013).

SELF-ASSESSMENT EXERCISE

With relevant examples, highlight and discuss the major classification of cybercrime as put forward by Schell and Martin (2004).

4.0 CONCLUSION

Regardless of how cybercrime is categorized, one thing that is clear is that its occurrence is often deleterious and devastating for victims. Different forms of crimes are emerging on the cyberspace daily. Therefore, its categorization is usually very complex and complicated. Be that as it may, cybercrime can be financial or non-financial; it can be targeted against a business, an organization or even a government. Moreover, computer device can be a target of cybercriminals; it can also be used as a weapon or an accessory for facilitating cybercrime.

5.0 SUMMARY

In this unit, students have been exposed to different typologies in which cybercrime have been classified by scholars and international bodies. Also, the difficulty that is embedded in the categorization of cybercrime was also discussed and explained.

6.0 TUTOR -MARKED ASSIGNMENT

1. Using relevant examples differentiate between phishing and spamming.

7.0 REFERENCES/FURTHER READING

Anti-Phishing Working Group. (2008). Phishing Activity Trends Report: Q2/2008.

Chawki, M., Darwish, A. Khan, M. B. & Tyagi, S. (2015). *Cybercrime, Digital Forensics and Jurisdiction*. Springer International Publishing.

Clough, J. (2010). *Principles of Cybercrime*. Cambridge University Press.

Ghernaouti, S. (2013). *Cyber Power: Crime, Conflict and Security in Cyber Space*. EPFL Press.

Hill, J.B. & Marion, N. E. (2016). *Introduction to Cybercrime, Computer Crimes, Laws, and Policing in the 21st Century*. Praeger Security International Textbook.

Holt, T. J., Adam, M. B. & Seigfried-Spellar, K. C. (2018). Cybercrime and Digital Forensics: An Introduction. Routledge: Taylor and Francis.

Lane, F. S. (2000). Obscene Profits: The Entrepreneurs of Pornography in the Cyber Age. New York: Routledge.

McQuade, S. C. (2009). *Encyclopedia of Cybercrime*. Green Wood Publishing Group.

Paget, F. (2007). Identity Theft, White Paper (McAfee).

Schell, B. H. and Martin, C. (2004). *Cybercrime: A Reference Handbook*. ABC CLIO.

United Nations Office on Drugs and Crime (2013). Comprehensive Study on Cybercrime. UNODC, Vienna.

Wall, D. (2001). *Crime and the Internet*. New York: Taylor and Francis Group.

UNIT 2 TYPES OF CYBERCRIMINALS

CONTENTS

1.0 Introduction
2.0 Objectives
3.0 Main Content
3.1 Types of Cybercriminals
4.0 Conclusion
5.0 Summary
6.0 Tutor -Marked Assignment
7.0 References/Further Reading

1.0 INTRODUCTION

In the world we find ourselves today, there are several internet-aided crimes known as cybercrime. These are carried out online by cybercriminals. Therefore, it becomes imperative to extend our discourse on cybercrime to its perpetrators that have been widely regarded as cybercriminals. Information and more awareness need to be provided on the type of cybercriminals and their mode of operations to enable individuals; government and organization better protect themselves against internet breach, inherent crimes, threats and attacks lurking on the cyberspace.

2.0 OBJECTIVES

At the end of this Unit, you should be able to:

- identify the types of cybercriminals
- discuss their modes of operation.

3.0 MAIN CONTENT

3.1 Types of Cybercriminals

Cybercriminals have become an integral part of our social structure and have naturally appeared in the virtual world like their non-criminal counterparts. The emergence of cybercriminals has become more pervasive today, because of the ubiquity of the increasingly tempting targets that is made possible by the freely growing online exchange of money and data. Cybercriminals are simply criminals who use the Internet for their purposes. They are not different from traditional criminals of the kind we have always known. They are looking for criminal opportunities and, when they find them, they exploit them according to their abilities or the abilities of other criminals with whom they can join forces to commit specific cyberattacks (Ghernaouti, 2013). In his book titled '*Scene of the Cybercrime*', Shinder (2002) cited in Brenner (2010) classified cybercriminals into the following main categories:

3.2 Hackers, Crackers, and Network Attackers

Internet network constitutes a major tool for this group of cybercriminals. Unless a hacker has physical access to a computer with the Net, it would be impossible for him or her to commit a crime. Hackers can commit several crimes, such as unauthorized access, theft of data or services, and destructive cybercrimes such as website defacement, release of viruses and DoS, and other attacks that bring down the server or network. Hackers learn their "craft" in a number of ways: by trial and error, by studying network operating systems and protocols with an eye toward learning their vulnerabilities, and perhaps most significantly, from other hackers. There is an enormous underground network where those new to hacking can get information and learn from more experienced hackers. There are numerous sites to meet hackers online, and many more that provide tools that can be used for hacking sites. Websites such as the Ethical Hacker Network, Cult of the Dead Cow, Hacktivismo, Security Hacks, and Darknet provide information and software to discover vulnerabilities and access systems. Of course, almost any network security tool used for testing problems can be used for these purposes. In addition to this, there are newsgroups, mailing lists, online papers and videos that provide guidance and detailed information. Hacker conferences such as DEFCON and the Black Hat Briefings provide real world opportunities for hackers to meet and exchange ideas.

3.3 Criminals Who Use the Net Incidentally to the Crime

Some criminals use the network in relation to their crimes, but the Net itself is not an actual tool of the crimes. That is, the network is not used to commit the criminal activity, although it can be used to prepare for or keep records of the criminal activity. Examples of this type of criminality include: (i) Criminals who use the Net to find victims (this category criminals go on to use the internet to actually commit the crime); (ii) Criminals who use computers or networks for recordkeeping (this category includes people who engage in non-computer-related criminal activity such as drug dealing, illegal gambling, or other illicit businesses, who use computers to keep financial records, customer lists, and other information related to the criminal activity, whilst simultaneously utilizing the internet to transfer those files to an off-site location where they will be safer from law enforcement.); and (iii)

Criminals who use email or chat services to correspond with accomplices (this group includes criminals who work in groups—terrorist groups, theft rings, black hat hackers—often use emails and chats in the same way that legitimate users do: to correspond with people they work with).

3.4 Real-life Noncriminals Who Commit Crimes Online

In some situations, people who are not criminals in real life do engage in criminal conduct online. This category of cybercriminals usually does not have any criminal intent. Rather, they commit illegal acts online because of ignorance of the law or lack of familiarity with the technology. An example is someone who is using the broadband internet access available in a public library and in the process inadvertently opens the Network Neighbourhood folder on his computer and sees other computers listed there. Out of curiosity, he or she clicked on it and was able to access files and folders in some computers that were not properly protected or kept secured by their owners. Accessing the contents contained in such vulnerable computer systems amount to cybercrime.

Another very useful and detailed typology of cybercriminals was put forward by McQuade (2009). He categorized them into the following groups:

1. negligent users who violate security policies or do not practice sound information security practices and thereby expose their data or that residing on a network to harm;

2. traditional criminals of conventional crimes who use computers or other types of electronic devices for communications and/or record keeping in support of their illegal activities;

3. fraudsters and thieves including those who phish, spoof, spim, or otherwise deceive people for financial gain;

4. hackers, computer trespassers, and password crackers (also known as white or gray hat hackers) who, in the tradition of the original hacker ethic, use computers to illegally explore, learn about, and take control of systems in order to pull mischievous pranks, and who may also find, exploit, or expose security vulnerabilities;

5. malicious code writers and distributors who create, copy, or release disruptive or destructive viruses, Trojans, worms, or adware/spyware programs;

6. music, movie, and software pirates who use IT to violate copyright laws by illegally copying, distributing, downloading, selling, or possessing software applications, data files, or code;

7. harassers and extortionists who use technologies to threaten, annoy, or coerce;

8. stalkers, pedophiles, and other cybersex offenders who use online and/or in- person methods when needed to acquire illegal sexual pleasure from or power over people;

9. academic cheats who use a variety of tools and techniques to plagiarize or cheat on assignments or exams, or who fake research methods or findings for profit or fame;

10. organized criminals including ethnic-based gangs who use computers or electronic devices in the course of their legal and illegal business enterprises;

11. corporate, government, and free-lance spies who use simple-to-complex tools and methods of espionage including spyware and key logger applications to snoop for personal or professional purposes; and

12. cyber terrorists who seek to advance their social, religious, or political goals by instilling widespread fear or by damaging either critical infrastructure or critical information infrastructure.

SELF-ASSESSMENT EXERCISE
Identify and discuss the types of cybercriminals discussed in this unit.

4.0 CONCLUSION

Regardless of the ways they are categorized, activities of cybercriminals typically constitute serious threats to other Internet users. Their illegal activities on the cyberspace can have national, transnational and international consequences for individuals, businesses, organizations, and governments.

5.0 SUMMARY

In this unit, students have been introduced to the major categorizations of cybercriminals and ways through which they constitute threat to people, governments, and organizations in the world.

6.0 TUTOR- MARKED ASSIGNMENT

1. Discuss cybercriminals that use the Net incidentally to commit crime

7.0 REFERENCES/FURTHER READING

Brenner, S. W. (2010). *Criminal Threats from Cyberspace*. Praeger.

McQuade, S. C. (2009). *Encyclopedia of Cybercrime*. Green Wood Publishing Group.

UNIT 3 MOTIVES OF CYBERCRIMINALS

CONTENTS

1.0 Introduction
2.0 Objectives
3.0 Main Content
3.1 Motives of Cybercriminals
4.0 Conclusion
5.0 Summary
6.0 Tutor -Marked Assignment
7.0 References/Further Reading

1.0 INTRODUCTION

The motivations for cybercriminals are quite numerous.. There is a generally held misconception that cybercriminals are mainly motivated by pecuniary gains. However, evidence abounds to indicate that cybercriminals motive(s) for the perpetration of illegal acts on the cyberspace can be both financially and non-financially induced. Our focus in this unit shall be on the major factors underlying criminals' perpetration of cybercrime.

2.0 OBJECTIVES

At the end of this unit, you should be able to:

- explain the major factors motivating cybercriminals to perpetrate different forms of crime on the cyberspace.

3.0 MAIN CONTENT

3.1 Motives of Cybercriminals

For a long time, the motivations of cybercriminals were mainly notoriety, publicity, intellectual challenges, and peer recognition. Nowadays, cybercriminals are more motivated by profit than by glory, power, or personal satisfaction (Ghernaouti, 2013). Information and communications technologies are the means and the targets of their criminality. They have integrated these technologies into their strategies to get rich, launder money, obtain power, or destabilize others. For them, the Internet is a tool to be used for many kinds of frauds, transactions, and general crimes (Ghernaouti, 2013).

People involved in cyber criminality are a numerous and heterogeneous group with differing motivations and backgrounds. Thus, it would be reductive to try to define a definitive typology of cybercriminals; as such an attempt would be unable to correctly reflect the diversity and complexity of all the participants (Ghernaouti, 2013). Although it is not easy to know the motivations of cybercriminals, one way to differentiate them is to consider whether or not they have used their illegal activities for financial gain. Some of them may not really understand the significance of what they are doing or their ability to cause problems. Others, on the other hand, do these things deliberately. They might have a feeling of superiority caused by a level of mastery of how the Internet works – a level certainly superior to that of the majority of Internet users and that of people who use out-of-the-book malware; this is fairly typical of hackers who want to show that they are better than the others. Or in addition, they might have a feeling that hacking activities – hacktivism – are legitimized by their passion for the subject and by the very existence of the Internet, and that these activities are in some way imposed upon the hacker as natural outlet (Ghernaouti, 2013).

Generally, the rise of cyber deviance, cybercrime, and cyber terror has led many to question why some people choose to engage in wrongdoing in virtual environments (Holt et al. 2018). Just like the conventional criminals, different motivating factors are propelling cybercriminals towards committing crime on the cyberspace. As established in the previous sections there are different types of cybercriminals. Therefore, their motivations for cybercrime involvement are likely to vary, and be dependent on the type of cybercrime that is of interest to them. Consequently, the motives that will be discussed in this Unit are by no means exhaustive. Some of the general reasons motivating cybercriminals into engaging in cybercrime are discussed below:

a. Financial Gains: the quest for financial gain is among the major primary factors predisposing cybercriminals towards cybercrime. Many cybercriminals do achieve this by engaging in cyber fraud through different deceptive schemes such as selling fictitious goods online, engaging in fake online romance, hacking into financial institutions and other corporate organizations' security architectures, by stealing victims' personal and confidential information such as their social security number or ATM pin and passwords which they often subsequently use to defraud them. A very good example of a group of cybercriminals that is motivated by financial gains is the *yahoo-yahoo* boys of Nigeria. Blau (2004) correctly pointed out that in the contemporary period; there is more of a financial incentive for hackers and crackers as well as for virus writers to write for money and not just for glory or some political motive.

b. Political Reasons: some cybercriminals perpetrate cyberattacks for political reasons. Cybercriminals with this form of motivation may hack into a computer system for different purposes such as attracting government attention to their cause, showing their support for a particular cause, raising donations, persuading people to join their group, or to sabotage a process. For instance, the 2011 Nigeria's general election was almost disrupted by cybercriminals that hacked both into the server and website of the Independent National Electoral Commission (INEC). Equally, the Zapatista social movement in Chiappas State in southern Mexico also deployed cyberattacks against the web servers of Mexican officials to pursue its political goals (Lee, 2000). However, in some instances, some governments also do hack into the systems of other governments as a way committing espionage or to steal secrets (especially technology secrets) (Hill and Marion, 2016). Every country engages in espionage against other nations to some extent, but China and Russia are better known for this. Other countries that have been accused of engaging in cyber espionage are Iran, North Korea, Sweden, Japan, United Kingdom, Germany, Netherland etc.

c. Adventure and Curiosity: Another motive behind some cybercriminals' action is adventure and curiosity. In this instance, cybercriminals commit crimes on the cyberspace as a means of adventure or out of curiosity. Hackers are a group of cybercriminals that are usually motivated by this factor to engage in cybercrime. For this group of cybercriminals, hacking into a secure system is considered as a kind of a challenge. Therefore, they engage in it out of curiosity to determine whether or not they can be able to break into a system. Many cybercriminals in this category do not intend to cause serious harm, but their actions can cause a significant amount of damage. In this instance, the potential psychological benefits provide strong incentives for some individuals to engage in cybercrimes

d. Cybercrime as Precursor to Other Forms of Organized Crimes: The emergence of the Internet has significantly increased the level of global interconnectedness. While this is remarkable, criminal syndicates around the world are also engaging in cybercrime as a way of furthering their criminal goals. Members of organized crime do perpetrate cybercrimes as a way of increasing their power and wealth. They see cybercrime as an easy way of making profit, partly because it is easier to carry out crimes on the Internet than to physically break into a building or facility. For instance, Internet is being used to traffic in drugs, even making alliances with drug traffickers in the Middle East and other locations to increase their supply and market (Hill and Marion, 2016). Also, some groups have used cybercrime as a way of laundering money or traffic in child pornography, illegal weapons, and even humans.

e. Lower Risk of Detection: compared to physical crimes, cybercrimes are relatively difficult to detect by victims, law enforcement officials, and other third parties. Therefore, recognizing the relatively safe and anonymous nature of the cyberspace, many criminals are emboldened to engage in cybercrimes. The faceless nature of the Internet makes it easy for individuals to hide their gender, age, or race in various ways. Also, a profile in a social networking site like Facebook or email account can be created using false information through Google, Yahoo, or Hotmail (Holt et al. 2018). This false account may be used to send threatening or harassing messages to others to help conceal their true identity (Bocij, 2004). Similarly, various technological resources are designed to hide a person’s location from others.

f. Victims’ Non-Reporting of Victimization: it is a common knowledge that some victims of cybercrime prefer to just move on with their lives rather than reporting their online victimization experiences to relevant law enforcement agencies that can help them track down and/or prosecute the perpetrators. While some victims may just want to forget and/or blur out their victimization experience altogether, some may not want to contact law enforcement officials because of the perceived embarrassment, shame, or harm that may come from reporting. Furthermore, within corporate and government computing environments, factors such as fear of losing customers and patrons or the perceived embarrassment and backlash that will likely follow public declaration of loss of sensitive and confidential information may engender cover-ups or diminished reporting (Holt et al., 2018).

SELF-ASSESSMENT EXERCISE

List and discuss the general reasons motivating cybercriminals into engaging in cybercrimes.

4.0 CONCLUSION

It has been clearly established in this Unit that cybercriminals are being motivated to engage in illegal activities on the cyberspace for different reasons**.** Some of the reasons motivating cybercriminals to perpetrate crime on the cyberspace range from political reasons to economic factor, curiosity, quest for fame and popularity, lower risk of detection, amongst others.

5.0 SUMMARY

This unit focused on the factors motivating cybercriminals to perpetrate crimes on the cyberspace. Some of the reasons mentioned include financial or economic reason, political reason, to satisfy curiosity, low of detection of perpetrators, victims' non-reporting of victimization experience to law enforcement agents, amongst others.

6.0 TUTOR- MARKED ASSIGNMENT

1. Identify and discuss the major factors motivating cyber crimes.

7.0 REFERENCES/FURTHER READING

Blau, J. (2004, May 26). Russia – a happy haven for hackers. Available at http://www.computerweekly.com/ Article130839.htm.

Bocij, P. (2004). Cyberstalking: Harassment in the Internet Age and How to Protect your Family. Westport, CT: Praeger Publishers.

Ghernaouti, S. (2013). *Cyber Power: Crime, Conflict and Security in Cyber Space*. EPFL Press.

Hill, J.B. & Marion, N. E. (2016). *Introduction to Cybercrime, Computer Crimes, Laws, and Policing in the 21st Century*. Praeger Security International Textbook.

Holt, T. J., Adam, M. B. & Seigfried-Spellar, K. C. (2018). Cybercrime and Digital Forensics: An Introduction. Routledge: Taylor and Francis.

Lee, J. K. (2000). The e-citizen, social education. Arlington, 64(6), 378–380.

UNIT 4 CYBERCRIMES AND THE *YAHOO YAHOO* PHENOMENON IN NIGERIA

CONTENTS

1.0 Introduction
2.0 Objectives
3.0 Main Content
3.1 Cybercrime and the *Yahoo Yahoo* Phenomenon in Nigeria
4.0 Conclusion
5.0 Summary
6.0 Tutor -Marked Assignment
7.0 References/Further Reading

1.0 INTRODUCTION

The widespread adoption of the Internet and other Information and Communication Technology (ICT) resources has brought about the problem of cybercrime in Nigeria. Just like in other parts of the world, cybercrime has become a nagging problem for many Nigerians, the federal and state governments, and relevant law enforcement agencies. Cybercrime is so pervasive and widely accepted among the youths in Nigeria to the extent that Nigeria is widely being regarded to be among the hubs of cybercrime committing nations.

2.0 OBJECTIVES

At the end of this Unit, you should be able to:

- understand the nature, trends, patterns, and dimensions of cybercrime in Nigeria
- describe the antics and methods of operations of the youths involved in cybercrime popularly known as the *yahoo yahoo* cybercriminals..

3.0 MAIN CONTENT

3.1 Cybercrime and the *Yahoo Yahoo* Phenomenon in Nigeria

Nigeria is among the highest cybercrime perpetrating countries in the world. The youths involved in this criminal act are locally known as the *yahoo-boys* (Ojedokun and Eraye, 2012). With the numbers of Internet users in Nigeria increasing tremendously from less than a million in 2003 to over 80 million in November 2015 (This Day, 2016), cybercrime has grown in leap and bound. However, the *yahoo-boy* nomenclature does not mean that this form of criminality is exclusively for boys. Rather, both male and female youths are functionally involved in this form of crime in Nigeria (Ogunleye, Ojedokun & Aderinto, 2019; Adeniran, 2008).

Since the late 1980s, networks of Nigerian criminals have been defrauding people through different fraudulent schemes popularly known as advance fee frauds or 419 scams. However, with the commencement of computer-mediated communication and Internet revolution which generally began in Nigeria in the late 1990s (Ojedokun, 2016), scammers and fraudsters are now moving online to lure their victims. Indeed, Internet fraud which is the most commonly perpetrated form of cybercrime in Nigeria has permeated the society with the youths leading the squad (Tade and Aliyu, 2011). The varieties of application offered by the Net such as, the electronic mailing system, 'chat' systems and Internet messaging (IM), and social media platforms have over time proven to be veritable tools in the hands of cybercriminals for carrying out nefarious 'webonomics' and other fraudulent activities (Adeniran, 2008).

According to the 2007 Internet Crime Report released by the Internet Crime Complaint Centre (IC3), Nigeria ranks third among cybercrime committing countries in the world (Odapu, 2008). The report indicates that the "Nigerian letter fraud" (Email Scams) received in the United States, constituted 1.1% and the individuals reporting fraud-type monetary loss in 2007 puts Nigerian letter fraud at 6.4%, amounting to 1,922.99 million US dollars (Odapu, 2008). In September 2019, the Federal Bureau of Investigation busted a cybercrime network in the United States of America that involves 77 Nigerians. The criminal gang was alleged to have defrauded their victims of close $3 billion using several cyber deceptions such as fraudulent business emails, romance scams and other facades.

The common forms of online scams usually perpetrated by Nigerian cybercriminals include;

a. Dating scam or 'sweetheart swindling': this involves developing a love or romantic relationship, which may be heterosexual or homosexual, with an individual online usually through dating sites or on social media platforms with the primary goal of defrauding such a person after gaining the victim's trust and confidence);

b. Classified scam: this usually involves advertising and selling fictitious goods online with the primary goal of swindling potential buyers

c. Next of kin format: for this, perpetrators usually contact potential victims mostly through e-mails to inform them that they have been selected as the son or daughter of a late millionaire who had a very large amount of money in his or her bank account. If the victim agrees to be part of the deal, certain confidential information that can be used to defraud him or her like bank account details, social security card password or ATM PIN would be requested. Once this is obtained, the victim would be defrauded;

d. Missionary Format: this typically involves perpetrators posing as a missionary who travels from one country to another on a mission. They usually solicit donations from their prospective victims by informing them that they have just been posted to a harsh location or region where they intend to create a charity for their host community;

e. Lottery Method: for this type of scam, a mail is usually sent to the client that he or she has won certain amount of dollars that he or she should provide his or her bank details or pay a certain amount of money through a dedicated website for him or her to be able to clear the lottery) are among the most common techniques usually employed by Nigerian cybercriminals.

Although the initially generally held opinions among scholars and government officials was that the majority of the cybercrimes perpetrated in Nigeria were generally targeted at individuals and not necessarily computer systems (Chiemeke and Longe, 2008; Aghatise, 2006), however, the prevailing situations has shown a significant shift in which local and foreign financial institutions, corporate organizations and government agencies are increasingly becoming the targets of cybercriminals operating in Nigeria (Aderinto and Ojedokun, 2018). According to the National Security Adviser (NSA), Maj-Gen. Babagana Munguno (rtd), the global tracking of cyber-attacks indicates that Nigeria is among the countries with high cases of software piracy, intellectual property theft and malware attacks (This Day, 2016). In addition, cyber security experts in Nigeria have equally confirmed that cybercriminals now use Carbanak or Anunak Advanced Persistent Threat malware to target financial institutions in a new and much more dangerous way than traditional APTs, which only target banks' customers by phishing emails (The Punch, 2015).

The activities of Nigerian cybercriminals have over time resulted in huge financial and psychological losses for individuals and corporate institutions. For instance, the 2014 annual report of the Nigeria Deposit Insurance Corporation (NDIC) shows that, between year 2013 and 2014 alone, fraud on e-payment platform of the Nigerian banking sector increased by 183 per cent (This Day, 2016). In a related development, the Centre for Strategic and International Studies, UK, in its 2014 report estimated the annual cost of cybercrime to Nigeria to be about 0.08 per cent of the Gross Domestic Product (GDP), representing about N127 billion (This Day, 2016). In addition, a 2015 survey conducted by Kaspersky Lab indicates that 45.3 per cent of the Internet users in Nigeria suffered attack in the third quarter of 2015 (Amaefule, 2016).

Longe and Chiemeke (2008) identify the most common categories of crimes on the Nigerian Internet landscape to include:

(a) Hucksters

The hucksters are characterized by a slow turn-around from harvest to first message (typically at least one month), a large number of messages are being sent to each harvested spam-trapped addresses, and typical product based spam (i.e spam selling an actual product to be shipped or downloaded even if the product is fraudulent). E-mail addresses are obtained from internet access points using E-mail extractor litel 1.4. These tools can automatically retrieve email addresses from web pages. They are therefore referred to as harvesters.

(b) Fraudsters

The fraudsters are characterized by an almost immediate turn-around from harvest to first messages (typically less than 12hours). Only a small number of messages are sent to each of the harvested addresses (e.g phising, advanced fee fraud-419, from Nigerian perspective). Fraudsters often harvest addresses of their potential victims and thereafter send only a message to them all at a particular time. The tools for getting addresses by these fraudsters are mailing address extractors (Longe and Chiemeke, 2006.

(c) Piracy

Piracy involves the illegal reproduction and distribution of software applications, games, videos, movies and audio CDs (Longe and Chiemeke, 2006). This can be done in a number of ways. Usually pirates buy a copy from the internet, an original version of a software movie or game and illegally make copies of the software available online for others to download and use without the notification of the original owner of the software. This is known as internet piracy warez. Modern day piracy may be less dramatic or exciting, but it is far subtler and more extensive in terms of monetary losses the victims face. This particular form of cybercrime may be the hardest of all to curb, as the most common man also seems to be benefiting from it.

(d) Nigerian Hackers

Young Nigerians can be observed on daily basis engaging in brain storming sessions at cybercafé trying to crack security codes for e-commerce, ATM cards and e-marketing product sites. The surprising thing is that even with their low level of education or little understanding of the intricacies of computing techniques, they get results! Phising is also becoming popular as criminal simulate product's websites to deceive innocent internet users in to ordering products that are actually non-existent. Phishing in this context involves imitating product and e-commerce web pages in order to defraud unsuspecting users. This method is used mostly to obtain credit card numbers.

SELF-ASSESSMENT EXERCISE

Discuss the emergence of the *yahoo yahoo* phenomenon in Nigeria.

5.0 CONCLUSION

Cybercrime has over time remained an intractable problem in Nigeria. This form of crime is a major source of concern for individuals, businesses, government officials, and law enforcement agencies. Youths are the major active players perpetrating cybercrime in Nigeria. This category of youths perpetuating illegal activities on the cyberspace are widely referred to as the *yahooyahoo* boys.

6.0 SUMMARY

In this unit, attention was devoted to the pervasive problem of cybercrime and the emergence of the *yahoo yahoo* phenomenon in Nigeria. The types of cybercriminals operating on the Nigerian cyberspace and their modes of operation are carefully discussed.

6.0 TUTOR -MARKED ASSIGNMENT

1. Mention and discuss the categories of crime being perpetrated on the Nigerian Internet landscape

7.0 REFERENCES/FURTHER READING

Adeniran, A. I. (2008). The Internet and Emergence of Yahoo-boys sub-Culture in Nigeria. *International Journal of Cyber Criminology* 2.2: 368–381.

Aderinto, A. A. & Ojedokun, U. A. (2017). "Cyber Underground Economy in Nigeria". In P. N. Ndubueze (Ed.), *Cyber Criminology and Technology-Assisted Crime Control: A Reader*. Ahmadu Bello University Press, Limited, Zaria. Pp. 219-228. ISBN 978-54894-7-7.

Amaefule, E.2016. Nigeria Loses N89bn to Cybercrimes Annually. *The Punch,* Mar. 30.

Chiemeke, S.C & Longe, O. B. (2008). Cybercrime and Criminality in Nigeria - What Roles are Internet Access Points in Playing? *European journal of social sciences-volume 6, Number 4.*

Ogunleye, Y. O., Ojedokun, U. A. & Aderinto, A. A. (2019). Pathways and Motivations for Cyber Fruad Involvement Among Female Undergraduates of Selected Universities in South-West Nigeria. *International Journal of Cyber Criminology* 13.2: 1001-1013.

Ojedokun, U. A. & Michael, C. E. (2012). Socioeconomic Lifestyles of the Yahoo-Boys: A Study of Perceptions of University Students in Nigeria. *International Journal of Cyber Criminology* 6.2: 309-324.

Ojedokun, U. A. (2016). ICT and Online Social Movements for Good Governance in Nigeria. *The Journal of Community Informatics* 12.1:7-20.

Tade, O. and Aliyu, I. (2011). Social Organization of Internet Fraud among Undergraduate Students in Nigeria. International of Cyber Criminology 5.2: 860-875.

The Punch. (2015). Cybercriminals Use Carbanak Malware to Defraud Banks – Experts. July, 14.

This Day. (2016). Nigeria Loses Over N127bn Annually Through Cybercrime. April 16.

UNIT 5 MEASURING THE SOCIO-ECONOMIC COSTS OF CYBERCRIME

CONTENTS

1.0 Introduction
2.0 Objectives
3.0 Main Content
3.1 Measuring the Socio-Economic Costs of Cybercrime
4.0 Conclusion
5.0 Summary
6.0 Tutor -Marked Assignment
7.0 References/Further Reading

1.0 INTRODUCTION

Cybercrime has been established as affecting individuals, businesses, corporate organizations and government at both national and international levels. Therefore, the collection of data for planning interventions to prevent and reduce crime is as important for cybercrime as it is for other crime types. In this section, the socio-economic costs associated with the occurrence of cybercrime shall be the focus of our attention.

2.0 OBJECTIVES

At the end of this Unit, you should be able to:

- analyse the socio-economic impacts of cybercrime on people, governments and organizations.

3.0 MAIN CONTENT

3.1 Measuring the Socio-Economic Costs of Cybercrime

The precise measurement of the socio-economic costs of cybercrime can be used to inform crime reduction initiatives; to enhance local, national, regional and international responses; to identify gaps in responses; to provide intelligence and risk assessment; and to educate and inform the public (Fafinski, Dutton & Margetts, 2010). Thus, stakeholders at different levels including government agencies, corporate organizations, law enforcement agencies, international organizations amongst others are interested in having a clear picture of the socio-economic costs of cybercrime. The major reason behind this is because the knowledge can help in the understanding of the nature, trends and patterns of cybercrime which can ultimately help in the design of strategic frameworks for addressing the problem. However, the sad reality is that the socio-economic cost of cybercrime is often very difficult to measure because accurate statistics on the number of cyber events and the revenue loss caused by cybercriminals are simply not known.

One approach to the measurement of new forms and dimensions of crime, including cybercrime, is to aim to characterize ‘who’ (and how many) are involved in ‘what’ (and how much). This requires a combination of data sources, such as: information on perpetrators, including organized criminal groups; information on flows within illicit markets; as well as information on numbers of criminal events, harms and losses, and resultant illicit financial flows (UNODC, 2013). Each of these elements has implications for the response to cybercrime. For instance, an understanding of organized criminal group structures and networks is central to the design of criminal justice interventions. Also, an understanding of illicit markets – such as the black economy centred on stolen credit card details – provides details of the underlying incentives for criminal activity (irrespective of the individuals or groups involved), and thus entry points for prevention programming. An understanding of the extent of harms, losses and illicit financial gains provides guidance on the prioritization of interventions (UNODC, 2013).

According to UNODC (2013), the four main information sources for the measurement of ‘what’ cybercrime acts occur and ‘how much’ include:

(i) police-recorded crime statistics;
(ii) population-based and business surveys;
(iii) victim reporting initiatives; and
(iv) technology-based cybersecurity information.

The list is not exhaustive but covers the main sources of information that have some degree of cross-national comparability. Other sources include individual studies on selected phenomena, such as URL crawling techniques, or botnet takeover.

However, in spite of availability of different sources of data as regards, factual information regarding the annual number of cybercrimes are often difficult to gauge due to the following reasons:

(i) the lack of consensus as to the meaning of ‘cybercrime’ means that it may not be included within official crime statistics. Even where there is a specific cybercrime, it may be concealed within other statistics.

(ii) many of the so-called ‘cybercrimes’ are in fact existing offences that are facilitated by technology. Consequently, although the offence itself, will be recorded in crime statistics, the use of technology by offenders may not. Therefore, care must also be taken in incorporating the use of computers within crime statistics.

(iii) most cybercrimes remain unrecognized and therefore are not reported to officials. Sometimes a criminal hacks into a computer system but does no damage, or the damage is so small that it is not identified. Pirated files may be shared among users without the knowledge of the original artist who thus cannot report the theft.

(iv) even when detected victims of cybercrimes may decide not to make a report to relevant authorities due to perceived embarrassment their action could attract. Also, companies affected may be hesitant to report cybercrime incidents because they wish to avoid the negative publicity and possible loss of confidence by customers. According to the 2008 CSI/FBI Computer Crime and Security Survey, only 27 per cent of incidents were reported to law enforcement, with 23.9 percent of incidents not reported at all (Richardson, 2008).

(v) there may be vested interests among security companies to exaggerate the level of cybercrimes. Hence, over estimating the actual number of the recorded incidents of cybercrime.

(vi) empirical findings regarding various indicators related to cybercrime are remarkably inconsistent largely to due to its underground nature.

(vii) media reporting of cybercrime may also present a distorted picture of the actual situation. As with other forms of crime, it is tempting to focus on the novel and/or the sensational rather than the mainstream, and stories of computer misuse may be uncritically accepted and repeated (Clough, 2010).

(viii) there are many methodological, logical, conceptual, and statistical problems in estimating the level and pattern of cybercrimes. While many associations, groups, and company publish their estimates on a regular basis, it is impossible to compare them meaningfully and evaluate their consequences (Rush, Chris, Erika, & Puay, 2009).

As for measuring the costs, the Detica Report suggested that the costs associated with cybercrime can be measured by considering these four categories:

1. costs in anticipation of cybercrime, such as antivirus software, insurance and compliance;
2. costs as a consequence of cybercrime, such as direct losses and indirect costs such as weakened competitiveness as a result of intellectual property compromise;
3. costs in response to cybercrime, such as compensation payments to victims and fines paid to regulatory bodies;
4. indirect costs such as reputational damage to firms, loss of confidence in cyber transactions by individuals and businesses, reduced public-sector revenues and the growth of the underground economy.

Although there are no accurate data on the amount of cybercrime that exists, but different international organizations have attempted to estimate the trends and patterns of this form of crime. Despite the fact that these reports have slightly different results, each show, generally speaking, that cybercrime is occurring more frequently and is more costly for businesses and individuals. The outcomes of some of these studies are discussed below.

3.2 2010–2011 Computer Crime and Security Study

The Computer Security Institute carried out its survey of agencies and asked if they had ever experienced a cyberattack (Hill and Marion, 2016). The goal of the study was to determine a more accurate picture of the number of cyber offenses. The Institute surveyed 5,412 security practitioners by traditional mail and email and asked questions about cybercrimes committed from July 2009 through July 2010. In total, 351 surveys were completed and returned. Of the 351 who responded, almost half (49.8 percent) had not experienced a security incident in the previous year, 41.1 percent had experienced some type of cybersecurity incident, and 9.1 percent did not know. Of those who had experienced an attack, 21.6 percent reported that they were the victim of a targeted attack, 54.5 percent were not targeted, and 24 percent were unable to determine the type of attack.5 This shows that under half of the security personnel admitted to an attack, but a significant portion (about 9 percent) did not know whether they had been attacked at all. The results of the survey showed that malware was the most common type of attack, reported by 67.1 percent of respondents who experienced attacks. Only 8.7 percent of those respondents reported financial fraud incidents. Few of the respondents were willing to share information about the financial losses the company had suffered as a result of the attack, but they did report that their losses were not due to cybercrime perpetrated by insiders. In fact, 59.1 percent did not believe their losses were because of malicious acts by insiders, but only 39.5 percent reported that none of their losses were because of non-malicious insider actions (Hill and Marion, 2016).

3.3 The 2012 Norton Cybercrime Report

The Norton Cybercrime Report was based on an annual survey of officials in 24 countries about their experiences with cybercrime. The 2012 survey included officials from Australia, Brazil, Canada, China, Colombia, Denmark, France, Germany, India, Italy, Japan, Mexico, Netherlands, New Zealand, Poland, Russia, Saudi Arabia, Singapore, South Africa, Sweden, Turkey, United Arab Emirates, United Kingdom, and the United States (Hill and Marion, 2016). The agency conducted an online survey of 13,018 adults between the ages of 18 and 64 years. The findings of the 2012 report showed that there were 556 million victims of cybercrime each year, or 18 victims per second. It estimated that there were 1.4 million cybercrime victims every day. The study put the average loss per victim at $197 when measured globally, but higher in the United States, at $290. In addition, the findings showed that the cost of consumer cybercrime is about $100 billion a year, though this figure may be low because so much cybercrime is unreported.

The Norton Cybercrime Report revealed some interesting patterns about cybercrime and social networks. Of the respondents, 15 percent had had their social network profiles hacked and said that another person had pretended to be them. About one in ten users of social websites reported that they had fallen for a scam or fake link on a social network. Finally, this report found that the highest number of cybercrime victims were in Russia (92 percent), followed by China (84 percent) and South Africa (80 percent). Of the men who participated in the survey, 71 percent reported being a victim of cybercrime, whereas 63 percent of the women reported being a victim.

3.4 The 2012 HP Cost of Cybercrime Study

HP also conducts an annual study of cybercrime, and the 2012 report found that both the number of cybercrime attacks and the costs related to them had increased for the third year in a row. This study looked at cybercrimes in the United States, the United Kingdom, Japan, Germany, and Australia. The results showed that the number of attacks had more than doubled since 2010, and the financial costs to businesses rose by nearly 40 percent. However, the rate of increase appeared to be slowing. Overall, there was an average of 102 successful cyberattacks each week. More than three quarters of these attacks involved malware, denial of service, stolen or hijacked devices, and malicious insiders (Hill and Marion, 2016).

3.5 The 2013 Norton Cybercrime Report

The 2013 Norton Cybercrime Report, which had 13,022 respondents showed that the number of online adults who had experienced cybercrime had decreased from 2012. There were 378 million victims of cybercrime, or about 12 victims per second. However, the average cost of cybercrime per victim had risen by 50 percent. In 2013, the average cost of a cybercrime was $298 (USD). Of the 2013 respondents, 64 percent of the men and 58 percent of the women reported being victims of cybercrime, a lower percentage than in the 2012 report (Norton, 2013).

3.6 2013 European Network and Information Security Agency

In 2013, the European Network and Information Security Agency, the European Union agency concerned with cybersecurity, published the report ENISA Threat Landscape: Responding to the Evolving Threat Environment, a meta-analysis of 120 separate reports published between 2011 and 2012 by different groups and agencies. The report reviews potential threats and threat agents and lists the top threats and emerging trends in today's advancing technology. Following are the 10 most critical threats identified were:

1. drive-by exploits
2. worms/trojan horses
3. code injection attacks
4. exploit kits
5. botnets
6. denial-of-service attacks
7. phishing
8. compromising confidential information
9. rogueware/scareware
10. spam (Hill and Marion, 2013).

3.7 The Verizon 2013 Data Breach Investigations Report

Verizon's annual Data Breach Investigations Report is widely regarded to be one of the most comprehensive analyses of the state of cybercrime and information security; in particular because Verizon partners with the U.S. Secret Service and Department of Homeland Security, the Dutch police are National High Tech Crime Unit, and the European Cybercrime Center, among others, to gather their data. The 2013 report analyzed 47,000 security incidents that occurred in 27 countries and 621

data breaches that were investigated by Verizon’s RISK Team. The results showed that there was a wider range of data breaches and network attacks in 2013 than in previous years. Attacks against financial organizations represented 37 percent of the breaches reported, which was the largest industry sector in terms of the number of attacks. Three-quarters of the attacks were motivated by a desire for financial gain.
In 2013, state-sponsored hacking made up a larger portion of attacks than in previous reports. These attacks focused on stealing intellectual property and industrial/military secrets. Such incidents accounted for 19 percent of the breaches, a much higher number than the year before. Even small companies own intellectual property that may be of interest to a foreign nation. Although many believe attacks by insiders are a serious concern to organizations, this idea was not supported by the data in Verizon’s report. Instead, it showed that only 14 percent of the breaches were committed by people inside the organization. Most attacks came from people outside the organization. However, though the majority of security incidents involved outsiders, insiders were more likely to be successful. When a security breach occurred, who was responsible? More than half of the attackers (55 percent) were members of organized crime groups, and 21 percent were state affiliated. About the same number either had unknown affiliations or were unaffiliated with any known groups. Only 1 percent were committed by former employees. The Verizon data showed that only 2 percent of the breaches were caused by someone who could be labeled as a hacktivist. About a third of these hackers were from China and about the same number from Romania (Hill and Marion, 2016). The remaining hackers were from the United States, Bulgaria, and Russia. Attacks involved hacking and malware, sometimes together, and stolen credentials. The report noted an increase in the use of phishing, which was used four times as frequently as in 2011.

Another critical finding was the time needed for a breach to be discovered. Many breaches went undetected for months. Many attacks (84 percent) took only a few hours to compromise a system, and 69 percent required just a few hours (or less) to steal data. In about 15 percent of cases, the data was stolen in a matter of seconds. In about two-thirds of the cases reported, months (and occasionally years) passed before a breach was discovered. However, the time period was usually only a few days (41 percent), weeks (14 percent) or months (22 percent) to contain the problem (Data Breach Investigation Report, 2013).

3.8 The 2013 and 2014 Internet Crime Reports by the IC3

The FBI’s Internet Crime Complaint Center (IC3) issues a yearly report of the amount of cybercrime reported to law enforcement. The reports shows that the number of complaints the IC3 receives about cybercrime indicates that there has been some fluctuation in the number of cybercrimes recorded since 2000. In 2014, the IC3 received 269,422 consumer complaints regarding cybercrime, with a total dollar loss of $800,492,073. The average dollar loss for victims reporting a loss was $6,472. Most cybercrimes happen to males (52 percent), and most occur to those between the ages of 40 and 59. They are also more likely to occur in California and in the United States (Hill and Marion, 2016).

3.9 The 2014 US State of Cybercrime Report

The 2014 US State of Cybercrime Report was the result of a survey of over 500 U.S. executives and security experts in both the public and private sectors. It was done to determine more about their cybersecurity policies and readiness to combat potential cyber threats.13 The results of this survey indicated that three of four respondents (77 percent) had detected a security breach event in the prior 12 months, and over a third (34 percent) of respondents reported that the number of security events detected had increased over the past year. Not surprisingly, over 59 percent of respondents reported that they were more concerned about cybersecurity issues this year than in the past. The average number of security incidents in 2013 was 135 per organization, though this figure is probably low because it does not include attacks that were not detected. While 14 percent of the respondents reported that their losses due to cybercrime have increased in the past year, over two-thirds (67 percent) of those reporting a security incident were unable to estimate the financial costs. Among those that were able to provide an estimate, the average annual monetary loss was approximately $415,000.15 (Hill and Marion, 2016).

3.10 The 2014 McAfee Report

The 2014 McAfee Report estimated that the annual cost of cybercrime to the global economy was over $400 billion, with conservative estimates at $375 billion and more liberal estimates at $575 billion in losses. When examined more closely, they found that the direct cost of cybercrime was only $875 million, but the recovery and opportunity costs reached $8.5 billion.16 These costs included the expenses related to hundreds of millions of victims who had their personal information stolen and the effects on businesses, such as damage to the brand and other reputational losses as well as harm to customer relations and retention (McAfee Intel Security, 2014)

3.11 The 2014 Identity Theft Resource Center Report

The Identity Theft Resource Center is an agency dedicated to helping victims of identity theft. It provides resources to victims so they can restore their personal records and names as quickly as possible at no cost. The group also provides prevention education and training as a way to prevent identity theft. The agency issues a report each year that documents information on the number of identity thefts that occur. In 2014, the agency reported that the number of U.S. data breaches was 783. Of these, the highest number of breaches was reported by the medical/health care industry at 42.5 percent. The business sector reported the second highest at 33 percent, followed by the government/military sector at 11.7 percent, the education sector at 7.3 percent, and the banking/credit/financial sector at 5.5 percent (Identity Theft Resource Centre, 2014). Hacking was the primary cause of the majority of the breaches. Of course, all of these breaches can lead to the loss of personal data, leading to other crimes such as identity theft.

Generally, the effect of cybercrime in the society is multi-dimensional. It has serious deleterious consequences on individuals, businesses, corporate organizations, and government agencies. At the individual level, some victims of cybercrime suffer great harm after falling for the antics of cybercriminals. They will often spend months, if not years, to clear their credit records. In some cases, the damages suffer go beyond a damaged credit history as a more severe cybercrimes can lead to the death of their victims. Similarly, the impact of cybercrime can be very disastrous for a business that is attacked by cybercriminals. While some cyberattacks result in little or no damage, others cause damages so extensive that a company may never recover. Not only could they lose profits from an attack but it can also impact a company’s image, reputation, and brand image, resulting in a loss of confidence by investors and customers. The company may be forced to shut down temporarily because of malware installed in their computer systems. Even a small attack can compromise a large business. Furthermore, cybercrimes can be particularly harmful to those in the banking and financial industries, where computers are used every day to send and receive funds. Indeed, it is estimated that the number of cybercrimes in financial firms is more than double the number of cybercrimes in other industries. Specifically, it has been estimated that 39 percent of companies that provide financial services suffered from cybercrime compared with 17 percent in other industries (Hill and Marion, 2016). It has been estimated that banking institutions lose billions of dollars each year through fraudulent transactions.

SELF-ASSESSMENT EXERCISE

Explain the reasons making the socio-economic costs of cybercrime difficult to measure.

4.0 CONCLUSION

The socio-economic cost associated with the occurrence of cybercrime is rising significantly for individual Internet uses, Internet Service Providers, businesses, and government agencies. Also, the increasing ubiquity and popularity of the Internet and ICT resources has further expanded the size of the potential victims of cybercriminals. Therefore, this unit analyses the socio-economic costs associated with the occurrence of cybercrime.

5.0 SUMMARY

This unit discusses the negative socio-economic impacts of cybercrime on victims which could be individuals, governments and corporate organizations. The major reasons why the measurement of the socio-economic costs of cybercrime is usually difficult to measure are analyzed. Also, the outcomes of some of previous studies conducted by some globally recognized institutions on the socio-economic costs of cybercrime are presented.

6.0 TUTOR- MARKED ASSIGNMENT

1. The negative impacts of cybercrime are multi-dimensional. Discuss

7.0 REFERENCES/FURTHER READING

Clough, J. (2010). *Principles of Cybercrime*. Cambridge University Press.

Data Breach Investigations Report (2013). The Rise of State-Sponsored Attacks. *Computer Fraud and Security*, May 2013, 1–3.

Detica and Office of Cyber Security and Information Assurance. The cost of cybercrime, Available at http://www.cabinetoffice.gov.uk/resource-library/costof-cyber-crime

Fafinski, S., Dutton, W.H. & Margetts, H. (2010). Mapping and Measuring Cybercrime. Oxford Internet Institute Forum Discussion Paper No. 18., June 2010.

Ghernaouti, S. (2013). *Cyber Power: Crime, Conflict and Security in Cyber Space*. EPFL Press.

Hill, J.B. & Marion, N. E. (2016). *Introduction to Cybercrime, Computer Crimes, Laws, and Policing in the 21st Century*. Praeger Security International Textbook.

Identity Theft Resource Center. (2014). "Breach Report Hits Record High in 2014. Available at http://www.idtheftcenter.org/ITRC-Surveys-Studies/2014databreaches.html.

McAfee Intel Security. (2014). *Net Losses: Estimating the Global Cost of Cybercrime*. Available at http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf.

Norton. (2013). Norton Cybercrime Report. Available at http://www.norton.com/2012cybercrimereport

Richardson, R. (2008). *CSI Computer Crime and Security Survey*. Computer Security Institute.

Rush, H., Chris, S., Erika, K. M., & Puay, T. (2009). Crime online: Cybercrime and illegal innovation, Research report: July 2009, CENTRIM, University of Brighton. Available at http://eprints.brighton.ac.uk/5800/01/Crime_Online.pdf.

United Nations Office on Drugs and Crime (2013). Comprehensive Study on Cybercrime. UNODC, Vienna.

MODULE 3 CYBERCRIME AND LAW ENFORCEMENT

Unit 1 Cybercrime and Transnational Legal Jurisdictions
Unit 2 International Legislative Efforts for Tackling Cybercrime
Unit 3 Challenges Associated with Cybercrime Prosecution
Unit 4 Agencies and Organizations Monitoring Cybercrime
Unit 5 Nigerian Government Efforts at Tackling Cybercrime

UNIT 1 CYBERCRIME PROSECUTION AND THE TRANSNATIONAL LEGAL JURISDICTIONS ISSUES

CONTENTS

1.0 Introduction
2.0 Objectives
3.0 Main Content
3.1 Cybercrime Prosecution and the Transnational Legal Jurisdiction Issues
4.0 Conclusion
5.0 Summary
6.0 Tutor -Marked Assignment
7.0 References/Further Reading

1.0 INTRODUCTION

Different efforts have been made through the enactment of laws and legislations by governments at national, regional and international levels to combat the scourge of cybercrime. For example, the Federal Government of Nigeria signed the Nigeria’s Cybercrime Act into law in 2015. In spite of the fact that nation-states have recognized the devastating impacts of cybercrime and are making efforts tackle it, the prosecution of cybercrime cases often comes with series of challenges because there are usually some transnational legal jurisdictions issues that are usually embedded in it.

2.0 OBJECTIVES

At the end of this Unit, you should be able to:

- discuss the transnational laws that have been instituted by government of different countries to tackle the menace of cybercrime and the activities of cybercriminals or internet monitoring groups to prosecute cybercriminals.

- explain different forms of punishment designated for liable cybercriminals in different countries of the world
- describe the problem of the unification of these laws due to the borderless nature of cybercrime.

3.0 MAIN CONTENT

3.1 Cybercrime Prosecution and the Transnational Legal Jurisdictions Issues

The largest populations of actors engaged in the identification of illegal activity online are Internet users. Due to the size of the World Wide Web and the various applications individuals use to communicate and share materials, it is virtually impossible for law enforcement to observe when most wrongdoing takes place online (Wall, 2001). As a result, the individuals actively engaged in online communities have the ability to observe and communicate when cybercrimes take place. They may not actively share this information with formal law enforcement agencies, however, which limits their efficacy in combating cybercrime (Holt & Bossler, 2016).

Beyond end users, Internet service providers, or ISPs, play a critical role in dealing with cybercrime. Though they are primarily owned and operated as for-profit businesses, some ISPs may also be universities, public libraries, and other entities that may not be traditional businesses. ISPs play a twofold role in the identification and management of cybercrimes: (1) they host and provide access to online content and have a formal legal obligation to remove harmful material; and (2) they provide Internet connectivity for individuals and require that users comply with all applicable local and federal laws (Holt & Bossler, 2016). ISPs have become a conduit for the identification of various forms of cybercrime, such as digital piracy, as they may be able to identify when individual users engage in file sharing or violate existing user agreements (Nhan, 2013). Similar to ISPs, corporate security personnel are tasked with the protection and management of the assets of their organization, including sensitive information. Corporate security officers play a unique position as gatekeepers to law enforcement agencies in the event that either their organization is compromised or internal resources are used in the course of a cybercrime.

Due to the increasing recognition of the pervasiveness of cybercrime and the magnitude of the danger it poses, different efforts are being made being at the local, regional, national, and international levels to address it. Legal measures play a key role in the prevention and combating of cybercrime. These are required in all areas, including criminalization, procedural powers, jurisdiction, international cooperation, and internet service provider responsibility and liability. At the national level, both existing and new (or planned), cybercrime laws most often concern criminalization, indicating a predominant focus on establishing specialized offences for core cybercrime acts. Countries increasingly recognize, however, the need for legislation in other areas (UNODC, 2013). Compared to existing laws, new or planned cybercrime laws more frequently address investigative measures, jurisdiction, electronic evidence and international cooperation.

By the 1980s, serious attempts aimed at controlling cybercrime started emerging globally because new forms of cybercrimes were surfacing at this time, and the general public was also having a better understanding of the potential dangers of associated with this form of crime. During this period, different anti-cybercrime legislations began to be passed into laws to deter potential cybercriminals and punish those convicted of these new crimes. The Canadian government was the first to enact a national law to address computer crime when they amended their Criminal Code in 1983 (Hill and Marion, 2016). Also, in Australia, the Australian Crimes Act was amended in 1989 to include Offenses Relating to Computers (Section 76), and the Australian states enacted similar laws at around the same time. In Britain, the Computer Abuse Act was passed in 1990 to criminalize computer intrusions. In the United States, the Federal Computer Fraud and Abuse Act was passed by Congress in 1984 and then amended in 1986, 1988, 1989, and 1990 (Hills and Marion, 2016).

Generally, most of the laws enacted against cybercrime and the activities of cybercriminals pertain to the issue in a particular country rather than internationally. Hence, the laws each country has passed to reduce cybercrime vary greatly (Hills and Marion, 2016). For instance, in Israel, the section 4 of the Computer Law of 1995 states that any person who unlawfully obtains access to data in a computer shall be sentenced to imprisonment not exceeding three years. In Italy, the Penal Code Article 615 stipulates that those who have unauthorized access into a computer or telecommunication system that is protected by security measures, or who remains in that site against the expressed or implied will of the one who has the right to exclude him, shall be sentenced to imprisonment not exceeding three years. If that person uses violence to commit the crime, of if the act causes the destruction or the damage to the system, then the punishment is either a sentence of one to five years or three to eight years' imprisonment, respectively.

The Malaysian law concerning cybercrimes is the Computer Crimes Act of 1997. The Part II of the law states that a person is guilty of an offense if he or she causes a computer to perform any function with the intent to secure access to any program or data held in any computer that is unauthorized if the person knows at the time that the program is unauthorized. In Norway, the relevant law is Penal Code 145, which states that any person who unlawfully opens a closed document or in some manner gains access to its contents, shall be liable to fines or to imprisonment for a term not exceeding six months. In 2003, the United Kingdom introduced a legislation requiring people to “opt in” to unsolicited emails. Called the Privacy and Electronic Communications Regulations, the law outlawed spam email without the prior consent of the recipient. In South Africa, The Electronic Communications and Transactions Act of 2002 outlaws the unauthorized access to, interception of, or interference with data. Anyone who breaks this law faces a fine or imprisonment not exceeding 12 months. The Philippine government passed an act providing for the recognition and use of electronic commercial and noncommercial transactions. Those who violate the law are subject to a fine and a mandatory term of imprisonment from six months to three years. The German Penal Code has many provisions related to cybercrime, including Section 202a on data espionage, Section 303 on alteration of data, and Section 303b on computer sabotage.

In the Computer Misuse Act of 1990 enacted in England, three new offenses were defined: unauthorized access to a computer, unauthorized access with intent to commit or facilitate the commission of further offenses, and unauthorized modification of computer material. The Police and Justice Act of 2006 amended that law. The courts have also relied on the U.K. Criminal Damage Act of 1971 to prosecute computer crimes. The Protection of Children Act of 1978 protects children in child pornography. The offenses of fraud and forgery are found in the Fraud Act of 2006 as well as the Forgery and Counterfeiting Act of 1981. Copyright statutes are found in the Copyright and Rights Related Acts.
In Australia, the Federal Cybercrime Act of 2001 amended the Criminal Code Act of 1995 to replace existing outdated computer offenses. In it, a person is deemed guilty of an offense if he or she causes any unauthorized access to, or modification of, restricted data; intends to cause the access or modification; and knows that the access or modification is unauthorized. One or more of the following must also apply: the restricted data is held in a Commonwealth computer or held on behalf of the Commonwealth and the access to, or modification of, the restricted data is caused by means of a telecommunications service. The penalty is two years in prison. In Austria, The Privacy Act of 2000: Section 10 states: Provided that the offenses does not meet the statutory definition of a punishable action within the relevant jurisdiction of the court nor is threatened by a more severe punishment under a different administrative penalty clause, a minor administrative offense shall be pronounced with a fine of up to S260.00.

Parties who: 1. willfully obtain unlawful access to a data application or willfully maintain discernible, unlawful and deliberate access.
2. Intentionally transmit data in violation of the Data Secrecy Clause (Section 15), especially data that were entrusted to him/her according to Section 46 and Section 47, for intentional use for other purposes or, 3. use data contrary to a legal judgment or decision, withhold data, fail to correct false data, fail to delete data, or 4. intentionally delete data contrary to (S) 26, Section 7 Brazil Law no. 9,983 of July 14, 2000: has been adopted covering provisions A. Entry of False Data into the Information System: Entry, or facilitation on the part of an unauthorized employee of the entry, of false data, improper alteration or exclusion of correct data with respect to the information system or the data bank of the Public Management for purposes of achieving an improper advantage for himself or for some other person, or of causing damages. Penalty is imprisonment for 2 to 12 years, and fines B. Unauthorized Modification or Alteration of The Information System: article 313-B: Modification or alteration of the information system or computer program by an employee, without authorization by or at the request of a competent authority; penalty: detention for three months to two years and fines (Hill and Marion, 2016).

Finally, the Canadian Criminal Code Section 342.1 states: 1. Everyone who fraudulently and without color of right, (a.) obtains directly or indirectly, any computer service, (b.) by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system (c.) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offense under paragraph (a) or (b) or an offense under section 430 in relation to data or a computer system, or d. uses, possesses, traffics in or permits another person to have access to a computer password that would enable a person to commit an offenses under paragraph (a), (b), or (c) is guilty of an indictable offense is liable to imprisonment for a term not exceeding ten years or is guilty of an offense punishable on summary conviction.
Generally, most of these federal laws that were enacted for the purpose of facilitating cybercrime investigation serve one or more of the following four primary purposes: (1) protect individual privacy while providing access to information held by the federal government, (2) secure information systems within the federal government, (3) ensure national critical information infrastructure along with its availability and reliability, or (4) specify illegal behaviors that involve using the Internet, information systems, or other electronic information technology (IT) devices (McQuade, 2009). In spite of these, the laws pertaining to cybercrime in each country are different, and there are a wide variety of approaches to containing cybercrime. This has serious implications for dealing with cybercrime and for the prosecution of cybercriminals.

Typically, the following are some of the questions that normally arise whenever an international cybercrime occurs: What country is responsible for investigating the crime, under what legal code, and what punishment would the offender receive? (Hill and Marion, 2009). Consequently, because of these observed inconsistencies in the laws of different countries, it is often possible for some computer offenders to go free after committing offenses, without facing any criminal sanctions for their actions.

Domestic legislations are clearly necessary to discourage cybercrime offenders. However, with the way that cybercrime is now committed, various problems make the use of domestic regulation by itself unworkable (Chawki et al. 2015). Indeed, acts on the internet that are legal in the country where they are initiated, may be illegal in other countries, even though the act is not particularly targeted at that single country (Chawki et al. 2015). Indeed, jurisdiction conflicts abound, both negative (no country claims jurisdiction) and positive (several countries claim jurisdiction at the same time).

Due to its transnational nature, cybercrime is a borderless crime. Unlike the conventional crime where geographical border separates jurisdictions (this can be in form of a state boundary, a national boundary, or an international boundary), and which ultimately defines the offense and the agency that has the power to enforce any relevant laws and arrest an offender, these easily identifiable boundaries do not exist when it comes to cybercrimes. A cybercrime can be committed in one country toward a victim in another country, thousands of miles away. Because every nation is connected to the Internet, cybercriminals can commit offenses from anywhere, and victims can be from anywhere. Moreover, offenders can be very mobile, moving from one place to the next very quickly. The borderless nature of cybercrime also means that any nation can be targeted and its citizens victimized from anywhere in the world. This makes it very difficult, if not impossible, for law enforcement to determine the country in which the crime was actually committed and then to locate the specific offender. If an offender is found, it may be unclear what agency should have jurisdiction to adjudicate the offense.

The current international cooperation picture risks the emergence of country clusters that have the necessary powers and procedures to cooperate amongst themselves, but are restricted, for all other countries, to ‘traditional’ modes of international cooperation that take no account of the specificities of electronic evidence and the global nature of cybercrime. This is particularly the case for cooperation in investigative actions (UNODC, 2013). A lack of common approach, including within current multilateral cybercrime instruments, means that requests for actions, such as expedited preservation of data outside of those countries with international obligations to ensure such a facility and to make it available upon request, may not be easily fulfilled. The inclusion of this power in the draft African Union Cybersecurity Convention may go some way towards closing this lacuna. Globally, divergences in the scope of cooperation provisions in multilateral and bilateral instruments, a lack of response time obligation, a lack of agreement on permissible direct access to extraterritorial data, multiple informal law enforcement networks, and variance in cooperation safeguards, represent significant challenges to effective international cooperation regarding electronic evidence in criminal matters (UNODC, 2013).

Another important issue bordering on the impact of transnational jurisdiction on the prosecution of cybercrime is variation in nations' level of tolerance to this form of crime. It is a fact that not all countries are equally distressed by cybercrime. Although it may not be a publicly declared policy, some nation states are tolerant of international cybercrime and make no effort to prosecute cybercriminals (Waschke, 2017). In extreme cases, the criminal act appears to be an instrument of government policy. Therefore, when cybercriminals hide behind practices like this, prosecuting them will be very difficult, if not unachievable. Hence, these locations have become cybercriminal havens. Consequently, international cybercriminals who keep the damage to each victim low enough can often get a free pass.

The high volume of offences on the internet and the lack of international boundaries require the cooperation and sharing of information between and among national and international police departments, government legislators, and the public and private sectors (Waschke, 2017). However, some issues seem to make it difficult to reach a consensus on the contents of such legal rules. For instance, many countries have not yet framed a balance between security and privacy concerns, thus delaying the process of approving procedural rules (Chawki et al., 2015). Some other countries resist against joining any international convention which they have not negotiated since its inception, or where they do not have equal opportunity for voicing views or claims. The outcome has been that a large number of countries still lack adequate cybercrime legislation and/or have not yet acceded to existing relevant Budapest Convention which was adopted by the Council of Europe in 2001. After 15 years, 49 nation states have ratified it, mostly in Europe, but non-European states such as the United States, Australia, Canada, Israel, and Japan have also ratified it (Waschke, 2017). Non-signatories protest that the convention intrudes on their national sovereignty. North and South Korea, Russia, China, and India are notable non-signatories.

As is the case for all security activities, the struggle against cyber criminality is based on political willingness and needs to follow a global approach that corresponds to a shared vision of public security, so as to provide efficient and effective protection for citizens, countries, and the fundamental values of democratic societies (Clough, 2010). The protection of fundamental rights includes, specifically, the protection of personal data and the protection of individuals in respect to the automated processing of personal data. It will be necessary, then, to acquire the means to implement a genuine security response, rather than to create a pseudo-security framework based on excessive social control that increasingly relies upon sophisticated and virtually invisible electronic surveillance – methods that reduce individual freedoms in the name of a relative collective security (Clough, 2010).

One of the major matters at stake in the fight against cyber criminality is the development of a genuine information culture that is not simply focused on security and based on fear. With cybersecurity it is not sufficient to make the population aware of the dangers of the Internet and the elementary precautions to be taken. Essentially all the players, i.e. all the service and technology providers, will need to accept responsibility for their role in the global and collective struggle (Clough, 2010). Mounting an effective response to cyber criminality is based upon developing a preventive approach that will make cyberspace a less attractive environment for committing crimes and also reduce the number of opportunities for criminal activities. To achieve this, it will be necessary to increase the level of difficulty of carrying out cyberattacks and increase the risks taken by criminals in going about their business (dissuasive measures), while all the time decreasing the expected profits. This kind of approach will require both reducing technical, organisational, and human vulnerabilities in order to increase the level of effort, difficulty, and investment required by the criminals, and possessing and knowing how to use the tools, procedures, and measures necessary to increase the risk for the criminals that they will be identified, localised, and pursued. Therefore, it will be necessary to reinforce the robustness and the resilience of IT and telecommunications infrastructures by reducing their vulnerabilities, protecting them through coherent technical, procedural and managerial security measures, and having recourse to an effective justice and police system. Thus, the whole process requires the combination of political will, legal, organisational, procedural, technical and human means, the establishment of partnerships between the public and private sectors, and good international cooperation (Clough, 2010).

SELF-ASSESSMENT EXERCISE

With relevant examples, discuss the efforts being made by countries to address the menace of cybercrime.

4.0 CONCLUSION

This unit exposes students to some of the laws and legislations that have been formulated in different parts of the world to tackle the problem of cybercrime and to curb the activities of cybercriminals. It also discusses the major challenges that are embedded in some of these laws and the typical challenges that are associated with their application. Furthermore, it explains how cybercrime prosecution efforts of a country can impact on another country’s sovereignty, a situation which often bring the issue of non-consensus among countries in the drive towards collectively instituting laws for the prosecution of cybercriminals.

5.0 SUMMARY

The main focus of this unit is on the efforts being made at local, national, regional and international levels towards combatting the menace of cybercrime. Equally, it x-rays some of the major transnational-jurisdictional challenges that are associated with the application of some of the extant laws and legislations in the prosecution of cybercriminals.

6.0 TUTOR-MARKED ASSIGNMENT

1. Discuss the major transnational-jurisdictional challenges that are embedded in the prosecution of cybercriminals

7.0 REFERENCES/FURTHER READING

Chawki, M., Darwish, A. Khan, M. B. & Tyagi, S. (2015). *Cybercrime, Digital Forensics and Jurisdiction*. Springer International Publishing.

Clough, J. (2010). *Principles of Cybercrime*. Cambridge University Press.

Hill, J.B. & Marion, N. E. (2016). *Introduction to Cybercrime, Computer Crimes, Laws, and Policing in the 21st Century*. Praeger Security International Textbook.

Holt, T. J. & Bossler, A. M. (2016). *Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses*. Routledge.

McQuade, S. C. (2009). *Encyclopedia of Cybercrime*. Green Wood Publishing Group.

Nhan, J. (2013). The evolution of online piracy: Challenge and response. In T.J. Holt (Ed.), *Crime On-line: Causes, Correlates, and Context* (pp. 61–80). Raleigh, NC: Carolina Academic Press.

Tiemo, P. A., Bribena, E., & Nowosu, O. (2010). Internet usage and regulations in Niger Delta University Libraries. Retrieved on 20th September 2015 from Chinese Librarianship: an International Electronic Journal, 31. URL: http://www.iclc.us/cliej/cl31TBN.pdf.

United Nations Office on Drugs and Crime (2013). Comprehensive Study on Cybercrime. UNODC, Vienna.

Waschke, M. (2017). *Personal Cybersecurity: How to Avoid and Recover from Cybercrime*. Bellingham, Washington, USA.

UNIT 2 CHALLENGES CONFRONTING LAW ENFORCEMENT AGENTS IN CYBERCRIME CONTROL

CONTENTS

1.0 Introduction
2.0 Objectives
3.0 Main Content
3.1 Challenges Confronting Law Enforcement Agents in the Cyber crime Control
4.0 Conclusion
5.0 Summary
6.0 Tutor -Marked Assignment
7.0 References/Further Reading

1.0 INTRODUCTION

Law enforcement agencies are charged with the important responsibility of maintaining law and order. Therefore, they are at the forefront of the war that is being waged against cybercriminals victimizing people on the cyberspace. Although law enforcement agents are making headway in this regard, yet, the rate of their success has consistently been hindered by some certain challenges. Hence, explanations will be provided in this unit on the challenges confronting law enforcement agents in the control of cybercrime.

2.0 OBJECTIVES

At the end of this Unit, you should be able to:

- list the challenges being faced by law enforcement agencies across the world in their obligation of maintaining law and order on the cyberspace
- understand the conventional and emerging challenges that law enforcement agents are confronting in their fight against cybercrime.

3.0 MAIN CONTENT

3.1 Challenges Confronting Law Enforcement Agents in the Cybercrime Control

The peculiarity of cybercrime poses multiple challenges for law enforcement personnel across the world. Generally, the *newness,* amorphous and transnational nature of cybercrime has serious implications for the overall ability of local and international law enforcement agencies to adequately control it. Due to the continuous advancements that is being witnessed in the area of technological development, new crimes that are initially unfamiliar to law enforcement agencies are emerging globally. Indeed, it has been estimated that only 5 percent of cybercriminals are ever arrested or convicted because the anonymity associated with web activity makes them hard to catch, and the trail of evidence needed to link them to a cybercrime is usually difficult to unravel (Hill and Marion, 2016). Some of the major challenges hindering law enforcement efforts at tackling cybercrime are highlighted and discussed below:

(a) Inter-jurisdictional Issues

As seen in the preceding unit, the transnational nature of cybercrime is often creating a serious challenge for law enforcement officials because the illegal act of a cybercriminal(s) on the cyberspace may affect victims residing in different countries. Consequently, the borderless nature of cybercrime often makes it very difficult for law enforcement to determine the country in which the crime was actually committed and then to locate the specific offender. Even if an offender is found, it may be unclear as to what agency should have jurisdiction to adjudicate the offense. Because of this typical confusion, many cybercriminals are not pursued, and if they are located, they may not be punished (Hill and Marion, 2016). Additionally, even if the jurisdictions can be determined and the perpetrator of a cybercrime can be found and a solid case established, the difficulties are not over when the perpetrator is not in the same jurisdiction as the victim. In that case, the perpetrator must be extradited to be prosecuted. Extradition is a complex and expensive process. However, it is a necessary procedure because a law enforcement authority can only prosecute a suspect within in their jurisdiction. Nevertheless, the sad reality is that extradition for cybercrimes tends to be more difficult than the conventional crime because conventional crime laws tend to be more consistent across jurisdictions than cybercrime laws.

(b) Cyber Victimizations are Often Unreported

Another major challenge that normally confronts law enforcement agents in the control of cybercrime is the unwillingness of victims to report their victimization experiences to relevant law enforcement agencies. Due to the sophistication of cybercriminals, some of the victims may not be aware that they have been victimized. Also, some victims may feel too embarrassed to report their experience because they feel they are partly responsible for their own misfortune by responding to a phishing email or for falling for a scam. Equally, businesses and corporate institutions are often unwilling to bring their loss to the attention of law enforcement officials because of fear of the envisaged potential liability that the action is likely to attract. The implication of this is that law enforcement officials continue to find it difficult to tackle the problem of cybercrime because of the under-reporting of incidents by victims.

(c) Low-Technical Knowledge of Law Enforcement Officials on Cybercrime

Due to the relative newness of cybercrime, many law enforcement officials across the world are yet to adequately develop necessary skills and strategies for detecting, preventing and combatting cybercrime. Although while the United State of America, China, and some European nations have made considerable progress in this regard by establishing specialized and dedicated cybercrime police units and departments, the majority of law enforcement agencies in African and Asian countries are still largely ill equipped and have poorly trained with regard to cybercrime policing. Consequently, the deployment of conventional policing strategies and approaches for dealing with traditional crimes for tackling cybercrime is a very serious challenge limiting the success of the fight against it. Similarly, despite the fact the costs associated with a cyber investigation can be extremely high due to their lengthy process, most law enforcement agencies do not have adequate resources to track cybercriminals.

(d) Socio-Cultural Variations in Cybercrime Designation

The transnational characteristic of cybercrime means that it is affecting nations with dissimilar socio-cultural backgrounds which ultimately inform nations and law enforcement officials perspectives on cybercrime. Consequently, the varied perceptions of acts designated as cybercrime may impact negatively on the level of cooperation amongst law enforcement officials as regards the prosecution of some cybercriminals. In essence, an act that is considered to be illegal or morally offensive in one country may be permissible and considered acceptable in another. For instance, acts amounting to cyber pornography considered illegal in some nations may be permissible in some other countries. Also, some statements and posts made on the cyberspace that may constitute hate speech under authoritarian regimes in some countries may not be viewed as such in nations practicing democracy.

(e) The Non-Static Nature of Cybercrime

The non-static and ever-changing nature of cybercrime also constitutes serious barrier in the drive of relevant law enforcement agencies towards addressing the problem. Although while it is true that many countries have enacted laws to tackle the antics of cybercriminals, the ever-changing nature and the newness of cybercrime is increasingly making some extant laws targeted at addressing it ineffective and outdated as they become easily overtaken by new criminal events. Generally, the reality is that whenever anti-cybercrime laws are passed, they become outdated or obsolete in a very short period of time.

(f) The Mobile Nature of Cybercriminals

Cyber offenders are rational beings who always take adequate precautions to evade arrest. Thus, they are highly mobile individuals. Equally, the portable nature of computer system and other ICT devices that can be used for the perpetration of cybercrime also constitute an advantage for the cybercriminals as they can easily move from one location with their *instruments* of crime. Consequently, this poses serious problems for law enforcement because technologically sophisticated cybercriminals know how to hide their tracks and any evidence of their crimes. They may commit the crime (i.e., a phishing operation) only for a short time in one location before moving to a different place (Hill and Marion, 2016). Indeed, many cybercrimes begin in locations so remote that it is difficult for law enforcement to determine the country in which a crime was committed. By the time an offense is discovered, the offender has moved to another location and little evidence remains.

SELF-ASSESSMENT EXERCISE
Identify and discuss the challenges confronting law enforcement agents in the fight against cybercrime.

4.0. CONCLUSION

Cybercrime is a universal crime affecting all nations of the world. The potency of the deleterious effects of this crime is compelling governments and law enforcement agencies to design different strategies to confront it. However, different challenges are inhibiting law enforcement agents' efforts at combatting cybercrime and the activities of cybercriminals.

6.0 SUMMARY

This unit exposes students to the challenges being faced by law enforcement agencies as regards the prosecution of cybercrime. It was pointed out in the discourse that multiple institutional and non-institutional constitute serious barriers to law enforcement agencies efforts towards combatting cybercrime.

5.0 TUTOR- MARKED ASSIGNMENT

1. Suggests ways through which the fight against cybercrime in Nigeria can be made more effective

7.0 REFERENCES/FURTHER READING

Clough, J. (2010). *Principles of Cybercrime*. Cambridge University Press.

Hill, J. B. & Marion, N. E. (2016). *Introduction to Cybercrime, Computer Crimes, Laws, and Policing in the 21st Century*. Praeger Security International Textbook.

UNIT 3 AGENCIES AND ORGANIZATIONS MONITORING CYBERCRIME

CONTENTS

1.0 Introduction
2.0 Objectives
3.0 Main Content
3.1 Agencies and Organizations Monitoring Cybercrime
4.0 Conclusion
5.0 Summary
6.0 Tutor- Marked Assignment
7.0 References/Further Reading

1.0 INTRODUCTION

Due to the increasing recognition of the deleterious impacts of cybercrime on individuals, businesses, governments and nations, some international agencies and organizations have come up with their own strategic frameworks aimed at tackling illegal and clandestine behaviours on the cyberspace and to combat the inimical activities of cyber cybercriminals.

2.0 OBJECTIVES

At the end of this Unit, you should be able to:

- state various efforts that are being made by some regional and multilateral agencies and organizations to tackle the menace of cybercrime
- discuss the illegal activities of criminals victimizing Internet users and information and communication technology security landscapes and architectures.

3.0 MAIN CONTENT

3.1 Agencies and Organizations Monitoring Cybercrime

A transnational dimension to a cybercrime offence arises where an element or substantial effect of the offence is in another territory, or where part of the modus operandi of the offence is in another territory (UNODC, 2013). International law provides for a number of bases of jurisdiction over such acts, including forms of territory-based jurisdiction and nationality-based jurisdiction. Some of these bases are also found in multilateral cybercrime instruments. While all countries in Europe consider that national laws provide a sufficient framework for the criminalization and prosecution of extraterritorial cybercrime acts, around one-third to over one-half of countries in other regions of the world report insufficient frameworks. In many countries, provisions reflect the idea that the 'whole' offence need not take place within the country in order to assert territorial jurisdiction. Territorial linkages can be made with reference to elements or effects of the act, or the location of computer systems or data utilized for the offence (UNODC, 2013). Where they arise, jurisdictional conflicts are typically resolved through formal and informal consultations between countries.

Cybercrime is a borderless crime that is neither affected by space nor time limitations. Therefore, many agencies and organizations across the world have developed some strategies aimed at tackling this transnational crime. The last decade has seen significant developments in the promulgation of international and regional instruments aimed at countering cybercrime. These include binding and non-binding instruments. Five clusters can be identified, consisting of instruments developed in the context of, or inspired by: (i) the Council of Europe or the European Union, (ii) the Commonwealth of Independent States or the Shanghai Cooperation Organization, (iii) intergovernmental African organizations, (iv) the League of Arab States, and (v) the United Nations (UNODC, 2013).

A significant amount of cross-fertilization exists between all instruments, including, in particular, concepts and approaches developed in the Council of Europe Convention on Cybercrime. Analysis of the articles of 19 multilateral instruments relevant to cybercrime shows common core provisions, but also significant divergence in substantive areas addressed. Globally, 82 countries have signed and/or ratified a binding cybercrime instrument. In addition to formal membership and implementation, multilateral cybercrime instruments have influenced national laws indirectly, through use as a model by non-States parties, or via the influence of legislation of States parties on other countries. Membership of a multilateral cybercrime instrument corresponds with the perception of increased sufficiency of national criminal and procedural law, indicating that current multilateral provisions in these areas are generally considered effective (UNODC, 2013).
Some of the international agencies and organizations that have been playing prominent roles in the fight against cybercrime are highlighted and discussed in this section:

(i) The United Nations

In the early 1990s, the UN Resolution 45/121 endorsed the recommendations of the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders. It called upon Member States to intensify efforts towards combatting computer crimes.

In 2001, the UN General Assembly Resolutions 55/63 and 56/121 on “Combating the criminal misuse of information technologies” were passed. The resolutions advocated a global framework to counter cybercrimes. The Resolutions 57/239 in 2002 and 58/199 in 2004 encouraged Member States to create a global culture of cybersecurity and to take action to protect critical infrastructure. The ITU, a UN Chartered organization, also developed the Tool kit for Cybercrime Legislation. The Toolkit intends to help develop “cybercrime legislation that is globally applicable and interoperable with existing national and regional legislative measures” (ITU, 2009). As of October 2009, the ITU had 191 countries and 700 organizations as its members. In 2007, the ITU announced a 2 years plan to combat cybercrime. Equally, it collaborated with the Malaysian company IMPACT to develop a system to help prevent, defend, and respond to cyber threats. In 2009, the ITU and IMPACT announced that they had successfully developed the Global Response Center. The Center provides an early warning system by bringing the global threat intelligence on a near real-time basis and helps identify threats that are associated with a country (Schlein, 2009).

(ii) The G8 High Tech Crime Working Group

The Group of 8, or G8, is composed of Canada, France, Germany, Italy, Japan, Russia, the United Kingdom, and the United States. The G8’s Subgroup on High Tech Crime is one of the five subgroups of the “Lyon Group” created to implement the Forty Recommendations adopted by the G8 in 1996 (Kschetri, 2010). The Subgroup was created in January 1997; and it adopted the “Ten Principles” to combat computer crimes. This Subgroup’s mission is to enhance the abilities to combat high-technology crimes. It was subsequently expanded to include the non-G8 countries. In May 2001, the G8 Government/Private Sector High Level Meeting on High Tech Crime held in Tokyo covered five major themes: data retention, data preservation, threat assessment and prevention, protection of electronic commerce, and user authentication and training (Miyake, 2001).The G8 crime policy domain has been developing for some time, with initial concentration upon political issues such as terrorism and extradition, but later drugs and declarations by the Heads of State about global crime problems. The move from rhetoric about crime and globalization to specific action against transnational organized crimes emanates from the decision of the 1995 G8 Summit (Halifax) to create the Senior Expert Group on Transnational organized crime (Kschetri, 2010). Its initially temporary mandate was to develop a wider-ranging but specific set of measures for states to adopt in their action against organized crime, which were presented to *Recommendation to Combat Transnational Organized Crime Efficiently* at the G7-P8 Summit (Lyon) in April 1996.

The European Commission

The European Commission is the executive board that oversees the European Union. It is a group of 28 representatives from nations located primarily in Europe. It makes policies and recommends legislation to member states on different issues of concern to European nations. Cybercrime is one of those policy areas. In 1995, the European Commission announced a Data Protection Directive. This document focused on protecting personal data on the Internet. A revised document was published in November 2011. Under the new document, mandatory data breach disclosure laws were extended to include telecommunication companies and Internet service providers. In 2013, the European Commission considered new laws on cybercrime. One of those would require all European organizations, such as banks, power companies, airports, hospitals, and industries, to report all serious cyberattacks on their systems. Only very small organizations (those with under 10 employees) would not be required to do this. The European Commission also issued a strategy for incident reporting titled "An Open, Safe and Secure Cyberspace." It announced proposals that became the Directive on Network and Information Security and was intended to ensure a common level of network and information security across Europe. Once the directive was announced, it would be up to individual member states to determine how to enact this directive in their own countries. Under the directive, member states were asked to launch a minimum level of network security by setting up Computer Emergency Response Teams and by adopting national strategies and modes of cooperation. Additionally, those who operate critical infrastructure organizations will be required to assess potential risks in their organizations and approve appropriate policies to ensure the safety of computer systems (Kschetri, 2010). The aim of the strategy is to harden smart grids and industrial control systems, fight botnets, raise security awareness, develop security standards, encourage research, and develop industrial and technical resources (Hill and Marion).

(iii) The North American Treaty Organization (NATO)

NATO (the North American Treaty Organization) is made up of 28 member states that cooperate on issues of defense and security. The long-term aim of the organization is to prevent conflict between nations. NATO has established a Computer Incident Response Capability (NCIRC) that is responsible for the cyber defense of all NATO sites around the world. If an attack were to occur, experts would meet and devise a response plan to restore the computer systems and return the situation to normal as quickly as possible with minimum loss of data and damage to computers. In October 2013, NCIRC upgraded its computer systems so it would be better protected. In 2012, NATO established rapid reaction teams that would assist member states in the case of an attack. The teams offer technical assistance to members, especially to countries that have not developed resources for their own cyber defense (Kschetri, 2010). Each team has a permanent core of six trained experts. Other professionals may join a team as needed. Each team has the necessary equipment to conduct an investigation, such as satellite telephones, equipment for digital evidence collection, cryptography, digital forensic analysis, vulnerability management, and network security. Once a rapid reaction team is activated, it responds within 24 hours (Kschetri, 2010).

(iv) The Asia-Pacific Economic Cooperation

The Asia-Pacific Economic Cooperation is a group of 21 nations. Its primary goal is to support trade and economic issues in the Asia-Pacific region. Its membership is divided into steering groups that recommend policies to the entire group. The Security and Prosperity Steering Group works with cybercrime issues. When it comes to crimes on the Internet, the steering group works to, among other things, promote security, trust, and confidence in computer networks and e-commerce. They encourage Computer Emergency Response Teams and Computer Security Incident Response Teams. A major topic is the prevention of spam, spyware, and other cybercrimes. The group sponsors training sessions and workshops to educate businesses about preventing and responding to cybercrime.

(v) The Association of Southeast Asian Nations

The Association of Southeast Asian Nations (ASEAN) is a group of 10 nations that cooperate to support economic growth, peace, and stability in the region. One way the group does this is to make policies regarding cybercrime. ASEAN has been committed to addressing cybercrime as a security threat. In 2014, its Senior Officials Meeting on Transnational Crime (SOMTC) finalized a road map or plan for combating cybercrime that included increased regional cooperation for training, law enforcement, and legal matters.

(vi) Organization for Economic Cooperation and Development (OECD)

The Organization for Economic Cooperation and Development (OECD) was created in 1961 as a way of enabling member countries to work together to promote policies that improve the economic and social well-being of people around the world. Through the OECD, governments can share information on many problems that affect people’s lives, predict future trends, and set standards on a wide range of topics. In 2012, OECD studied cybercrime and noted that it has now become a national priority for many countries. However, a major concern is how to leave the Internet free, open, and a platform for innovation and growth, while at the same time making it a secure place that businesses, individuals and governments can use for their needed functions. The final report highlighted suggestions made by business, individuals, and the Internet community as to how to protect users from harm while at the same time supporting the Internet (Kschetri, 2010). OECD has also written reports on malware and ways to reduce the risks of cybercrime.

(vii) The Council of Europe Cybercrime Treaty (CECT)

In 1997, the 41-nations Council of Europe (CoE) started working on international cooperation on cybercrime. The ambition of the group was to build on its binding International Treaty on Cybercrime. In November 2000, the Council released the 22nd draft of its treaty (BBCNewsOnline,2000). In April 2008, the Council settled on voluntary guidelines to strengthen cooperation between the police and Internet service companies (Carvajal, 2008). Its Cybercrime Convention asks signatory countries to enact legislation criminalizing the Convention-specified cybercrime categories (Council of Europe, 2001). As of August 2009, 46 nations including four non-member states of the CoE (Canada, Japan, South Africa, and the United State) had signed the Treaty and 26 of them including the United State ratified it (COE, 2009). The US Senate had approved the Treaty in August 2006 (Chertoff, 2009). One of the goals of the CoE is to harmonize laws against cybercrime. It also aims to ensure that police forces and investigators in individual countries follow standard evidence-gathering techniques and promote the use of latest technology for tracking and catching cyber-criminals. In its 4th Annual Octopus Conference against Cybercrime held in Strasbourg, France in March 2009, the CoE launched the second phase (March 2009–June 2011) of its project. The CoE intends to help countries worldwide to implement its Convention. For instance, as of the early 2009, Laos and Cambodia had no computer crime laws. However, the Council translated the Convention into the Lao language, which provided a groundwork for cybercrime laws in the country (Kirk, 2009). In May 2007, the European Commission pledged to support the implementation of the Convention on Cybercrime worldwide. Over 100 countries in the world are using the Convention as a framework to develop their cybercrime-related regulative institutions (COE, 2009). Countries outside the CoE have been invited to join the Treaty. That is, a non-CoE member conforms to the Treaty like a CoE member. Many non-CoE countries have also joined the Convention (Britt, 2008; Cybercrime Law, 2009).

(viii) The Internet Crime Complaint Centre (IC3)

One of the prominent non-governmental agencies dealing with cybercrime in the USA is the Internet Crime Complaint Center (IC3) that was created in 2000. The IC3 was established in 2000 as a publicly funded, joint operation of the FBI, the Bureau of Justice Assistance (BJA), and the National White Collar Crime Center (NWC3) to provide a reporting mechanism for cybercrime complaints. The IC3 serves as a coordinating agency for the FBI and local law enforcement to respond to various forms of cybercrime, with a specific emphasis on economically motivated offenses. In fact, the Center was originally called the Internet Fraud Complaint Center, though it was changed from Fraud to Crime in 2003 to better recognize the range of offenses reported by victims (Internet Crime Complaint Center, 2017). The primary role of the IC3 is to offer cybercrime victims a reporting mechanism through an online complaint form. Respondents must complete questions concerning the incident, the offenders (if known), and the response from the victim, including when and who may have received information about the incident. Complaints are then processed by the IC3 staff, and forwarded to the appropriate local, state, or federal agency when necessary (Internet Crime Complaint Center, 2017). The trends and statistics developed from reports are also published by the IC3 as an aggregated yearly report on cybercrime incidents.

(ix) Computer Emergency Response Terms (CERT)

One of the largest groups of NGOs is computer emergency response teams (CERTs), which may be publicly funded and operate to support the community, or run by private industry to facilitate information sharing (see Chapter 4 for more details). There are 369 CERTs operating around the globe, located in universities, government agencies, and private industry (FIRST, 2017). Although CERTs play somewhat different roles depending on where they are housed, their primary functions are to provide information on emerging hardware and software vulnerabilities, malware threats, and security tools to insulate systems from compromise. Some CERTs are also able to engage in incident response for government agencies, organizations, and businesses to determine how an attack took place (USCERT, 2017).

(x) Working to Halt Online Abuse (WHOA)

An additional form of NGOs operates via private citizens who have come together for a specific cause. A notable example of such an NGO is Working to Halt Online Abuse (WHOA), which is a volunteer-driven organization established in 1997 as a resource to assist individuals who experience harassment or stalking. WHOA takes reports of cyberstalking directly from victims, and employs advocates who live in countries around the world to aid individuals (WHOA, 2015). Since WHOA is not a law enforcement agency, it cannot bring charges against a prospective offender. Instead, when a victim contacts WHOA, the staff of volunteer Internet Safety Advocates assist the victim in maintaining evidence of their experiences, and assist in contacting law enforcement and industrial sources such as ISPs (WHOA, 2015).

(xii) The Strategic Alliance Cybercrime Working Group

In 2008, the Strategic Alliance Cybercrime Working Group was created when law enforcement agencies from five countries and three continents (the Australian Federal Police, the Royal Canadian Mounted Police, the New Zealand Police, the United Kingdom's Serious Organised Crime Agency, and the FBI) came together to fight cybercrime. Representatives of this subcommittee of the Strategic Alliance Group (a partnership between these nations dedicated to tackling larger global crime issues, particularly organized crime) discuss ways to share information and investigations on critical issues, carry out joint training programs, and support public awareness campaigns.

(xi) International Multilateral Partnership Against Cyber Threats (IMPACT)

The International Multilateral Partnership Against Cyber Threats (IMPACT) is an international public–private initiative dedicated to enhancing the global community's capacity to prevent, defend, and respond to cyber threats. In May 2008, the ITU was invited to become a member of the IMPACT Advisory Board. In November 2008, IMPACT's headquarters in Cyberjaya, Malaysia, formally became the GCA's operational, physical, and state-of-the-art home (Andreasson, 2012). IMPACT Center for Policy and International Cooperation under the leadership of the ITU, and together with UN agency partners, Interpol, Council of Europe, and Organization for Economic Cooperation and Development (OECD), among others, the Center for Policy and International Cooperation contributes to the formulation of new policies and the harmonization of national laws around a variety of issues relating to cyber threats, including cybercrimes. The Center for Policy and International Cooperation also provides advisory services to interested member states on policy and regulatory matters for cybersecurity. With the support of the ITU, the Center fosters international cooperation through specific programs such as coordinated cyber-drill exercises between countries.

In collaboration with leading ICT companies and institutions, IMPACT conducts high level briefings for the benefit of representatives of ITU member states. Many of IMPACT's key partners have made available their respective chief technical officers, chief research officers, and other experts in a unique high-level IMPACT program to keep governments abreast of present and future cyber threats (Andreasson, 2012). The ITU contributes its experience to the center in capacity-building and developing frameworks for policy response to this program. Such high-level, cross-industry briefings give countries invaluable exposure and private sector insight about the latest trends, potential threats, and emerging technologies. IMPACT is committed to making facilities available and encouraging joint research efforts to address specific areas of concern. In collaboration with the ITU, IMPACT is making its research network available for the benefit of the global community. Besides the academic network, IMPACT global headquarters provides ITU member states with access to specialized ICT laboratories, specialized equipment, resource center, and other facilities (Andreasson, 2012).

SELF-ASSESSMENT EXERCISE

Discuss the efforts of the G8 High Tech Crime Working Group in the fight against cybercrime.

4.0 CONCLUSION

The importance of state-actor and non-state actors cannot be overemphasized in the drive towards combatting the menace of cybercrime and the activities of cybercriminals locally, regionally and internationally. From the above discourse, it is clear that cybercrime monitoring groups have emerged to launch cyber security watch that are restricted to their area of operation or jurisdiction (national and regional) for the purpose of identifying, reporting and initiating the prosecution of cybercrime cases. Also, these monitoring groups have made efforts at different times to institute cybercrime legislations or laws that will be globally applicable so as to complement existing national, regional, and international legislations on the phenomenon.

5.0 SUMMARY

This unit explains the activities of both state and non-state actors in the fight against the menace of cybercrime. Different cybercrime monitoring groups have emerged for the purpose of identifying, reporting, and initiating the prosecution of detected cases of cybercrimes. Also, it clearly explains the motives for their establishment, their activities and collective goal which is primarily to curtail cybercrime on the Internet or cyberspace. In addition, the achievements and challenges of these monitoring groups in controlling cybercrime were equally explained.

6.0 TUTOR-MARKED ASSIGNMENT

1. Discuss the mandate of the International Multilateral Partnership Against Cyber Threats (IMPACT)

6.0 REFERENCES/FURTHER READING

Andreasson, K. (2012). *Cybersecurity: Public Sector Threats and Responses*. Auerbach Publications.

Britt, P. (2008). *International Cybercrime Convention Gains Adherents around the World*.

Chertoff, M. (2009). The responsibility to contain: Protecting sovereignty under international law. Foreign Affairs, 88(1), 130–148.

IC3. (2007). *Internet fraud crime report, January 1, 2006–December 31, 2006*. National White Collar Crime Center and the Federal Bureau of Investigation. Available at www.ic3.gov/media/ annualreport/2006_IC3Report.pdf.

Kirk, J. (2009, March 11). Countries move forward on cybercrime treaty. PC World. Available athttp://www.pcworld.com/article/161067/countries_move_forward_on_cybercrime_ treaty.html

Kschetri, N. (2010). *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives*. Berlin: Springer-Verlag.

Miyake, K. (2001). G8 Concludes Tokyo High-Tech Crime Meeting. Available at http://archives.cnn.com/2001/TECH/internet/05/31/g8.cyber.crime.idg/index.html.

Schlein, L. (2009). ITU Tackles Global Cyberattacks. Available at http:// www.voanews.com/english/2009-10-07-voa51.cfm

Telecom News, The Heartland Institute.

United Nations Office on Drugs and Crime (2013). Comprehensive Study on Cybercrime. UNODC, Vienna.

UNIT 4 THE NIGERIAN GOVERNMENT EFFORTS AT TACKLING CYBERCRIME

CONTENTS

1.0 Introduction
2.0 Objectives
3.0 Main Content
3.1 The Nigerian Government Efforts at Tackling Cybercrime
4.0 Conclusion
5.0 Summary
6.0 Tutor -Marked Assignment
7.0 References/Further Reading

1.0 INTRODUCTION

The Nigerian Government has designed different measures not only to combat the menace of cybercrime, but to also salvage the problem of bad image that the pervasive youth perpetration of this form crime has attracted to Nigeria. The country is globally recognized to be among the major hubs of cybercrime perpetrating nations. Therefore, the major steps that have been taken over time by the Federal Government of Nigeria to tackle the illegal activities of cybercriminals are discussed in this Unit.

2.0 OBJECTIVES

At the end of this Unit, you should be able to:

- track the efforts that have been made by the Nigeria Government towards combatting the phenomenon of cybercrime
- identify and discuss the Nigerian anti-cybercrime legislation and other efforts that have been by the government to address the problem.

3.0 MAIN CONTENT

3.1 The Nigerian Government Efforts at Tackling Cybercrime

The Federal Government of Nigeria recognizes the pervasiveness of cybercrime and its associated socio-economic costs for individuals, businesses, industries, financial institutions, government agencies, amongst others. Thus, different efforts have been made to stem the tide of this form of criminality. Some of the measures that have been formulated by the government are discussed below:

a. The Enactment of the Cybercrime Prohibition Act 2015

The Cybercrimes (Prohibition, Prevention, etc. Act, 2015, is the first Act specifically enacted to regulate the conduct of persons in the cyberspace and cybercrimes in Nigeria. The Act was passed into Law by the Nigerian National Assembly on the May 5, 2015. It contains 59 sections, 8 parts and two schedules. The explanatory memorandum to the Act provides for an effective, unified and comprehensive legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria. This act also ensures the protection of critical national information networks, electronic communications, data and computer programs, intellectual property and privacy rights.

b. The Economic and Financial Crime Commission Act 2004

The Economic and Financial Crimes commission (Establishment) Act was adopted in 2004 (Oriola, 2005). It repealed the Financial Crimes Commission Act of 2002 and established a commission for economic and financial crimes. Under this act, the commission has the power to investigate all financial crimes relating to terrorism, money laundering, drug trafficking etc. Section 14-18 stipulates offences within the remit of the Act. These include offences in relation to financial malpractices, offences in relation to terrorism, offences relating to false information and offences in relation to economic and financial crimes.

The Act defines economic and financial crimes as:

> *the non-violent criminal and illicit activity committed with the objectives of earning wealth illegally either individually or in a group or organized manner thereby violating existing legislation governing the economic activities of government and its administration and includes any form of fraud, narcotic drug trafficking, money laundering, embezzlement, bribery, looting and any form of corrupt malpractices, illegal arms deal, smuggling, human trafficking and child labour, illegal oil bunkering and illegal mining, tax evasion, foreign exchange malpractices including counterfeiting of currency, theft of intellectual property and piracy, open market abuse, dumping of toxic wastes and prohibited goods, etc..*

c. *The Computer Security and Critical Information Infrastructure Protection Bill*

In 2005, the Nigerian Government adopted the Computer and Critical Information Infrastructure Protection Bill (known as the Cybercrime Bill). The Bill aims to ‘secure computer systems and networks and protect critical information infrastructure in Nigeria by prohibiting certain computer-based activities’ and to impose liability for global crimes committed over the Internet (Chawki, 2009). The Bill requires all service providers operating in the country to record all traffic and subscribe information and to relate this information to any law enforcement agency on the production of a warrant. Such information may only be used for legitimate purposes as determined by the court of competent jurisdiction or other lawful authority.

c. The Nigerian Cybercrime Working Group (NCWG)

The Nigerian Cybercrime Working Group is an inter-agency body comprising law enforcement, intelligence security, as well as ICT agencies of government and key private sector ICT organizations. It was established by the Federal Executive Council (FEC) on the recommendation of the President of Nigeria on March 31, 2004 (Chawki, 2009). The group was created to deliberate on and propose ways of tackling the malaise of internet 419 in Nigeria, by educating Nigerians on cybercrime and cyber security, providing legal technical assistance to the National Assembly on cybercrime and cyber security in order to promote general understanding of the subject matters amongst the legislature and undertaking international awareness programs for the purpose of informing the world of Nigeria’s strict policy on cybercrime and to draw global attention to the steps taken by the government to rid the country of internet 419 in particular and all forms of cybercrime.

d. *The Regulation of Cyber Cafes’ Operations*

Cyber café also known as the Internet café or PC café is a place where internet public access service is provided by entrepreneurs for a fee (Adomi, 2007). Previously, cyber cafés in Nigeria render overnight browsing, a special internet service is offered from 10.00pm to 6.00am. Though overnight browsing is very important, and useful, it was banned by the EFCC and the Association of Cyber café and Telecentre Owners (ATCON) in Nigeria as part of their strategies to address the problem of cybercrime. However, cyber cafés are no longer important nodes in cybercrime perpetration in Nigeria today because of the liberalization of the Internet Service Provisions in Nigeria.

e. *The Nigerian Government and Microsoft Partnership*

The Nigerian Government and the Microsoft Corporation signed a Memorandum of Understanding defining a framework for cooperation between Microsoft and EFCC of Nigeria with the aim of identifying and prosecuting cybercriminals, creating a safe legal environment and restore hundreds of millions of dollars in cost investment. This agreement was the first of its kind between Microsoft and an African government and gives the EFCC access to Microsoft technical expertise information for successful enforcement. The memorandum is aimed at combating cybercrime issues such as spam, financial scam, phishing, spy ware, viruses, worms, malicious code launches and counterfeiting (Adomi, 2007).

5.0 CONCLUSION

The series of efforts that had been taken by the Federal Government of Nigeria show that the danger that the activities of cybercriminals pose to the well-being of Nigerian citizens and Nigeria as a nation is fully recognized. The steps taken so far to tackle the menace of cybercrime have been fruitful to a large extent as cybercriminals operating in the country are being arrested on a daily basis. However, for the war against cybercrime to be effectively won, the Government and relevant law enforcement agencies need to continually tinker and innovate new strategies to match the illegal activities of cybercriminals on the cyberspace.

6.0 SUMMARY

This unit discusses the steps and measures that have been taken over time by the Nigerian Government in its fight against the menace of cybercrime and the illegal activities of cybercriminals operating in the country.

6.0 TUTOR- MARKED ASSIGNMENT

1. With relevant examples, discuss the role of the Economic and Financial Crimes Commission in the fight against the menace of cybercrime in Nigeria.
2. Aside from the legislative measures, identify and discuss other efforts that have been made by the Nigerian Government to combat the scourge of cybercrime.

7.0 REFERENCES/FURTHER READING

Adomi, E. (2007). Overnight Internet Browsing among Cyber café users in Abraka, Nigeria. *Journal of Community Informatics* 3.2.

Chawki, M. (2009). Nigeria Tackles Advance Free Fraud. *Journal of Information. Retrieved from http://isuisse.ifrance.com/emma/base/impvic.html.*

Oriola, T. (2005). *Advance Fee Fraud in the Internet: Nigeria's Regulatory Response*. 21(3). Computer Law and Society Review.

MODULE 4 CYBER THREAT AND CYBER SECURITY

Unit 1 Cyber Threats and Cyberattacks in the Cyberspace
Unit 2 The Necessity for Cyber Security
Unit 3 Cybercrime, Surveillance, and Privacy Issues
Unit 4 Cyber Threats and Cyber Safety Tips

UNIT 1 CYBER THREAT IN THE CYBERSPACE

CONTENTS

1.0 Introduction
2.0 Objectives
3.0 Main Content
3.1 Cyber Threat and Cyber attack in the Cyberspace
4.0 Conclusion
5.0 Summary
6.0 Tutor- Marked Assignment
7.0 References/Further Reading

1.0 INTRODUCTION

Generally, every new invention often comes with both intended and unintended consequences. While the intended consequences are usually positive and expected, unintended consequences are most times negative and not envisaged. The emergence of cyberspace environment made possible by the development of the Internet that was primarily aimed at improving the ways of life of human population. However, criminally minded individuals are exploiting its downside to victimize vulnerable Internet uses through the introduction of different forms of threats onto the Internet.

2.0 OBJECTIVES

At the end of this unit, you should be able to:

a. identify sources of threats on the cyberspace
b. determine forms of threat on the cyberspace
c. explain why cyber threats are introduced into cyberspace.

3.0 MAIN CONTENT

3.1 Cyber Threat and Cyber attack in the Cyberspace

As established in the previous modules, the Internet has significantly transformed our ways of live. Cyberspace is now playing dominant roles in our day-to-day activities. The Internet is making it possible for people in different parts of the world to engage in business transactions without necessarily seeing each other in person, it is allowing individuals to initiate and build social relationships, it is assisting companies to employ staffers without necessarily being involved in face-to-face interactions and interviews, it is enabling students to learn without necessarily sitting down to listen to tutor(s) within the four walls of a classroom, it is providing opportunities for passengers to get transported to their desired destinations without necessarily visiting a taxi terminus. Indeed, the advantages offers by the Internet are innumerable. However, the abundant opportunities embedded in it are also associated with numerous threats that can adversely affect its users.

The threats lurking around on the cyberspace are collectively known as cyber threat. Conceptually, cyber threat refers to all malicious acts that seek to damage data, steal data, or disrupt digital life in general. Typically, these threats usually occur in form of computer viruses, data breaches, Denial of Service (DoS) attacks etc. It can also be defined as any form of cyberattack targeted at gaining unauthorized access, damage, disrupt, or steal an information technology asset, computer network, intellectual property or any other form of sensitive data (UpGuard, 2020).

Cyber threat has become an issue of serious security concern for individual Internet users, national governments, and corporate organizations, amongst others. Johnson (2015) likened cyberspace to a virtual battleground that has become a place for confrontation in which appropriation of personal data, espionage of the scientific, economic and commercial assets of companies which fall victim to competitors or foreign powers, disruption of services necessary for the proper functioning of the economy and daily life, compromise of information related to our sovereignty and even, in certain circumstances, loss of human lives are nowadays the potential or actual consequences of the overlap between the digital world and human activity. According to Johnson (2015), this “virtual battleground” in cyberspace has only continued to increase global awareness of security and impact global political stability exponentially, cutting a wide swath across physical geographical boundaries, impacting the security of individuals, commercial enterprises, economies, and the sovereignty and stability of global nations.

The term “cyberattack” can have several meanings, depending on the targets, victims, motivations of the perpetrators, scope, impact, and the consequences of the attacks. Some have minor impacts and can often be attributed to straightforward delinquency, while others could have drastically negative effects on people, organizations, and states, and could be linked to crime, terrorism, or war. When combining the impact on a specific target with the generic consequences of an attack in the wider world, it is possible to develop a classification of cyberattacks having significant negative impacts on society (Clough, 2010). Such a classification could take the form of:

- attacks on public safety through the manipulation of the ICT systems involved in the management or control of vital infrastructures (flight, railway or subway control systems, water or flood supply control systems, health control systems, financial and banking control systems, electricity grid control systems, Supervisory Control and Data Acquisition (SCADA systems). This category also includes all types of attacks on the ICT systems and infrastructures used in disaster recovery plans;
- attacks on national defense systems involved in offensive or defensive military activities; attacks on e-government systems;
- attacks that lead to the manipulation of information (cyberpropaganda), to intelligence gathering, and to electronic espionage;
- attacks involved in economic crime;
- attacks involved in the harassment of people;
- attacks combining elements of two or more of the above.

The use of the word "cyberattack" instead of "cybercrime" indicates that the attacks were mostly directed against the computer and telecommunication systems involved in vital infrastructures that have a serious role to play in the economy, the safety of people, the sovereignty of a state, and the military and defence systems of a country (Clough, 2010). These attacks are offensive actions that alter, disrupt, manipulate, degrade, or destroy data, information and communication infrastructures (hardware or software). They could impact the whole of society by destabilizing, for example, the efficient operation of the economy or of governmental services. In other circumstances, when a cyberattack leads to specific offences, it is most commonly described as a cybercrime.

For an attack to be identified and treated as a crime action that breaks a law, that law by definition must already exist. But cyberattacks exist without any laws to qualify them. The term cyberattack covers a broad range of activities and is independent of any specific classification of offenses. Terms and definitions are not yet well defined or broadly accepted, but it seems that an agreement has been reached for presenting cyberattacks by describing their modus operandi (the way a cyberattack is performed and its vectors of propagation), the consequence and impact on relevant security criteria, and their generic and global impact

(Clough, 2010). At the same time, the word cyberattack can also be understood as referring to a military weapon. ICT infrastructures, information/disinformation procedures, and cyberattack-related tools are increasingly being linked to war- making capacities that contribute to developing the potential for cyberwarfare (Clough, 2010).

Generally speaking, the necessary conditions for a successful attack on the cyber space are the:

- knowledge of the target system (function, service, configuration, security policy and tools, administration);
- efficient use of programs (called exploits) that automatically exploit vulnerabilities to break into a computer;
- capacity of the aggressor to cover his tracks to avoid being detected and identified;
- rapidity of the attack (the attack is so fast that reactive security measures are ineffective).

If the attacker does not know the target well (phase 1 of the attack is insufficient), the risk of being tracked down increases. An attack can target a security system (firewall, authentication server, etc.), a security-related system (router, DNS, etc.), or a system that has no link to security measures, services or functions, such as workstations or web servers. According to the type of system targeted, the attack will be more or less difficult to carry out, and more or less rapidly detected, with a varying degree of negative impact (Clough, 2010).

From a technological perspective a cyberattack threatens all three of the main information security criteria: availability, integrity, and confidentiality (Clough, 2010).

Availability

A resource's availability relates to its ability to be used to accomplish the service for which it has been designed. The availability rate of a network, a server or a file should be close to 100% during the service opening period, being available 24 hours a day, seven days a week, in order to provide the permanent capacity to meet users' requirements in an appropriate timeframe (the notion of accessibility and continuity of services). Some computing attacks consist of making some resources unavailable, damaging not only the users but also the owners of the resource.

Integrity

The notion of integrity expresses the fact that resources, be they transactions, processing, services or data, have not been degraded or destroyed. This criterion contributes to assuring the security of a piece of information in that it has not been accessed and that its contents have not been modified. Confidence can be placed in the correctness and reliability of this information because it can be demonstrated that it has not been modified or deleted without the owner's authorization. Some malicious acts consist of modifying or falsifying information in order to have an impact on a particular decision (for example, the modification of an organized market leading to the sale or purchase of stocks). Acts of misinformation or cyber-propaganda do exist and are used to manipulate public opinion by providing false information, as could be the case of the modification of information on the website of a political party. The integrity of hardware can also be affected by physical destruction, deterioration, or by deliberately provoked damage. Acts of sabotage that create obstacles to the legitimate use of systems can harm the integrity or the availability of the resources.

Confidentiality

Confidentiality is the fact of keeping information secret. As a security criterion, confidentiality is protecting data against unauthorized disclosure. Having data intercepted, monitoring individuals, and using IT to perform acts of espionage can have a negative impact upon:

- professional secrecy;
- fundamental rights, especially the right to intimacy and to a private life including digital intimacy, and the right to the respect of correspondence;
- the efficient functioning of organizations and the economy; and state security.

3.2 Sources of Cyber Threat

Cyber threat is usually systemically deployed by nations and different groups of people to achieve their desired goal(s). Although, cyber threat is often driven by human actors, however, some natural disasters can also impact on the *wellbeing* or effective functioning of the digital architecture. The UpGuard (2020) identified the sources of cyber threat as including the following:

- **Hostile nation-states:** national cyber warfare programs provide emerging cyber threats ranging from propaganda, website defacement, espionage, disruption of key infrastructure to loss of life. Government-sponsored programs are increasingly becoming sophisticated and pose advanced threats when compared to other threat actors. Their developing capabilities could cause widespread, long-term damages to the national security of many countries including the United States. Hostile nation-states pose the highest risk due to their ability to effectively employ technology and tools against the most difficult targets like classified networks and critical infrastructure like electricity grids and gas control valves.

- **Terrorist groups:** terrorist groups are increasingly using cyberattacks to damage national interests. Although they are less developed in cyberattacks and have a lower propensity to pursue cyber means than nation-states. However, it is likely that terrorist groups will present substantial cyber threats as more technically competent generations join their ranks.
- **Corporate spies and organized crime organizations:** corporate spies and organized criminal organizations around the world also constitute serious risks because of their ability to conduct industrial espionage to steal trade secrets or large-scale monetary theft. Generally, these parties are interested in profit-based activities, either making a profit or disrupting a business's ability to make a profit by attacking key infrastructure of competitors, stealing trade secrets, or gaining access and blackmail material.
- **Hacktivists:** Hacktivists activities revolve around political ideals and issues. Most hacktivist groups are concerned with spreading propaganda rather than damaging infrastructure or disrupting services. Their goal is to support their political agenda rather than cause maximum damage to an organization.
- **Disgruntled insiders:** disgruntled insiders are a common source of cybercrime. Insiders often do not need a high degree of computer knowledge to expose sensitive data because they may be authorized to access the data. Insider threats also include third-party vendors and employees who may accidentally introduce malware into systems or may log into a secure S3 bucket, download its contents and share it online resulting in a data breach. Check your S3 permissions or someone else will.
- **Hackers:** malicious intruders could take advantage of a zero-day exploit to gain unauthorized access to data. Hackers may break into information systems for a challenge or bragging rights. In the past, this required a high level of skill. Today, automated attack scripts and protocols can be downloaded from the Internet, making sophisticated attacks simple.
- **Natural disasters:** natural disasters represent a cyber threat because they can disrupt your key infrastructure just like a cyberattack could.
- **Accidental actions of authorized users:** an authorized user may forget to correctly configure S3 security, and thereby causing a

potential data leak. Some of the biggest data breaches have been caused by poor configuration rather than hackers or disgruntled insiders.

Generally, cyber threats can be categorized into those that are politically motivated (such as cyber warfare, cyber terrorism, espionage, and hacktivism, the hacking for political purposes) and those that are non-politically driven (typically financially motivated, such as cybercrime, intellectual property theft, and fraud, but also hacking for fun or retribution, for example, from a disgruntled employee (Kschetri, 2010).

The aim of politically motivated attacks is generally to disrupt services with or without the intention to also cause physical damage. A common approach is to use a botnet, a collection of infected computers (agents) that allows someone to control them remotely, to launch a distributed denial of service (DDoS) attack, which attempts to disrupt websites by overwhelming them with traffic (Johnson, 2015). A very good example in this context is the attacks on Estonia during its diplomatic standoff with Russia in April 2007, when several government websites were made inaccessible for up to 3 weeks. Equally, politically motivated attacks can also seek to gain publicity in order to undermine the perception of the public.

In 2010, a group called "*Anonymous*" successfully brought down the websites of various organizations, including the Swedish prosecution authority, and the private sector sites of MasterCard and Visa, in support of WikiLeaks, the whistle-blowing website. If sufficiently efficient, attacks on public sector websites can affect the trust of e-government to such a degree that public perception turns increasingly negative whereby people would be averse to make certain transactions online, be unwilling to share data, or be reluctant to believe the information provided. The motivation for nonpolitically motivated attacks is generally financial. As such, they tend to focus on stealing data, such as credit card information, while keeping a low profile (Johnson, 2015). The following are identified by UpGrade (2020) to be among the most common forms of cyber threat:

- **Malware:** malware is software that does malicious tasks on a device or network such as corrupting data or taking control of a system.
- **Spyware:** spyware is a form of malware that hides on a device providing real-time information sharing to its host, enabling them to steal data like bank details and passwords.
- **Phishing attacks:** phishing is when a cybercriminal attempts to lure individuals into providing sensitive data such as personally identifiable information (PII), banking and credit card details and passwords.

- **Distributed denial of service (DDoS) attacks:** distributed denial of service attacks aim to disrupt a computer network by flooding the network with superfluous requests to overload the system and prevent legitimate requests being fulfilled.
- **Ransomware:** ransomware is a type of malware that denies access to a computer system or data until a ransom is paid.
- **Zero-day exploits:** a zero-day exploit is a flaw in software, hardware or firmware that is unknown to the party or parties responsible for patching the flaw.
- **Advanced persistent threats:** an advanced persistent threat is when an unauthorized user gains access to a system or network and remains there without being detected for an extended period of time.
- **Trojans:** a trojan creates a backdoor in your system, allowing the attacker to gain control of your computer or access confidential information.
- **Wiper attacks:** a wiper attack is a form of malware whose intention is to wipe the hard drive of the computer it infects.
- **Intellectual property theft:** intellectual property theft is stealing or using someone else's intellectual property without permission.
- **Theft of money:** cyber attackers may gain access to credit card numbers or bank accounts to steal money.
- **Data manipulation:** data manipulation is a form of cyberattack that does not steal data but aims to change the data to make it harder for an organization to operate.
- **Data destruction:** data destruction is when a cyberattacker attempts to delete data.
- **Man-in-the-middle attack (MITM attack):** a MITM attack is when an attack relays and possibly alters the communication between two parties who believe they are communicating with each other.
- **Drive-by downloads:** a drive-by download attack is a download that happens without a person's knowledge often installing a computer virus, spyware or malware.
- **Malvertising:** this involves the use of online advertising to spread malware.
- **Rogue software:** rogue software is malware that is disguised as real software.
- **Unpatched software:** unpatched software is software that has a known security weakness that has been fixed in a later release but not yet updated.
- **Data centre disrupted by natural disaster:** the data centre your software is housed on could be disrupted by a natural disaster like flooding

4.0 CONCLUSION

Cyber threats are a serious problem that is associated with the cyberspace environment. There are numerous attacks that have led to online theft of sensitive data, money, breaches of national security data, failure of institution of the movement like the military internet infrastructures, hacking of organizations' data, online child trafficking, and circulation of child pornography, terrorism radicalization and recruitment among others. Regardless of their source(s), the danger that cyber threats pose to digital environment cannot be overemphasized.

5.0 SUMMARY

This unit has made student to understand what constitutes cyber threat, why the existence of cyber threat constitutes a problem for Internet users, the sources and types of threats the cyberspace. It has opened students' eyes to different forms of cyber threats to which they could fall victim on the digital environment.

6.0 TUTOR-MARKED ASSIGNMENT

1. Cyber threat constitutes a major cause for concern for all Internet users. Discuss.
2. Mention and explain the sources of cyber threat on the cyberspace.
3. List and discuss the common forms of cyber threat on the cyberspace.

7.0 REFERENCES/FURTHER READING

Clough, J. (2010). *Principles of Cybercrime*. Cambridge University Press.

Johnson, A. (2015). *Cyber-Security: Protecting Critical Infrastructures from Cyberattack and Cyber-Warfare.* CRC Press.

Kschetri, N. (2010). *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives*. Berlin: Springer-Verlag.

UpGuard. (2020). *What is a Cyber Threat.*

UNIT 2 THE NECESSITY FOR CYBER SECURITY

CONTENTS

1.0 Introduction
2.0 Objectives
3.0 Main Content
3.1 The Necessity for Cyber Security
4.0 Conclusion
5.0 Summary
6.0 Tutor-Marked Assignment
7.0 References/Further Reading

1.0 INTRODUCTION

It was established in the preceding unit that cyber threats are endemic on the cyberspace and constitute a major cause of concern for all users of digital environment. Therefore, it becomes highly imperative for governments, Internet Service Providers, and other relevant stakeholders to develop strategies and frameworks to make cyber environment safe and secured for their users. Efforts being made to tackle threats lurking on the cyberspace culminated in the emergence of cyber security.

2.0 OBJECTIVES

At the end of this unit, you should be able to:

- explain the need for cyber security
- understand the meaning of cyber security
- discuss measures that can be taken to achieve cyber security
- describe the major categories cyber security.

3.0 MAIN CONTENT

3.1 The Necessity for Cyber Security

The continuous challenge which cyber threat poses to the digital space and its users makes cyber security a necessity. Therefore, cyber security is not only among the most critical concerns of the information age, it also forms the cornerstone of a connected world (Johnson, 2015). Each person using an information and communication device, tool, or service, for professional or private issues, needs information security. It is true for governmental institutions as for big or small organisations and individuals. The security answer should satisfy particular protection and defence level requirements regarding the actor's need (Clough, 2010).

Security approaches are often limited to the installation of risk reduction measures designed to protect the information technology resources of large organizations. However, the security approach must also necessarily meet the security needs of small- and medium-sized organizations, as well as those of end users (individuals). Individuals have a particular need to protect their personal or sensitive data, their privacy, and their basic human rights. As the Internet is global and has international coverage, all countries over the world need to develop and implement national cybersecurity policies (Maras, 2015).

For developing countries, attempts to reduce the digital divide through investment in infrastructure only, without taking into account the need for security and control of IT risks (unsolicited incident, malevolent acts, etc.), would result in the creation of a security divide as prejudicial as the digital divide. The use of a technological and legal approach would minimize the digital divide and more quickly create a reliable infrastructure that meets global cyber security needs. It has become imperative that developing countries not only introduce measures to fight against cybercrime, but also control the security of their infrastructures and information technology services (Clough, 2010).

Cyber security impacts the security of the digital and cultural wealth of people, organizations, and countries. It is a social issue as well as one of economics and public policy. The challenges involved are complex, and meeting them requires the political will to devise and implement an overall strategy for the development of digital infrastructures and services that includes a coherent, effective, verifiable, and manageable cybersecurity strategy (Clough, 2010). The cybersecurity strategy must be part of a multidisciplinary approach, with solutions in place at the educational, legal, management, and technical levels. A strong response to the human, legal, economic, and technological dimensions of digital infrastructure security needs builds confidence and generates economic growth that benefits all of society. Controlling digital information wealth, distributing intangible goods, adding value to content, and bridging the digital divide – these are all problems of an economic and social nature, calling for more than a one-dimensional, strictly technological approach to cybersecurity (Clough, 2010).

Around the year 2000, the computing industry began to realize that cybersecurity was not being taken seriously enough to keep up with the increasing penetration and criticality of the role of computers in almost every aspect of culture and society. At the same time, cybercriminals were becoming more active and visible (Waschke, 2015). Around this time, the computing industry became aware that cybercrime and lack of security could be a significant deterrent to current and future business. Therefore, it is not surprising that security consciousness grew as the Internet began to be a necessity in homes and businesses. Some of the contradictions between a free and open Internet and safe and reliable computing had become evident. Networked computers had become the norm, and criminal hackers were building steam. And it was becoming evident that enforcing cybercrime laws is demanding and requires training and resources that are not easy for law enforcement to obtain (Waschke, 2015). Hence, designing a framework to ensure the of the cyberspaces becomes inevitable for computing industry.

Cyber security has been conceptualized in different ways by scholars and some international organizations. Kaspersky Lab. (2020) defined cyber security as the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. Also, the Interagency Committee on National Security Systems viewed it as “the ability to protect or defend the use of cyberspace from cyberattacks,” where cyberspace is defined as a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. Equally, the International Telecommunications Union (ITU), the United Nations’ specialized agency for information and communications technology conceived cyber security as the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user’s assets.

Cybersecurity must insist on the strategic dimension of ICT infrastructure and services in respect of state sovereignty, organizational competitiveness, and the safety of individuals. Cybersecurity cannot be abstracted away from its field of application and socio-cultural environment. It must be approached in an interdisciplinary and multi-stakeholder context, placing the individual at the heart of the ICT security question in order to encourage the development of a conscious and inclusive information society (Clough, 2010).

The terms “information security” and “cybersecurity” can carry different meanings. In some contexts, it refers to the protection of assets or to the fight against industrial and economic espionage, against international terrorism or economic crime, against the manipulation of illicit contents or the unauthorized use of resources. In other contexts, cybersecurity covers everything from computer surveillance and monitoring to tyrannical control or to a struggle for fundamental human rights.

Information security deals with a range of issues, such as state sovereignty, national security, the protection of critical infrastructures, the security of tangible and intangible assets, and the protection of personal data, to mention only a few. In addition, any potential malfunction of information technologies, regardless of its origin (accident, error, malevolence), constitutes an operational risk for people or organizations that rely upon ICT, as they mean a consequent risk of losses from the inadequacy or failure of processes (Clough, 2010).

Cybersecurity also arises from the need for technologies to be less vulnerable – to decrease the number of potential threats. Cybersecurity concerns the creation of secure, transparent and manageable products, the development of reliable and safe behaviours around the use of ICT, and the definition of appropriate legal frameworks. Because humans are the weak link in the security chain, and because humans are the final "consumers" of ICT service and infrastructures, any security solution should also take into consideration social needs. At the same time, security solutions should not transform the Internet and information technologies into an excessively controlled territory, because their doing so may undermine basic human rights (Clough, 2010).

To ensure a global information society in which trust and security in the use of ICTs is the norm for the benefit of mankind, the ITU Secretary General on May 17, 2007 launched the Global Cybersecurity Agenda (GCA) to provide a framework within which an international response to the growing challenges to cybersecurity can be coordinated and addressed (Andreasson, 2012). The GCA is an international cooperation framework and strives to engage all stakeholders, including governments, the private sector, civil society, and international organizations, in a concerted effort to build confidence and security in the information society. The GCA is built upon five pillars with seven strategic goals. The five pillars are:

(1.) Legal measures: this means that national laws need to be put in place where they do not yet exist, and existing laws as well as regional and international agreements need to be based upon a shared understanding of what constitutes cybercrimes and cyberattacks, and how to confront them.

(2.) Technical and procedural measures: this suggests that technical solutions need to be identified and developed, taking into account the principles of globally accepted standards, aimed at providing hardware and software security baselines that can be adopted by vendors, manufacturers, and end users

(3.) Organizational structures: this suggests that appropriate organizational structures, such as coordination and response centers with national responsibility need to be established in order to promptly respond to cyberattacks and coordinate with their counterparts at the international level.

(4.) Capacity building and (5.) International cooperation: these last two pillars cross-cut all areas and aim at elaborating strategies to ensure that the required capacity is available to allow IT security professionals to properly react in case of cyberattacks as well as to build relations and partnerships at the international level.

The Kaspersky Lab (2000) divides cyber security into the following categories:

a. **Network security:** is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.

b. **Application security:** this focuses on keeping software and devices free of threats. A compromised application could provide access to the data its designed to protect. Successful security begins in the design stage, well before a program or device is deployed.

c. **Information security:** this deals with the protection of the integrity and privacy of data, both in storage and in transit.

d. **Operational security:** this includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella.

e. **Disaster recovery and business continuity:** this defines how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data. Disaster recovery policies dictate how the organization restores its operations and information to return to the same operating capacity as before the event. Business continuity is the plan the organization falls back on while trying to operate without certain resources.

f. **End-user education:** this addresses the most unpredictable cyber-security factor -people. Anyone can accidentally introduce a virus to an otherwise secure system by failing to follow good security practices. Teaching users to delete suspicious email attachments, not plug in unidentified USB drives, and various other important lessons is vital for the security of any organization.

Information security constitutes a driving force for the economic development of regions and must be developed and implemented simultaneously with the implementation of ICT infrastructure. The benefits to be derived from the deployment of information technology services are dependent upon the accompanying development of both the ICT infrastructure and an appropriate legal and regulatory framework. With sufficient security measures and effective laws, a digital economy can be developed (Clough, 2010). ICT security in a broad sense, including the legal framework, is critical for attracting players with the resources and drives to develop a favourable business environment. This is the main factor that guarantees that investment in infrastructure would be profitable. Of course, cybersecurity tools and the accompanying legal framework constitute an additional challenge for developing countries that want to participate in the global economy. An inclusive global information society would avoid pitfalls such as the emergence of digital paradises or the exclusion of users from effective digital security (Clough, 2010).

SELF-ASSESSMENT EXERCISE

List and discuss the categories of cyber security as proposed by the Kapersky Lab.

4.0 CONCLUSION

Cyber security represents a rational response to the threats that are daily being introduced onto the digital space by criminally minded individuals for financial gains or for the purpose of furthering a non-financial objective. Therefore, if cyber security and cyber safety are not given serious attention which they deserve, cyberspace would be hijacked and rendered useless for its legitimate users.

5.0 SUMMARY

In this Unit, attention has been devoted to the emergence of cyber security as a counter strategy to the activities of cybercriminals who are developing and introducing different forms of cyber threats onto the cyberspace as a way of furthering their clandestine goals and objectives.

6.0 TUTOR- MARKED ASSIGNMENT

1. Cyber security is an inevitable measure in the 21st century. Discuss.
2. Highlight and discuss the major categories of cyber security.

7.0 REFERENCES/FURTHER READING

Clough, J. (2010). *Principles of Cybercrime*. Cambridge University Press.

Kapsersky Lab. (2020). *What is Cyber-Security?*

Maras, M. (2015). *Computer Forensics: Cybercriminals, Laws and Evidence (Second Edition)*. Jones & Bartlett Learning.

UNIT 3 CYBERCRIME, SURVEILLANCE, AND PRIVACY ISSUES

CONTENTS

1.0 Introduction
2.0 Objectives
3.0 Main Content
3.1 Cybercrime, Surveillance, and Privacy Issues
4.0 Conclusion
5.0 Summary
6.0 Tutor- Marked Assignment
7.0 References/Further Reading

1.0 INTRODUCTION

Cybercrime is among the dominant crimes of the 21st century. Cyber surveillance is among the major widely recognized measures that is being adopted by governments, security experts, and law enforcement agencies for tackling the problem. Although this approach has been adjudged to be effective in certain areas, it also has serious implications for Internet users' right to privacy and freedom of speech. Hence, this Unit seeks to discuss the contentious issue of cyber surveillance within the context of cyberspace security.

2.0 OBJECTIVES

At the end of this Unit, you should be able to:

- explain what cyber surveillance entails
- describe the development of cyber surveillance as a response to cybercrime
- Understand the contention between cyber surveillance and privacy issue
- discuss the basic strategies for strengthening privacy on the cyberspace

3.0 MAIN CONTENT

3.1 Cybercrime, Surveillance, and Privacy Issues

Globally, governments and law enforcement agencies are innovating new strategies to combat the security and safety threats that are embedded in the cyberspace. This critical step is not only informed by the realization that cybercriminals are not only posing serious threats to individuals, businesses, and corporations, but they are also targeting critical national infrastructures. Cyber surveillance is among the most commonly adopted approaches for addressing the problem. Cyber surveillance essentially involves a covert monitoring of computer activity and data stored on a hard drive, or data being transferred over computer networks via the Internet. This monitoring activities which may be legally or illegally conducted can be conducted by governments, corporations, criminal organizations, or individuals. However, regardless of the means through which it is being carried out, be it legal or illegal, a major common feature of cyber surveillance is its ***covert*** nature.

Cyber surveillance takes a rather different approach from its terrestrial counterpart. Rather than monitoring the physical presence and bodily actions of subjects, Internet surveillance observes and collects the digital footprints that all online activities leave in their wake. All Internet users, whether they know it or not, leave a 'data trail', the electronic record of their mouse clicks and keystrokes, the websites they have visited, the searches they have run, the materials they have downloaded, the personal information they have entered, the words and images they have sent via email, and so on. From such *dataveillance* (Gandy, 1993) it is possible to construct a digital double or simulation of an individual and her or his activities, without ever having to engage in physical observation (Poster, 1990; Bogard, 1996). Therefore, from a web user's online activities, it is possible to discover and track, among other things, her or his consumer choices and preferences; sexual orientation, fantasies and fetishes; political opinions and sympathies; professional interests and career aspirations; personal associations, friendships and intimate relationships (King, 2001).

The use of cyber surveillance by governments and law enforcement agencies to monitor the online activities of Internet users is increasingly generating serious debates in many countries as it challenges peoples' rights to privacy and confidentiality. The opponents of cyber surveillance argue that though law enforcement agents need to able to identify offenders and collect evidence of online crimes, yet unapproved monitoring constitutes a form of privacy intrusion that has serious implications for their fundamental human rights. Furthermore, critics of Internet surveillance point out that we risk losing control over the personal information that circulates on the web – the content of our emails, the sites we visit, our financial and other sensitive information because the potential for abuse is all too apparent. Thus, efforts to secure society against the threat of cybercrime thus carry with them far-reaching consequences for the future of online freedom itself (Yar, 2006).

Generally, it is an undeniable fact that we are currently witnessing an intense struggle over the balance between online surveillance and privacy; while authorities move towards greater monitoring in order the tackle organized criminals, terrorists, paedophiles, stalkers, and so on, civil libertarians encourage users to evade such invasion of privacy by making greater recourse to privacy-enhancing tools (Yar, 2006).

Alex and Fieke (2018) suggest the following steps as possible strategies that can enable one to regain a certain amount of control over one's data and digital shadow:

a. limiting data generation by withholding information - You do not need to fill out all the fields in registration forms online
b. cleaning your online identity by deleting apps that you no longer use from your mobile phone, and erase pictures, emails and messages that are outdated
c. blocking unwanted access, and installing Privacy Badger and NoScript to block cookies and other third party scripts from running in your browser and collecting data
d. masking your individual identity on Facebook by creating a group account and identity
e. creating noise by clicking on random ads, or install Adnausium, a tool that will do this for you, while you do other things
f. misleading Google by installing TrackMeNot, a tool which generates random search queries, masking your real searches and questions
g. using a VPN to change your IP address
h. changing the name on your phone
i. breaking your online routine
j. creating a barrier: install an anti-virus program and keep it up to date
k. keeping your data under lock and key: encrypt your mobile phone, computer and tablet
l. breaking all signals, turning off Wi-Fi and Bluetooth when not in use and putting your phone in a faraday shield (you can make one yourself) when you don't want to be tracked
m. a simple but effective measure is to cover your webcam when not in use
n. ensuring that you connect to websites through a secure connection (wherever possible), by installing HTTPS Everywhere in your browser.

4.0 CONCLUSION

Cybercrime has led to the emergence of cyber surveillance as part of measures that is being deployed by security experts, governments, and law enforcement agencies to counter the illegal activities of cybercriminals on the cyberspace. Although this is a right step in a right direction. However, strategies being adopted in the course of conducting cyber surveillance are also throwing up serious controversies as to its violation of the privacy of legitimate Internet users.

5.0 SUMMARY

In this unit, students have been exposed to the emergence of cyber surveillance as a rational response to the inimical activities of cybercriminals on the cyberspace. Equally, the concerns of legitimate Internet users and human rights groups as to the implication of cyber surveillance for their privacy were also discussed.

6.0 TUTOR MARKED ASSIGNMENT

1. Cyber surveillance is a major cause of concern for legitimate Internet users. Discuss
2. Explain the strategies that can be adopted by Internet users to safeguard their data and digital shadow from cyber surveillance

7.0 REFERENCES/FURTHER READING

Alex, H. & Fieke, J. (2018). *Privacy, Surveillance and Data Tracking: Why Does It Matter for Human Rights Defender?*

Gandy, O. (1993). *The Panoptic Sort: A Political Economy of Personal Information.*

Yar, M. (2006). *Cybercrime and Society*. Sage Publishers Ltd.

UNIT 4 CYBER THREAT AND CYBER SAFETY TIPS

CONTENTS

1.0 Introduction
2.0 Objectives
3.0 Main Content
3.1 Cyber Threat and Cyber Safety Tips
4.0 Conclusion
5.0 Summary
6.0 Tutor-Marked Assignment
7.0 References/Further Reading

1.0 INTRODUCTION

Cyber threat comes in different dimensions. The degree of their impacts varies considerably in terms of magnitude and damages. Although while it is true that cyber safety cannot be totally guaranteed because of the transient and fluid character of cybercrime, there are certain tips that can help Internet users to strengthen their security on the cyberspace.

2.0 OBJECTIVES

At the end of this Unit, you should be able to:

- discuss threat modeling and control flow integrity approaches to cyber safety
- state the basic cyber safety tips

3.0 MAIN CONTENT

3.1 Cyber Threat and Cyber Safety Tips

Today, it is a common reality that cyber threat has become a permanent feature of the digital space. The level of exposure to cyber threat varies considerably for individuals, business, government agencies, corporate institution, amongst others. Nonetheless, all users of cyberspace need to take appropriate conscious security steps to remain safe from the threats lurking around on the digital space, and from the antics of cybercriminals. Each participant has to assume part of the shared responsibility. Each must stop transferring security responsibilities onto other entities and start discharging them himself. Therefore, this unit focuses on the basic cyber safety tips.

Waschke (2017) asserts that for a computer system to be fully secured it has to fulfill the triad goals of security theory which include:

confidentiality (when a system is confidential, data and processes are only available to actors who have a legitimate right to access), integrity (when a system has integrity, data and processes will only be affected by authorized actors in a regulated fashion), and availability (a system has availability when legitimate actors can get to data and processes in an orderly and predictable manner). Therefore, as a computer user, the security triad can help you systematically review the security of features of a new laptop, tablet, or smartphone. They can help point out the weaknesses and strengths of applications you consider for installation. They can also help you evaluate the safety of items from the Internet of Things you might place in your home or office and connect to your network. Furthermore, Waschke (2017) submits that by designing computer operating systems such as Microsoft Windows, Apple iOS, OS X, Android, or Linux, computer security experts are utilizing the following techniques to anticipate, recognize, and tackle the problem of cyber security threat:

i. Threat Modeling

One of the techniques developers use to design and construct more secure systems is called threat modelling. To achieve this, a developer, or group of developers will sit down to imagine all the threats that a system may be subject to and the consequences if the threats were carried out. The security triad provides a systematic pattern for thinking about threats. Simply taking time to imagine the possible threats is a big step forward from the old days when security was an afterthought. Developers have taken threat modelling beyond a lightly structured “what if” exercise. The details of threat modeling techniques vary but they all identify the data processed by the system, the users of the system, and who the adversaries of the system might be and what they might be after. They also identify how data moves through the system and where it is stored. The next step is to spot the points where the system is vulnerable. That is easier than it may appear because almost all vulnerabilities occur when data moves from one module to another. One of the key tools in threat analysis is a data flow diagram that delineates the flow of data from one module to another. With the system assets and points of vulnerability all listed out, the threat modelers evaluate each threat, rating them by the amount and seriousness of damage they could cause. The results of this evaluation are fed back into the project plans and developers are assigned to mitigate the threats. Threat modeling is usually an iterative process (Waschke, 2017). Modeling is repeated during development, continually modeling new threats as they may appear and testing the mitigation of old threats. This process replaces the old plan, where a developer would be assigned to code a solution to a security defect whenever defects happened to show up in testing or in the field, but no one systematically looked for vulnerabilities and developed plans for eliminating before they made it to testing.

ii. Control Flow Integrity

Control flow integrity is important because it is an attempt to build resistance to one type of system attack into the operating system and application code, rather than address individual flaws. This procedure adds a layer of sophistication to the operating system software that determines the conditions when privileged instructions will be executed by looking at the flow of control from one software section to another. Researchers have identified patterns of shifts in control that indicate a program is doing something it was not intended to do. (Waschke, 2017). For all the complexity of software and hardware, each core in a running computer is simply executing one instruction after another. The mechanisms that are used to determine which instruction will be executed next can be quite intricate, but they all answer a simple question: what next? If a hacker can insinuate a change into the control mechanism that will start the computer executing his sequence of instructions and abandon the legitimate sequence, the hacker has won and the computer is pawned.

Control flow integrity does not address how control is hijacked from its legitimate path. Instead, it detects when the control goes awry and raises a flag. No matter how the system was rigged by the hacker, if the program strays, control flow integrity detects the misadventure and guides it back to a safe path. Enforcing control flow is a way of approaching the problem at a higher level. Rather than eliminate buffer overruns that cause control flow misadventures, control flow integrity measures detect deviations in flow control and stops the deviation. For example, Microsoft Windows 10 supports a feature called Control Flow Guard, which is an example of forcing control flow integrity. Developers use features built into the operating system to write applications that detect when the flow control of their code has been diverted from its intended direction.

Generally, the following basic security and safety steps can a long way in protecting your computer system and safeguard you from being victimized on the cyberspace:

a. Installing Antivirus Software on your Computer System

Antivirus software is important because it provides basic protection against specific and generic types of malware, including worms, viruses, Trojans, keyloggers, etc. This is readily available for all types of computers and operating systems. The following guidelines should be taken into consideration when using antivirus software:

- Acquire antivirus software from a reputable source
- Make sure you install reputable antivirus products before you connect your computer to the Internet; otherwise your computer will be compromised even before you finish downloading needed product upgrades and patches.
- Update the virus definition or signature files daily. Most antivirus software provides a way to do this automatically
- Scan your system for viruses weekly.
- Enable any automatic protection, such as email scanning.

b. Use a Software or Hardware Firewall

A firewall regulates communication between your computer and the network, including the largest network of all, the Internet. It provides a set of access lists installed on a computer or coded into an appliance that protects a computer or network from intruders. If a worm or a hacker attacks your computer from the Internet, the firewall will block access to your computer. Some firewalls only regulate communications attempting to enter your computer (Windows XP); others also provide control over what leaves your computer (e.g., Zone Alarm) (McQuade, 2009). Firewall rules can be configured to detect and deny intruder probes in various ways. Firewalls are available in both hardware (appliance) versions and as software. A properly configured router will also provide much of the protection of a firewall. Firewalls provide protection from individuals who do not know the specific access credentials (such as passwords) to your computer system and will eliminate a good deal of risk from outside attack.

c. Applying Patches Against Vulnerabilities

One method used by cybercriminals to attack your computer is taking advantage of vulnerabilities or weak spots. The vulnerabilities may be in your operating system or the specific applications you are using. Patches provide protection against software vulnerabilities. When a software vendor discovers vulnerability, it will often make available a patch to address that vulnerability. Although most operating systems provide an automatic updating feature, some applications do not. It is critical to apply patches as soon as possible. When a patch is released, cybercriminals will develop exploits for the respective vulnerability, often within hours. Release of a patch provides both a fix for vulnerability and a target for a cybercriminal. Cybercriminals will use an exploit to attack the specific vulnerability on computers whose users have not yet applied the patch. Patches may be released on a regular cycle. They may also be released when vulnerabilities are discovered. Patching also is one of the chief defenses against worms.

d. Installing Antispyware and Adware

Software spyware has become the scourge of the Internet (McQuade, 2009). Unlike other types of attacks whose effects may be obvious, spyware infestations are designed to run unobtrusively, capturing information about your Internet activities. Antispyware and adware software products will help you to detect and remove these types of malware from your system, may speed up system performance, and may provide protection when you visit malicious Web sites. Use of antispyware products is not as straightforward as use of antivirus products. Although most antivirus products are interchangeable, different antispyware and antiadware products will detect different types of spyware and adware. You must use more than one antispyware product to provide adequate protection. Antispyware is often free and available online. However, some spyware actually masquerades as antispyware, so use care when downloading from a company that is not a well-known security vendor.

e. Use Strong Passwords

Passwords provide a means of limiting access to your computer use and to information stored on the computer or the network. A strong password provides a fundamental layer of protection. Because of advances in password cracking technologies, eight-character passwords may not prove to be sufficient. Ideally, a password should be 15 characters or longer, although not all systems will support a password of this length (McQuade, 2009). A strong password should be intuitively associated with tangible items, pictures, or other intelligence known about the workstation or device owner. Using a strong password can eliminate significant risk of system manipulation and loss of data. Here are the basic rules for selecting a strong password:

- make your password at least 8 characters long, consisting of a mix of lower and upper case letters, numbers, and symbols.
- use a passphrase of at least 15 characters if at all possible. A good passphrase can include dictionary words, but should also include special characters, etc. An example of a good passphrase would be ‘‘IfI0nlyHad8Brain?’’
- do not use proper names or words from a dictionary or encyclopedia, including those printed in foreign languages
- make sure the password does not contain data of a personal nature, such as birthday, anniversary, street address, part of your social security number, or pet’s name, etc

- change your password at least every 120 days.
- do not repeat use of a password.
- do not share your password.
- do not write it on a sticky note on your computer or keyboard.

f. Protect Yourself When Using Wireless Devices and Access Points

Wireless networking allows you to connect to a network and often the Internet without using a cable. As more people purchase laptops, PDAs, and other mobile devices, wireless network access has become increasingly popular and convenient. Wireless access points must be set up properly to provide sufficient security. However, most wireless access points are set up in a manner that is extremely insecure. Without the proper precautions, wireless networking can place your privacy, your data, and your computer at significant risk. When connected to an insecure wireless network, anyone within range of your computer and using the right tools can easily capture your traffic as it is transmitted across the network. This type of ‘‘listening in,’’ known as sniffing, can be done with a laptop (or PDA), a wireless card, and some freely available software and is very difficult to detect. Attackers may also use your connection for their own nefarious purposes. This could include anything from illegally downloading copyrighted files to posting child pornography on the Internet. Follow these tips to use someone else’s wireless connection safely:

- avoid sending sensitive information over a wireless network.
- encrypt your traffic
- provide sensitive information only to ‘‘secure’’ sites, i.e., sites that display https:// in the address bar and a padlock
- use virtual private networking (VPN) to encrypt all network traffic to and from your computer. If you have VPN access through your company or school, use it whenever you access a wireless network.

Focusing more on information systems and network security, the following elements from the Organization for Economic Co-operation and Development’s (OECD) 2002 guidelines for the security of information systems and networks – “*Towards a Culture of Security*” – are a good starting point for examining security issues. Although published a decade ago, they remain a robust set of general guidelines that can be applied independently of technological developments (Clough, 2010).

(i) Awareness: participants should be aware of the need for securing information systems and networks and what can be done to enhance security;

(ii) Responsibility: all participants are responsible for the security of information systems and networks;

(iii) Response: participants should act in a timely and co-operative manner to prevent, detect, and respond to security incidents;

(iv) Ethics: participants should respect the legitimate interests of others;

(v) Democracy: the security of information systems and networks should be compatible with the basic values of a democratic society;

(vi) Risk assessment: participants should conduct risk assessments;

(vii) Security design and implementation: participants should incorporate security as an essential element of information systems and networks;

(viii) Security management: participants should adopt a comprehensive approach to security management;

(ix) Reassessment: participants should review and reassess the security of information systems and networks and make appropriate modifications to security policies, practices, measures, and procedures.

These security guidelines apply everywhere and constitute a good starting point for considering ICT security issues. ICT security is not simply a cultural problem that has a technological dimension. It is also a regulatory issue. A cyberspace regulatory framework could help to transform the Internet into a safer place to conduct activities. An appropriately adapted legal framework and laws that are applicable to the digital world must be both operational at the national level and internationally compatible. At the same time, qualified participants in the justice system and police authorities skilled in ICT and cybercrime should enforce the legal aspects of information technologies and cooperate with their partners at the international level (UNODC, 2013).

4.0 CONCLUSION

Having explained the issues of cyber threats and cyber safety in this Unit, it is crystal-clear that cyber safety measures aimed at anticipating, recognizing, and tackling the problem of cyber security that were developed by internet developers and security groups are important mechanisms for combatting cybercrime and its associated threats on the cyberspace.

5.0 SUMMARY

In this unit, students have been made to understand how to anticipate, recognize, and tackle the problem of cyber threats. Also, both simple and complex strategies that Internet users can adopt for ensuring safety on the cyberspace were highlighted and discussed.

6.0 TUTOR-MARKED ASSIGNMENT

1) Differentiate between threat modelling and control flow integrity
2) With relevant examples, discuss the major cyber safety tips that you are familiar with

7.0 REFERENCES/FURTHER READING

Clough, J. (2010). *Principles of Cybercrime*. Cambridge University Press.

McQuade, S. C. (2009). *Encyclopedia of Cybercrime*. Green Wood Publishing Group.

United Nations Office on Drugs and Crime (2013). *Comprehensive Study on Cybercrime*. UNODC, Vienna.

Waschke, M. (2017). *Personal Cybersecurity: How to Avoid and Recover from Cybercrime*. Bellingham, Washington, USA.

MODULE 5 CYBERCRIME AND ELECTRONIC EVIDENCE

Unit 1 What is Electronic Evidence?
Unit 2 Procedures for Generating Electronic Evidence
Unit 3 Electronic Evidence Handling in Cybercrime Investigation
Unit 4 Sourcing for Electronic Evidence in Cybercrime Investigation
Unit 5 The Place of Electronic Evidence in Criminal Trials

UNIT 1 WHAT IS ELECTRONIC EVIDENCE?

CONTENTS

1.0 Introduction
2.0 Objectives
3.0 Main Content
3.1 What is Electronic Evidence?
4.0 Conclusion
5.0 Summary
6.0 Tutor- Marked Assignment
7.0 References/Further Reading

1.0 INTRODUCTION

With the rapid advancement in the nature, dimension and patterns of cybercrime, electronic evidence has assumed a pivotal position in the detection of online crimes, the prosecution of cybercriminals, and the court determination of cybercrime cases. Generally, electronic evidence is tendered in court for the purpose of either convicting or acquitting a criminal suspect. Before an electronic can become admissible in a court of law, its authenticity and integrity have to be clearly established. Also, it must be adequately confirmed that the procedure for its extraction and preservation comply with the extant laws governing the use of electronic evidence.

2.0 OBJECTIVES

At the end of this Unit, you should be able to:

- define electronic evidence
- state the importance of evidence in criminal trials
- discuss types of evidence
- explain electronic evidence in relation to cybercrime.

3.0 Main Content

3.1 What is Electronic Evidence?

Evidence is anything that is useful to a judge or jury in deciding the facts of a case. It may take the forms of witness testimony, written documents, videotapes, magnetic media, photographs, physical objects, and so on

(Schmalleger, 2011). Therefore, evidence can be defined as any object or piece of information that is relevant to the crime being investigated and whose collection was lawful. It is the means by which facts relevant to the guilt or innocence of an individual at trial are established.

Evidence is central to the determination of any criminal trial due to the following reasons:

a. prove that an actual crime has taken place ("corpus delicti")
b. link a particular person to a crime
c. disprove or support the testimony of a victim, witness, or suspect
d. identify a suspect
e. provide investigative leads
f. eliminate a suspect from consideration.

Types of Evidence

Evidence comes in different forms ranging from direct to circumstantial, testimonial, documentary, demonstrative, physical, hearsay amongst others. They are all primarily employed to determine or establish the merit (to prove or disprove) of a case. Explanation regarding the nature of some types of evidence is provided below:

a. Direct evidence: this is straightforward evidence that establishes the fact of case. Typically, it is usually employed to prove a fact of a case without requiring the judge or jury to draw inferences. For example, direct evidence may consist of the information contained in a photograph or a videotape. It might also consist of testimonial evidence provided by a witness on the stand. Another form of direct evidence that a particular individual engaged in illicit activity is the confession of the suspect that he or she actually committed the alleged offense.

b. Circumstantial Evidence: this type of evidence is indirect in nature. It essentially requires the judge or jury to make inferences and to draw conclusions. Circumstantial evidence is sufficient to produce a conviction in a criminal trial. It generally allows someone to infer the truth of a given fact.

c. Testimonial Evidence: testimony is a type of evidence that consists of witnesses speaking under oath, including eyewitness and expert testimony. A witness is considered competent to testify if he or she meets several criteria outlined in the criminal code of a country. For instance, the individual who testifies must have personal knowledge of the subject about which he or she is providing information. This can be either firsthand knowledge of the crime—if the individual is an eyewitness—or specialized knowledge directly resulting from education, training, experience, and skills required to authenticate or refute a piece of information that is being presented in the case

(Clough, 2010). This specialized knowledge is required for those individuals who are called to provide expert testimony.

d. Physical Evidence: this is also known as real evidence. This type of evidence is generally utilised to corroborate suspect, witness, and victim statements; to link a suspect to a crime scene or crime; to link a suspect to a victim; or to rule out a person as a possible suspect. This tangible evidence includes objects such as ammunition, firearms, knives, glass, and questioned documents (handwritten or typewritten documents whose authenticity has yet to be established). Physical evidence found on computers and related electronic devices usually take the form of trace evidence and impression evidence. Trace evidence includes items that are extremely small (i.e., microscopic), such as soil, hair, fibers, and dust. Fingerprints are considered impression evidence. Normally, fingerprints are not visible to the human eye (and, therefore, are known as latent fingerprints) and need to be enhanced with some sort of chemical developer (Clough, 2010).

e. Documentary Evidence: this form of evidence consists of any kind of writing, video, or sound recording material whose authenticity needs to be established if it is introduced as evidence in a court of law. Examples include business records, manuals, and computer printouts. The genuineness of each piece of documentary evidence needs to be established. Typically, an expert provides testimony as to the authenticity of the evidence being presented, although certain exceptions to this rule exist.

f. Demonstrative Evidence: this form of evidence cannot independently prove a fact of a case. It is typically used to explain other evidence; illustrate, demonstrate, or recreate an event; or show a situation similar to something being presented in a case. Diagrams, drawings, maps, models, and sketches are used to make evidence more understandable. Photographs and videos are other examples of this type of evidence, which provides a visual depiction of what happened at a crime scene and/or what is being narrated by the individual testifying in court.

Typically, evidence of cybercrime acts is almost always in electronic or digital form. These data can be stored or transient, and can exist in the form of computer files, transmissions, logs, metadata, or network data (UNODC, 2013). Electronic evidence consists of any type of information that can be extracted from computer systems or other digital devices and that can be used to prove or disprove an offense or policy violation (Maras, 2015). Such evidence can illustrate possession and intent. The presence of child pornography images on one’s computer can show possession, for example. Intent could be shown if these images were organized and placed in alphabetized files according to the child’s screen name. Electronic data can be used to support a claim or can serve as an alibi. By analyzing the evidence retrieved during computer forensics investigations, investigators try to figure out what happened, when it happened, how it happened, why it happened, and who was involved (Maras, 2015).

Generally, acquisition of electronic evidence requires an amalgamation of traditional and new policing techniques because it often requires a delicate procedure. Law enforcement authorities may use ‘traditional’ police work (interviewing victims or undercover visual surveillance of suspects) in some stages of an investigation, but require computer-specific approaches for other parts. These can include viewing, and seizing or copying, computer data from devices belonging to suspects; obtaining computer data from third parties such as internet service providers, and – where necessary – intercepting electronic communications (UNODC, 2013).

Regardless of the way that a piece of technology may be utilized or affected, any information stored on the device that ties it to a crime constitutes digital evidence, defined as information that is either transferred or stored in a binary format (Casey, 2011). Laptops, desktops, mobile phones, tablet computers, Kindles, GPS devices, digital cameras, flash drives, CDs, DVDs, and even video game systems all store digital files in some fashion. Thus, any applications, email, images, video, audio files, browser histories, search histories, user contacts, and other information stored on these devices constitute digital evidence (Holt & Bossler, 2016). This information may be used in the course of investigations of both on and off-line crime. For instance, the browser history of an individual’s laptop may provide evidence of searches for and attempts to illegally download movies and television shows (Casey, 2011; Ferraro & Casey, 2005). At the same time, law enforcement officers may seize a drug dealer’s mobile phone in order to capture text messages, call logs, and contact details to see who they are communicating with, and determine if the device may implicate the individual in drug trafficking or other crime (e.g. Holt, Bossler, & Seigfried-Spellar, 2015).

The inherently social nature of the web and CMCs has also led law enforcement and intelligence agencies to seek digital evidence, or artifacts, from websites and social media that implicate individuals in criminal activity. The broad range of storage devices that may contain digital evidence requires law enforcement to carefully search any suspect and crime scene to identify all potential pieces of technology that may implicate an individual in an offense (Holt & Bossler, 2016). Moreover, there are major variations in the ways that different devices work, and how they may connect to the Internet. This directly impacts the way that an officer must handle the device to ensure that it is properly maintained and will not be rendered inadmissible later during any court proceedings. Not all law enforcement officers are aware of the differences in the processes and storage capacities between devices—even those made by the same company. In fact, the constantly evolving nature of technology makes digital evidence handling one of the most complex issues that law enforcement may face in the field (Holt & Bossler, 2016).

4.0 CONCLUSION

The importance of electronic evidence in the 21st century cannot be overemphasized. As the advancement in technology has increased the range and intensity of cybercrime, so also has the scope of digital devices from which electronic evidence can be extracted.

5.0 SUMMARY

In this unit, effort has been made to introduce students to the type of evidence, with particular focus placed on the meaning and expected qualities of electronic evidence. The centrality of electronic evidence to the operation and criminal investigations of law enforcement officials was also carefully explained.

5.0 TUTOR-MARKED ASSIGNMENT

1. What is electronic evidence?
2. Compare and contrast electronic evidence and physical evidence
3. The prosecution of cybercriminals will be impossible without electronic evidence. Discuss

7.0 REFERENCES/FURTHER READING

Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Third edition. Waltham, MA: Academic Press.

Clough, J. (2010). *Principles of Cybercrime*. Cambridge University Press.

Ferraro, M., & Casey, E. (2005). Investigating Child Exploitation and Pornography: The Internet, the Law, and Forensic Science. New York, NY: Elsevier Academic Press.

Holt, T. J. & Bossler, A. M. (2016). *Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses*. Routledge.

Holt, T.J., Bossler, A.M., & Seigfried-Spellar, K. (2015). Cybercrime and Digital Evidence: An Introduction. London: Routledge.

Maras, M. (2015). *Computer Forensics: Cybercriminals, Laws and Evidence (Second Edition)*. Jones & Bartlett Learning.

Schmalleger, F. (2011). *Criminal Justice Today: An Introductory Text for the 21st Century*. Pearson Prentice Hall.

United Nations Office on Drugs and Crime (2013). Comprehensive Study on Cybercrime. UNODC, Vienna.

UNIT 2 PROCEDURE FOR GENERATING ELECTRONIC EVIDENCE

CONTENTS

1.0 Introduction
2.0 Objectives
3.0 Main Content
3.1 Procedures for Generating Electronic Evidence
4.0 Conclusion
5.0 Summary
6.0 Tutor -Marked Assignment
7.0 References/Further Reading

1.0. INTRODUCTION

The retrieval of evidence from electronic device involves a careful and meticulous process which usually starts from search, discovery, and documentation of such evidence and confiscation /archiving of the extracted electronic device. Such evidence in electronic form could be documents, photos, image files, e-mails. Forensic experts with special knowledge are in charge of this type of investigation to avoid damage, loss, and manipulation of evidence. The common principles and approved procedures generally apply when investigating electronic evidence to avoid formal challenges in court to the authenticity, integrity and originality of the extracted data.

2.0 OBJECTIVES

At the end of this Unit, you should be able to:

- know the basic steps to be followed in the extraction of digital evidence
- explain the procedures to be followed by electronic evidence investigators.

3.0 MAIN CONTENT

3.1 Procedures for Generating Electronic Evidence

Many forms of electronic evidence may be comparatively straightforward, such as a printout of a readily available email sent by a perpetrator of a crime, or IP connection logs reported directly by an internet service provider. Other forms, on the other hand, may require sophisticated tools and techniques in order to recover traces of activity or data from computers and networks that can provide evidence of criminal behaviour (UNODC, 2013). To discover such traces, digital forensics experts take advantage of the tendency of computers to store, log and record details of almost every action that they, and hence their users, perform (Clough, 2010).

To acquire electronic evidence, an investigator must determine whether he or she will conduct an onsite or offsite search. More often than not, the factors that usually influence this decision include the size and complexity of the computer system and related electronic devices, the technical demands of the search, and the specialized knowledge and skills required to successfully conduct the search (Maras, 2015). Computer forensics investigations can be very time-consuming. Partly for this reason, searches of computers and electronic devices are frequently conducted off site.

When the target of the search and seizure is a computer or information stored in the computer, the investigator needs to document how the computer was set up when it was found and what it was doing at the time of the seizure. It is important to note that computers can be accessed remotely. As such, computers should be isolated from networks (i.e., connections to other computers) and telephone lines to prevent the tampering with or destruction of data (Maras, 2015). Computers may also be connected to the Internet on a wireless basis. In all of these circumstances, an investigator should document these connections to computers and then disconnect them. The status of the computer (on, off, or in sleep mode) must first be documented in the investigator's notes and photographed. To determine if the computer is on, the investigator will check whether the computer's light is on and whether the fan is running (which, of course, can be heard). If the computer is warm, that fact may indicate that the computer was on or that it was recently turned off. To secure the computer as potential evidence, if the computer is off, it should remain off. If the computer is on, it should remain on. If an investigator immediately shuts down the computer after arriving at the scene, potential evidence could be destroyed (Maras, 2015).

Electronic evidence is fragile and could be changed if the investigator accidentally or even purposely hits a key on the keyboard or clicks on the mouse. In particular, data held in computer memory could be lost through such an action. As such, all volatile data should be immediately noted and photographed. The date and time of the computer system must also be documented (Maras, 2015). If the computer is in sleep mode, the investigator should move the mouse slightly, without touching any keys. Under no circumstance should the investigator click on the mouse or press any keys on the keyboard to display something on the computer screen; doing so may modify data. Moreover, the suspect may have created a kill switch. For instance, the suspect may have programmed the computer to write over the hard drive in such a manner as to render the data in it unusable if a particular key is pressed on the keyboard (e.g., "Enter"). The investigator should note how the computer is set up. Photographs of the computer from each side should be taken (Maras, 2015). The entire computer system configuration should also be photographed, including cable connections, electrical wires, and outlet configuration. The investigator should also thoroughly document the peripheral devices that are connected to the computer. The ports that the cables are connected to should be documented as well. Color-coordinated tags should be used to label the cables and their connections to ports of the computer. This will allow a computer forensics specialist to set up the computer at the forensic lab in exactly the same manner it was set up at the crime scene. The status of the peripheral devices —whether they were on or off—must also be noted. If dealing with a desktop computer, the investigator should also note the position of the mouse in relation to the keyboard. Was it on the left side or the right side of the keyboard? This factor will help determine whether the computer user was left-handed or right-handed (Maras, 2015).

After the investigator has completed documenting the computer and its attached peripheral devices, the unit will be powered down if it was found on or in sleep mode. After the computer is powered down, its power cable should be disconnected from the wall socket, but not from the computer. This procedure, however, is not appropriate for each computer system; rather, the procedure used depends on the computer's operating system. The previously described procedure can be used for Windows operating systems. Other operating systems, such as UNIX/Linux and Macintosh, require different shutdown procedures. For example, to shut down computers with Macintosh operating systems, an investigator must click on the apple icon in the menu bar and then select "Shutdown. When the screen indicates that it is safe to turn off the computer, the investigator should then pull the computer's power cord from the wall socket (Maras, 2015).

Finally, other electronic devices found on scene such as mobile phones, personal digital assistants (PDAs), and caller ID boxes should be handled with special care, as they contain volatile data. If such devices are on, then the data displayed must be documented as soon as possible. When seizing mobile devices or PDAs, special procedures are required for their packaging and analysis at the forensic lab. The appropriate procedures for analysis of these devices must be followed to ensure the admissibility of data extracted from them in court (Maras, 2015).

4.0 CONCLUSION

Electronic evidence is highly fragile and sensitive in nature. Thus, the process of extracting them is not often simple and haphazard to the extent that it can be conducted by a layman. Rather, electronic evidence gathering typically requires a carefully a planned systematic procedure that can be only handled by forensic experts.

5.0 SUMMARY

In this unit, you have been exposed to the basic rules and regulations guiding forensic investigators in the course of extracting electronic evidence on the field. Also, the basic procedure that need to be followed in the analysis of electronic devices so as to guarantee the admissibility of data extracted from them in court are discussed.

5.0 TUTOR-MARKED ASSIGNMENT

1. Discuss the procedure for generating electronic evidence

2. What are the steps expected of a forensic investigator in the course of electronic evidence extraction?

7.0 REFERENCES/FURTHER READING

Maras, M. (2015). *Computer Forensics: Cybercriminals, Laws and Evidence (Second Edition)*. Jones & Bartlett Learning.

United Nations Office on Drugs and Crime (2013). Comprehensive Study on Cybercrime. UNODC, Vienna.

UNIT 3 ELECTRONIC EVIDENCE HANDLING IN CYBERCRIME INVESTIGATION

CONTENTS

1.0. Introduction
2.0. Objectives
3.0. Main Content
3.1 Electronic Evidence Handling in Cybercrime Investigation
4.0. Conclusion
5.0. Summary
6.0. Tutor-Marked Assignment
7.0. References/Further Reading

1.0. INTRODUCTION

In the process of investigating cybercrime, there are some digital devices usually seized for the purpose of being searched for evidence extraction. Thus, some level of technical know-how is often required of specialists handling such electronic evidence. Consequently, the handling of electronic evidence in cybercrime investigation usually involves a systematic collection of items of evidence that typically starts from the point of documentation to the point of analysis of extracted evidence.

2.0 OBJECTIVES

At the end of this Unit, you should be able to:

- discuss how electronic evidence should be handled in cybercrime investigation
- describe the requirements expected of computer forensic experts.

3.0 MAIN CONTENT

3.1 Electronic Evidence Handling in Cybercrime Investigation

Electronic evidence is generally very delicate by nature. Therefore, it must be professionally handled all through its lifecycle. Typically, certain requirements are expected of computer forensics experts for the purpose of ensuring the protection and preservation of electronic evidence. These requirements are the focus of this section:

i. *Identifying Evidence*

When identifying potential evidence in computer forensics investigations, an investigator should not overlook nondigital evidence. Specifically, the investigator should not forget about any physical evidence (e.g., trace and impression evidence, such as fibers, hair, dust, and fingerprints) that might be on or near the computer, keyboard, mouse, and other related electronic devices. Storage devices such as DVDs, CDs, and flash drives should be considered physical evidence as well. Because the chemicals used to process extract the electronic evidence from, for example, a CD before he or she dusts it for fingerprints so as not to damage it. The investigator should photograph and collect any books, papers, notes, and hardware relating to his or her investigation. In addition, it may be necessary to seize any documentation that explains the hardware and software installed on the system (Maras, 2015). Often, individuals keep passwords and decryption keys within their view. As such, notes, papers, Post-it notes, and other such items that are found on a desk, table, bookcase, computer, and related devices, as well as on walls or boards close to the computer, may hold such information and, therefore, should be collected. As part of the search for evidence, an investigator should look under desks and tables, in areas of concealment near the computer, and inside manuals and books. Any trash bins should be checked for potential evidence as well. Basically, investigators should look everywhere they are authorized to by law.

ii. *Extracting Electronic Evidence*

When investigating a computer system, the computer forensics technician must also choose a computer forensics tool to image the hard drive whose validity for this purpose has been upheld in court. Otherwise, the validity of the tools used to create the image of the hard drive may be called into question and the evidence deemed inadmissible. The investigator must also have all the appropriate tools with which to examine the evidence. For instance, most computers are password protected. As such, a password cracking tool would be required to gain access to the suspect's computer system. Consistent with applicable law, it is better to try to get the owner of the computer to voluntarily divulge his or her username, passwords, and decryption passphrase, if possible. Password cracking software should be used cautiously, as an individual may have set the computer to recognize unauthorized access to the system (with repeated failed attempts to access the system) by setting a "booby trap" to delete the data that the investigator is trying to retrieve (Maras, 2015).

iii. Tagging, Bagging, and Transporting Evidence

All physical items that are collected as evidence must be labeled, packaged, and transported to a forensic laboratory. At a minimum, the label should include the case number, the initials of the investigator, the date when the evidence was found, a description of the evidence, and the location where the item was found. All evidence should be packed into antistatic packaging. Faraday bags are required to prevent messages from being sent or received by electronic devices (such as PDAs and mobile phones). Items should be wrapped in static-free bubble wrap and placed in separate containers to prevent shifting (Maras, 2015) Each external hard drive, flash drive, and other electronic storage device must be placed in a separate paper envelope. Items should be disassembled for packaging and transport only as required. Special factors that computer forensics investigators need to consider when packaging and transporting evidence are magnetic fields, static electricity, corrosive elements, and temperature. Caution should also be taken to ensure that evidence is not altered, damaged, or destroyed by any of these factors during its packaging and transport.

iv. *Preservation of Evidence at the Forensic Lab*

After its collection, evidence is usually sent to a laboratory for forensic analysis. At the forensic laboratory, all of the seized items need to be inventoried, recorded, and secured in a locked room. Access to this room must be restricted to essential personnel only. The room should be guarded, and access to it should be regulated and recorded in a log. In the lab, computer systems and related devices must be secured away from extreme temperatures, humidity, dust, and other possible contaminants. Thus, when electronic evidence has been transported to the forensic lab, it should be kept in a cool, dry place, away from magnetic fields or radio frequency interference sources and in a climate-controlled environment.

v. *Analysis of Evidence*

All of the actions of the computer forensics specialist must be documented. Investigators need to document which evidence was obtained, where the evidence was taken from, when the evidence was collected, how the evidence was acquired, and who retrieved the evidence. Investigators will need to provide proof in court that they preserved all the data in a computer system without damaging or modifying it. If any modifications were made to the evidence, the investigators must be able to provide a reasonable explanation for why this change occurred. An exact copy of the data contained in the hard drive of a computer or electronic device is required for analysis. Security measures must be taken to ensure that computers and related electronic devices and the data in them are protected from potential damage or modification (with, for example, tamperproof storage devices and a write blocker). To minimize possible alternations, destruction, or damage of data, the computer forensics specialist should limit access to the data. An investigator can analyze the copy of the hard drive in several ways. For example, he or she might search the copy for any files that the suspect may have purposely hid or deleted. An investigator could also conduct an analysis to find suspect application software—for instance, software such as Timestomp, which seeks to modify or erase timestamp information of a file, a program, or the computer system itself. Data can be analyzed to determine the dates and times when files, emails, and programs were created, accessed, modified, and downloaded. The dates and times of the computer system can provide information on who accessed the system and, if shared computers are involved, which users were logged on to the computer.

4.0 CONCLUSION

Specialised skills and knowledge are indispensable to the effective handling of electronic evidence needed for the successful investigation of cybercrime and for the successful prosecution of cybercriminals. Therefore, five major requirements are typically expected of computer forensic investigators at the point of extracting evidence from digital devices.

5.0 SUMMARY

In this unit, students have been introduced to the five basic requirements expected of computer forensic investigators handling cybercrime investigations. These requisite steps include: electronic evidence identification, electronic evidence extraction, tagging, bagging/transportation of electronic evidence, preservation of electronic evidence at selected forensic laboratory, and electronic evidence analysis.

6.0 TUTOR-MARKED ASSIGNMENT

1. With relevant examples, discuss the procedures involved in the extraction of electronic evidence.
2. Explain the process of electronic evidence analysis.

7.0 REFERENCES/FURTHER READING

Maras, M. (2015). *Computer Forensics: Cybercriminals, Laws and Evidence (Second Edition)*. Jones & Bartlett Learning.

United Nations Office on Drugs and Crime (2013). Comprehensive Study on Cybercrime. UNODC, Vienna.

UNIT 4 SOURCING FOR ELECTRONIC EVIDENCE IN CYBERCRIME INVESTIGATION

CONTENTS

1.0 Introduction
2.0 Objectives
3.0 Main Content
3.1 Sourcing for Electronic Evidence in Cybercrime Investigation
4.0 Conclusion
5.0 Summary
6.0 Tutor-Marked Assignment
7.0 Reference/Further Reading

1.0. INTRODUCTION

Cybercrimes are traced and investigated with various sources of electronic evidence that are helpful for prosecution and conviction of cybercriminals. Cybercrime investigation, therefore, requires the discovery of electronic evidence, alongside non-electronic evidence. Such electronic evidence can be found on any type of computer and any other type of digital device used for the perpetration of the crime. Evidence of cybercrimes may be present on a computer's hard drive or any other peripheral equipment. The identification of potential electronic evidence can be simple and overt or complex and covert. Therefore, the process of sourcing for electronic evidence often requires the expert knowledge of digital forensics experts.

2.0 OBJECTIVES

At the end of this Unit, you should be able to:

- discuss the generation of electronic evidence during cybercrime investigation
- classify and discuss the procedure for electronic evidence sourcing on digital devices and the locations from which such type of evidence can be generated.

3.0 MAIN CONTENT

3.1 Sourcing for Electronic Evidence in Cybercrime Investigation

Despite the fact that electronic evidence is increasingly becoming ubiquitous as a result of the growing availability of computer systems, PDAs and storage devices, this important information may not readily accessible to an untrained person. Trained computer forensics experts are better professionally skilled to source for electronic evidence in cybercrime investigation. Electronic evidence is not conspicuously obvious on the digital devices containing them. Rather it is to be professionally sourced in certain locations.

Electronic evidence is most commonly found on hard drives. Generally, data in the hard drives of computers consist of both volatile and nonvolatile data

(Maras, 2015). Volatile data disappear when the computer is powered off, whereas nonvolatile data are stored and preserved in the hard drive when the computer is powered off. Evidence in the hard drives of computers may be found in files created by the computer user (e.g., emails, spreadsheets, and calendars), files protected by the computer user (e.g., encrypted and password-protected files), files created by the computer (e.g., log files, hidden files, and backup files), and other data areas (e.g., metadata). Maras (2015) identified some of the locations that should be examined for evidence on a digital device as including the following:

1. Files Created by Computer Users

Files created by the user usually include document (e.g., Word; file extensions of either ".doc" or ".docx"), text, spreadsheet (e.g., Excel), image, graphics, audio, and video files. These files contain metadata (i.e., data about data).

1a. Metadata can provide the following kinds of information:

i. name of the author of the document and the company the document belongs to
 owner of the computer
ii. date and time the document was created
iii. last time the document was saved and by whom it was saved
iv. revisions made to the document
v. date and time the document was last modified and accessed
vi. last time and date the document was printed
vii. metadata can also yield substantial evidence related to an incident or crime.

1b. Timestamp data (i.e., the time of events recorded by computers) may also provide valuable information to an investigation. It can yield the following data:

i. validate a statement or testimony the suspect made
ii. provide the suspect with an alibi
iii. eliminate the person from consideration as a possible suspect.

The use of Timestomp can frustrate computer forensics investigations if the offender has taken specific measures to conceal his or her use of this software. For instance, an investigator will be alerted to the use of this type of software if the suspect clears the timestamp of the entire system. Therefore, an investigator should also check the computer to see if the suspect has created a calendar. Calendars may hold appointment information and other data that can reveal important clues about the suspect's whereabouts on a given date and time. It can also reveal the contacts of a suspect.

1c. additionally, investigators should examine Web browsers for any files created by the user. In particular, they may look at particular websites that a user may have bookmarked or added to his or her favorites folder in the Web browser. Evidence can also be retrieved from email accounts. For instance, address books in email accounts can include the contacts of the suspect. Other pertinent information to a criminal or civil case under investigation can be retrieved from emails in the inbox, sent, delete, draft, and spam folders of an account, which reveal the content of communications and the persons with whom the suspect was communicating.

2. *Files Created by the Computer*
Files that are created by the computer may also have evidentiary value. Files that may assist a computer forensics specialist in his or her investigation include event logs, history files, cookies, temporary files, and spooler files.

2a. Event Logs

Event logs automatically record events that occur in a computer to provide an audit trail that can be used to monitor, understand, and diagnose activities and problems within the system. Several event logs are now displayed on the screen including the following:

- Application logs: these logs contain the events that are logged by programs and applications. Errors of these applications and programs are also recorded in this log.
- Security logs: these logs record all login attempts (both valid and invalid) and the creation, opening, or deletion of files, programs, or other objects by a computer user.
- Setup logs: these logs provide data on applications that are installed on a computer.
- System logs: these logs provide information on Windows system components. For example, they record any failure of a component to load during the startup process.
- Applications and services logs: these are new event logs in Windows 7. Instead of recording events that may affect the system as a whole, each log stores events from a single application or component.

The most important event log of those mentioned previously is the security log, which records all login attempts and activities of the computer user. As such, this log can indicate that malicious activity or other forms of cybercrime have been or are being committed. For instance, numerous failed login attempts in the security log may indicate that someone is trying to access the computer without authorization. Moreover, this log can reveal a suspect’s attempt to delete data from the computer.

2b. History Files

The operating system also collects data about the websites visited by a user. The toolbars of most Web browsers save the browsing history of the computer user. Although the majority of cybercriminals erase their browser history, it is important to check it in case its contents have been overlooked by the offender. The address bar of a Web browser should also be checked, as it is often overlooked by offenders. This area does not provide information on all websites viewed, but includes those whose addresses were explicitly typed or copied and pasted into the address bar by the user. Most online chatroom software temporarily stores chat session logs. It also affords users the opportunity to permanently save logs of chat sessions. The default settings of certain chat room software (e.g., Gmail instant messenger) are set to temporarily save messages until the user clicks on "More" and chooses "Go off the record." Once this option is selected, chats are not saved and a message appears informing the user that chats "are now off the record". Users may actually set this software to save all of the messages sent or received. With these settings, the logs can provide details of the discussions the suspect had. Thus, chatroom software provides a wealth of information of potential value to investigations.

2c. Cookies

Cookies are files created by websites that are stored on a user's computer hard drive when he or she visits that particular website. As such, by viewing cookies, the investigator can determine which websites the user has visited. Certain cookies are used by websites to gather information about an individual's activities, interests, and preferences. Others are used to store credit card information, usernames, and passwords. Some cookies do both. The type of information an investigator finds depends on the cookies stored on the suspect's computer.

2d. Temporary Files

Some files are created by the computer that is unknown to the user. Specifically, the operating system collects and hides certain information from the user. Computer also stores information about websites browsed, items searched online, usernames, and passwords. This material is stored in temporary Internet files or cache. Therefore, an investigator should check the temporary files because criminals may forget to delete the information that the computer stores. Some are not even aware that this information is stored. Other criminals take additional steps to delete these data. In particular, they may use software to delete browser cache, cookies, and other files. One such software package, Evidence Shredder Pro, claims to permanently delete this information and even provides the user with a panic button that will close all browser windows and wipe the computer if the user clicks on it.

2e. Spooler Files

As a default setting, most Microsoft Windows operating systems have print jobs "spool" to the hard drive before they are sent to the printer. Accordingly, a copy of the printed item is stored on the hard drive of the computer. This copy can be recovered and could provide vital evidence in the case under investigation.

3. Peripheral Devices

Peripheral devices are devices that are not essential parts of a computer system, such as scanners, copiers, printers, and fax machines. Such devices can contain valuable information about the case being investigated. Suppose the crime being investigated is child pornography, and images of child pornography have been found on the suspect's computer. These digital images could have been generated from a variety of sources. It is possible for investigators to determine the particular device that generated the image and the make and model of the device. For instance, the scanner may leave potential markings on scanned items that may link pictures or documents to the particular scanner. Specks or marks on the scanned item may result from dirt or scratches on the glass window where the original document was placed and scanned.

4. *Telecommunication Devices*

Evidence can also be generated from a wide range of telecommunications such as fixed telephony, mobile phones, and answering machines. The following types of evidence are available from fixed telephony:

- calls made, received, and missed
- voice mails
- messages
- favorite numbers.

In mobile phones, the following types of evidence may be found:

- names and numbers of contacts
- calls made, received, and missed
- date, time, and duration of calls
- text messages.

Nowadays, mobile phones have vast storage capacities and can hold even more information than that listed above that can be used by investigators. In particular, mobile phones may be able to send emails, take photographs, download music, send instant messages, record and play videos, open application files (e.g., documents, spreadsheets, and presentations), and browse the Internet. Mobile phones may even store global positioning system (GPS) coordinates when photographs are taken, along with the time and date when the photo was created. Additionally, mobile phones may contain GPS navigation systems. Thus, an investigator can pull up the GPS history and any addresses programmed into the GPS and determine which places an offender visited. Moreover, some mobile phones can link to work and home computers, thereby providing investigators access to even more potential evidence. Finally, answering machines can contain, among other things, recorded voice messages (current or deleted), missed calls, caller identification information, and the last number called or dialed on the device.

5. *Handheld Computing and Wireless Devices*

Examples of handheld computing and wireless devices include pagers and personal digital assistants (PDAs). Extra care must be taken when seeking evidence from these devices because these devices usually lose their evidentiary value if power is lost. The information on these devices is also easily destroyed. For instance, incoming messages can delete a pager's stored information. Pagers may contain messages that are of interest to the investigator seeking forensic evidence. Many different kinds of pagers are available on the market, and the type of pager will determine the data that may be retrieved from it:

- a tone-only pager alerts the user that an individual has tried to contact him or her. To hear a message that an individual may have left for the user, the recipient must contact the paging service.
- numeric pagers, as the name implies, provide data in the form of a numeric code or telephone number.
- alphanumeric pagers can handle both text and numeric messages.
- voice pagers actually transmit the voice messages directly to the user.

Pagers have largely fallen out of favor today, and many companies have discontinued making them. However, they are still used by some people (e.g., emergency services and medical personnel). The procedure for handling a PDA is similar to that for handling a pager. PDAs may contain evidence of a crime or incident in its documents. Previously, these devices were limited to a single function—acting as a personal information organizer. These days, PDAs can be used not only as organizers but also, among other things, to browse the Internet and send and receive text messages and emails; all of these actions may produce information that is pertinent to an investigation.

5. *Miscellaneous Electronic Devices*

Another type of electronic device that may be of interest to computer forensics investigators is the digital camera. Evidence of images, sounds, and date and timestamps may be retrieved from the memory cards of digital cameras. Digital cameras contain a wealth of metadata in Exchangeable Image File Format (EXIF). EXIF can provide the following kinds of information:

- date and time when a picture was taken (assuming that this capability has been set properly by the user)
- make and model of the camera used
- latitude, longitude, altitude, and Universal Time Coordinates (UTC) of the location where the picture was taken.

4.0 CONCLUSION

Regardless of the type of cybercrime committed, electronic evidence for cybercrime investigation is mainly sourced to nail and prosecute a suspected cybercriminal(s). This evidence is typically found on a computer system and other digital devices which allows for storing, processing, and dissemination information. Identifying such electronic evidence helps in cybercrime investigation if properly handled by a digital forensic investigator.

5.0 SUMMARY

This unit discussed the procedure for sourcing for evidence from a computer system and other digital devices. Attention was also devoted to locations where potential evidence can be extracted from electronic devices. Evidence of cybercrime perpetration can be found on a computer's hard drive or other peripheral equipment, internet history, removable media, and so on.

6.0 TUTOR-MARKED ASSIGNMENT

1. What are the sources for electronic evidence in cybercrime investigation?
2. With relevant examples, discuss the information that can be yielded by metadata and history files.

7.0 REFERENCE/FURTHER READING

Maras, M. (2015). *Computer Forensics: Cybercriminals, Laws and Evidence (Second Edition)*. Jones & Bartlett Learning.

UNIT 5 THE PLACE OF ELECTRONIC EVIDENCE IN CRIMINAL TRIALS

CONTENTS

1.0. Introduction
2.0. Objectives
3.0. Main Content
3.1 The Place of Electronic Evidence in Criminal Trials
4.0. Conclusion
5.0. Summary
6.0. Tutor -Marked Assignment
7.0. References/Further Reading

1.0. INTRODUCTION

Electronic evidence and computer forensics are relatively recent additions to the means of proof in legal proceedings. Therefore, in establishing the guilt or innocence of a defendant during a criminal trial, electronic evidence is admissible in courtroom if it has been confidently established that it has not been altered and damaged in any way. In the courtroom, the importance of electronic evidence is predicated upon how relevant and reliable it is. Before presentation of such evidences during criminal trials, it is necessary for an investigator to first of all establish that the electronic evidence is what it claims and carries an accurate representation of the data or information it claims before it becomes presentable in a criminal proceeding.

2.0 OBJECTIVES

At the end of this Unit, you should be able to:

- state the importance of electronic evidence in criminal trials
- explain the procedure for determining the admissibility of electronic evidence in criminal trials

3.0 MAIN CONTENT

3.1 The Place of Electronic Evidence in Criminal Trials

Procedures in a modern courtroom are highly formalized. Rules of evidence, which govern the admissibility of evidence, and other procedural guidelines usually, determine the course of a criminal hearing and trial. The primary purpose of any criminal trial is the determination of the defendant’s guilt or innocence (Schmalleger, 2011). In this regard, it is important to recognize the crucial distinctions that scholars make between factual guilt and legal guilt. Factual guilt deals with the issue of whether the defendant is actually responsible for the crime of which he or she stands accused. If the defendant did it, then he or she is, in fact guilty. Legal guilt is not as clear. Legal guilt is established only when the prosecutor presents sufficient evidence to convince the judge (where the judge determines the verdict) or the jury that the defendant is guilty as charged. The distinction between factual guilt and legal guilt is crucial because it points to the fact that the burden of proof rests with the prosecution, and it indicates the possibility that guilty defendants may, nonetheless, be found "not guilty" (Schmalleger, 2011).

Electronic evidence can play pivotal role in the outcome of a criminal trial. The following are some of the ways in which electronic evidence can be utilized in the course of a criminal proceeding:

i. electronic data can be used to support a claim or can serve as an alibi by a defendant. By analyzing the evidence retrieved during computer forensics investigations, investigators try to figure out what happened, when it happened, how it happened, why it happened, and who was involved.

ii. digital information can help to validate or dismiss an alibi or a witness statement, to prove that a specific action was performed at a given time, to determine how a crime was committed, to reveal links between an offender and a victim, etc.

iii. electronic evidence can be used to link a particular suspect to the crime.

iv. electronic evidence can also be used to eliminate a suspect from consideration.

v. electronic evidence can be useful for reconstructing a crime history.

According to Clough (2010), the following conditions are usually expected to be met before electronic evidence can be deemed admissible in the court of law:

a. that the investigator has the necessary technical background;
b. that the data collected are an identical copy of the original data (no changes made to the data or the media);

c. that the correspondence between the data presented and the original data can be demonstrated and authenticated;

d. that in the case of storage media that have been damaged or destroyed, intentionally or otherwise, any data supposed to have been deleted or destroyed can be recovered in a useful form and condition; and

e. that records of the time (time and date stamping) and the place of collection of data are systematically recorded, authenticated, and stored in a reliable way.

The data collected in this way can then be analysed, interpreted, and formatted in such a way that they are understandable to a non-technical audience that will include detectives, police officers, defense lawyers, magistrates, judges, and jury members. The investigators should always be capable of defending the results they have obtained, as well as describing and justifying the methods, tools, and techniques they have used to generate those results (Clough, 2010).

When searching for digital evidence, many problems arise including these key questions:

i. which elements may contain pertinent information for the case being investigated?
ii. how can the relevant data to be seized first be identified?
iii. how can investigators proceed?
iv. what procedural rules must be followed?
v. how can data be collected, stored and preserved?
vi. how can data be safeguarded and proof of its origins established, such that others may later analyze or review it?
vii. how can digital data be preserved as evidence for a potential trial, given that the storage medium from which the evidence was recovered is not infallible (for example, with date and time information being treated differently from one computer system to another) and subject to tampering?
viii. how can data be copied from its original support to another for analysis without modifying it?
ix. how can a non-modifying “bit by bit” copy be performed?
x. how can a copy be authenticated?
xi. how can the original data be preserved?
xii. how can it be guaranteed that the process of copying data does or did not modify it?
xiii. how can data copy analysis be conducted?
xiv. how can deleted files be recovered?
xv. how can a cybertrail be followed?
xvi. how can the origin of a message be proven?
xvii. how can an IP address that identifies a system in a network be linked to an individual?
xviii. how can primary binary data be transformed into significant and comprehensible information?
xix. how can results be presented to non-specialists?
xx. how can one avoid digital evidence becoming a false alibi?

To begin to answer these questions, some ICT computer forensic tools and procedures have been developed. However, only specially trained and competent experts should use them. Over the past few years, some evidence processing tools have been developed and commercialized, and their standardization is also a current issue (Clough, 2010). For instance, active communication monitoring and live surveillance could track criminals. Telephone, e-mail, or instant messaging eavesdropping is technically feasible to collect information related to both the content of communications and useful non-content, such as e-mail headers or IP addresses. In fact, criminals can also be identified through undercover investigation when investigators join, for example, Instant Messaging (IM) services, Peer-to-Peer networks (P2P), Internet Relay Chat servers (IRC), or newsgroups to lure criminals. But cybercriminals will always try to find ways to bypass security measures or to fool computer forensic tools or simply to develop anti-forensic actions (Clough, 2010).

4.0 CONCLUSION

It was explicitly established in this unit that electronic evidence is increasingly becoming important in legal proceedings during criminal trials. Electronic evidence is considered admissible in a court of law if it has carefully been established that it is not damaged, manipulated or altered in any way. Also, the presentation of electronic evidence during a criminal trial is dependent on how relevant and reliable such evidence is.

5.0 SUMMARY

In this unit, effort has been made to explain the importance of electronic evidence during criminal trials, the conditions that need to be fulfilled before electronic evidence can become in a court of law, and the major challenges that are usually present in the search for electronic evidence.

6.0 TUTOR-MARKED ASSIGNMENT

1. Explain the importance of electronic evidence during criminal trials.
2. Describe the basic conditions that electronic evidence need to meet before becoming admissible in a criminal tria.l
3. Discuss the major challenges that usually arise when searching for digital evidence.

7.0 REFERENCES/FURTHER READING

Clough, J. (2010). *Principles of Cybercrime*. Cambridge University Press.

Schmalleger, F. (2011). *Criminal Justice Today: An Introductory Text for the 21st Century*. Pearson Prentice Hall.

MODULE 6 COMPUTER FORENSICS AND CYBERCRIME INVESTIGATIONS

Unit 1 Meaning of Computer Forensics
Unit 2 Standard Phases in Computer Forensic Investigation
Unit 3 Computer Forensic Investigation Tools
Unit 4 Mobile Devices in Computer Forensic Investigation
Unit 5 Challenges associated with Computer Forensic Investigations

UNIT 1 MEANING OF COMPUTER FORENSICS

1.0. Introduction
2.0. Objectives
3.0. Main Content
3.1 Meaning of Computer Forensics
4.0. Conclusion
5.0. Summary
6.0. Tutor- Marked Assignment
7.0. References/Further Reading

1.0. INTRODUCTION

The purpose of computer forensics is to conduct an organized investigation with the goal of archiving a documented chain of evidence to find out exactly the type of crime perpetrated with the aid of a computer device (including other digital devices) or on a computer device (including other digital devices), and the perpetrator(s) of such a crime. In essence, computer forensic is typically conducted to extract useful evidence by carefully searching, uncovering, sieving and examining conspicuous and hidden folders in a computer device or other forms of digital device.

2.0 OBJECTIVES

At the end of this Unit, you should be able to:

- explain the meaning and purpose of computer forensics.

3.0 MAIN CONTENT

3.1 Meaning of Computer Forensics

With the increasing cases of cybercrime being recorded globally, computer forensics has now become crucial for public safety, national security, and law enforcement. Tracking the digital activities of potential criminals can help investigators find digitally stored information about their criminal activity (Information Technology, 2020). Computer forensics is not only capable of uncovering deliberate criminal intent but can also prevent future cybercrimes.
Computer forensics is a branch of forensic science that focuses on criminal procedure law and evidence as applied to computers and related devices

(McQuade, 2009). This branch of forensics is not only limited to computers, but also includes mobile phone forensics, personal digital assistant (PDA) forensics, and network forensics. Computer forensics is the process of obtaining, processing, analyzing, and storing digital information for use as evidence in criminal, civil, and administrative cases (Maras, 2015). The major goal of computer forensics is to provide forensic practices, legal processes, and ethical principles to assure reliable and detailed digital evidence that can be used for the courtroom needs, while its sole objective is to essentially guarantee a well-structured investigation and a follow-up of processes in order to resolve incidents and malfunctions in an organization.

Computer forensics is essentially concerned with the analysis of information that can be obtained from computers and other electronic devices such as printers, scanners, copiers, CDs, DVDs, Blu-ray disks, external hard drives, universal serial bus (USB) flash drives, magnetic tape data storage devices (e.g., linear tape-open [LTO] devices), cameras, mobile phones, fixed telephony, faxes, PDAs, portable media players (e.g., Apple's iPod), and gaming consoles (Maras, 2015). Technically, all these digital assets have a different design to store data and this makes the very base for dividing digital forensics into several categories. Its various subbranches include computer forensics, network forensics, forensic data analysis, and mobile device forensics (Maras, 2015).

As law enforcement, private investigation, and scientific discipline, computer forensics began during the early 1990s as personal computers (PCs) became popular among business and residential users (McQuade, 2009). The misuse of PCs to violate acceptable use policies, violate computer crime laws, or harm people in other ways led to the onset of computer forensics and advancements within this field (McQuade, 2009). Law enforcement in particular needed policies, procedures, and tools to identify, collect, and preserve digital evidence of various types of cybercrimes increasingly being committed by criminals.

Computer forensic specialists investigate security issues, data breaches, and other cybercrimes. Law enforcement, criminal justice, forensics, and cybersecurity all come together inside this field. That is why many computer forensic specialists work for law enforcement agencies. These experts recover documents, photos, emails, and other files from computer systems, hard drives, and other devices. They often work on "cybercrime" and digital cases and examine computer systems to help find digital evidence of illegal activity (Information Technology, 2020). Computer forensics is also focused on helping organizations deal with network breaches. In this context, forensic specialists will help determine how a breach happened in a computer system—the main focus of these experts is to look at digital breaches and hacks that have already happened, and learn from them for the future (McQuade, 2009).
Computer forensics consists mainly of searching for evidence and artifacts that indicate use, possession, or ownership of digital evidence. For this reason, computer forensics is like archeology insofar as the examiner is looking for evidence and artifacts that provide information from the past about who possessed, owned, and used certain things (i.e., computerized files) and for

what purposes. And like sciences underlying information technology (e.g., mathematics, physics, electronics, and chemistry), the scientific nature of computer forensics relies upon tested and verified processes recognized in courts of law for identifying and protecting incriminating data (McQuade, 2009).

Through the possibility created by forensics science, data can be retrieved from existing files (even those that have been deleted, encrypted, or damaged) or by monitoring user activity in real time. The information acquired from computers and other electronic devices can be used as evidence of a wide range of traditional crimes, cybercrimes, and computer misuses. It can also assist in the arrest and prosecution of criminals, the prevention of future illicit activity, the investigation of employee misconduct, and the termination of employment. The use of the acquired information depends on the type of investigation being conducted.

Information Technology (2020) identified the six stages involved in computer forensics examination in matters bordering on cybercrime as including:

i. Readiness

This stage assists the investigator to ensure that they are ready to take on investigation at any time. It ensures everyone has been trained correctly, ensures they understand legal ramifications of investigations, plan ahead for technical and non-technical issues, and make sure their equipment is ready anytime.

ii. Evaluation

This happens when a team is given information about an investigation. They assign roles and resources to the team, get details on facts and particulars about the case, and identify risks of the investigation.

iii. Collection

This involves the process of gathering evidence and learning about the cyberattack or cybercrime. Many tools and techniques are used to obtain this data, and can involve conducting interviews, obtaining the hard drives and other devices, and more. Devices are sealed in evidence bags to be further evaluated at the forensics lab.

iv. Analysis

This stage is vital to the success of an investigation. Evidence and data collected are analyzed to generate as much information as possible about the breach or crime. This can involve who performed the crime, when it happened, what data was lost, digital evidence, and more. The analysis must be accurate, must be documented and recorded, it must be unbiased, and it must meet correct deadlines.

v. Presentation

After analysis, the team presents a summary of its findings. They offer strategies to companies to help them increase their security and prevent issues in the future. A presentation will also be given to a court of law that needs details about the forensics evidence.

vi. Review

After the process is completed, the forensics team will do a review of how their investigation went, talk about things to improve in the future, and evaluate how to better serve in the next investigation.

4.0 CONCLUSION

This unit has discussed the meaning of computer forensics and the set of procedures that must be followed while investigating a computer device and other digital devices to avoid accidental contamination and unintentional damaging of electronic evidence.

5.0 SUMMARY

In this unit, effort has been made to explain adequately what computer forensics is all about and the six stages involved in computer forensics examinations.

6.0 TUTOR-MARKED ASSIGNMENT

1. Computer forensics is central to cybercrime investigation. Discuss
2. With relevant examples, discuss the six stages involved in computer forensic investigations

7.0 REFERENCES/FURTHER READING

Maras, M. (2015). *Computer Forensics: Cybercriminals, Laws and Evidence (2nd Ed.).* Jones & Bartlett Learning.

McQuade, S. C. (2009). *Encyclopedia of Cybercrime*. Green Wood Publishing Group.

UNIT 2 THE STANDARD PHASES IN COMPUTER FORENSIC INVESTIGATION

CONTENTS

1.0. Introduction
2.0. Objectives
3.0. Main Content
3.1 Standard Phases in Computer Forensic Investigations
4.0. Conclusion
5.0. Summary
6.0. Tutor -Marked Assignment
7.0. References/Further Reading

1.0. INTRODUCTION

Computer Forensics Investigation generally involves the investigation of electronic data retrieved from a computer hard disk or any other storage computing devices in line with strict adherence to standard policies and procedures to ascertain the type of crime perpetrated, the time/date such a crime was perpetrated, the location where the crime was committed amongst others. Specifically, the investigative processes involved in computer forensics investigation are in several stages. There are five major standard phases, and these are highlighted and discussed below.

2.0 OBJECTIVES

At the end of this Unit, you should be able to:

- discuss the five standard phases involved in computer forensic investigations.

3.0 MAIN CONTENT

3.1 Standard Phases in Computer Forensic Investigations

In computer forensics investigations, the following five steps usually enable digital examiners to effectively conduct their assignments:

1. Policy and Procedure Development

Computer forensics plays a vital role in investigating activities bordering on cybercrimes, criminal conspiracy, or any kind of digital evidence indicating a committed crime. These data are delicate and highly sensitive. Computer forensics investigators do understand how important it is to handle these data under proper protection; otherwise, it can be compromised easily. For this reason, it is important to establish strict guidelines and procedures to be followed by concerned investigators. These procedures usually include detailed instructions for computer forensic investigators about when they are authorized to perform recovery operations on possible digital evidence, what steps to follow to prepare systems for evidence retrieval, where to store the retrieved data, and how to document the complete activities for ensuring the integrity and credibility of the retrieved evidence (EC-Council, 2018). Typically, law enforcement and government agencies hire experienced cybersecurity experts to draw proper guidelines, policies, and procedures to be followed during computer forensic investigation. This policy and procedure also include a set of explicitly stated actions including what counts as evidence, what are the places on a computer to look for evidence, and how to handle the retrieved evidence (EC-Council, 2018). Another integral part of computer forensics is that there are times when prior permissions or warrants are required to get through the computer data of an individual.

2. *Evidence Assessment*

Evidence assessment is a critical part of digital forensics as it provides a clear understanding of the case details. This directly helps in classifying the cybercrime at hand. For an instance, to find pieces of evidence against someone with potential identity theft-related crimes, computer forensic investigators usually examine his/her hard drives, email accounts, social networking sites, and other digital archives for digital evidence linking him/her to the crime (EC-Council, 2018). Before starting an investigation, it is mandatory for the investigators to define the type of evidence they are seeking, with minute details like specific platforms and data formats. The investigators should also be clear about how to preserve the acquired evidence. Also, it is the investigator’s responsibility to verify the authenticity of the source and integrity of the pertinent data before including it into the list of evidence.

3. *Evidence Acquisition*

Rigorous documentation is needed before, during, and after the evidence acquisition phase. In this phase, you are required to document every tiny detail such as all hardware and software specifications, systems used for the investigation, and the system containing the potential evidence. During evidence acquisition, computer forensic investigators are subjected to follow the policies dedicated to preserving the integrity of potential evidence (EC-Council, 2018). With that, the investigators also need to follow general guidelines which list the physical removal of storage devices, proper retrieval of sensitive data, and ensuring operations by using controller boot discs and taking appropriate steps while copying and transferring digital evidence from targeted system to investigator’s system. This step should be completed carefully and legally as the documented evidence are crucial in the proceedings of a court case.

4. *Evidence Examination*

At this stage, the developed procedure should include guidelines for retrieving, copying, and storing evidence. The computer forensic investigators usually investigate officially assigned archives and recently deleted files by using specific keywords. Even the intentionally hidden or encrypted files are the suspicious evidence that investigators look for. Also, the analysis of file names offers you details like the date, time, and location where the data were created and downloaded. It simply helps the investigators to link the connection between uploading of files from storage devices to a public network (EC-Council, 2018). During this stage, the computer forensics investigators is expected to work closely with all the other personnel involved in the case as it helps in understanding what type of information can be tagged as evidence.

5. Reporting

For this last stage, the investigators need to have accurate records of their activities during the complete investigation. This step will ensure that all the guidelines, policies, and procedures have been followed throughout. Along with that, it ensures the authenticity and integrity of the data retrieved for the evidential reasons. The report will directly impact the civil proceeding if the validity of the evidence cannot be justified.

4.0 CONCLUSION

In cybercrime investigation, computer forensics is considered to be very important as it is mainly concerned with the generation of useful information from data extracted from a computer device or any other digital device suspected to have been used for the perpetration of a crime. Generally, five major phases are involved in computer forensics investigations.

5.0 SUMMARY

This unit has carefully discussed the five standard phases that are involved in computer forensics investigation. The phases identified and discussed included: policy and procedure development, evidence assessment, evidence acquisition, evidence accumulation, and reporting.

6.0 TUTOR-MARKED ASSIGNMENT

1. Describe the processes that need to be followed in the course of evidence assessment.
2. Critically discuss evidence acquisition phase in computer forensics investigation.

7.0 REFERENCE/FURTHER READING

EC-Council (2018). *An Introduction to Computer Forensics and How to Become a Computer Forensics Investigator*. EC-Council.

UNIT 3 COMPUTER FORENSIC INVESTIGATION TOOLS

CONTENTS

1.0. Introduction
2.0. Objectives
3.0. Main Content
3.1 Computer Forensic Investigation Tools
4.0. Conclusion
5.0. Summary
6.0. Tutor -Marked Assignment
7.0. References/Further Reading

1.0. INTRODUCTION

The retrieval of digital evidence in the course of forensic investigations requires the use of some specialised forensics tools. Depending on the type of computer device and the digital evidence to be retrieved, computer forensic investigation requires a set of dedicated tools as well as the use of some specific techniques. Among the most popular types of computer crimes that are investigated tusing forensics tools are credit card skimming, malware, phishing, denial of service (DoS) attacks, hacking amongst others.

2.0 OBJECTIVES

At the end of this Unit, you should be able to:

- discuss different computer forensic investigation tools
- explain the purpose of each computer forensics investigation tool.

3.0. MAIN CONTENT

3.1 Computer Forensic Investigation Tools

Due to the delicate nature of digital evidence, computer forensics investigation is often a systematic procedure involving the utilization of different specialised professional tools. A digital investigator should be able to determine how to apply specialised technical tools for the collection, preservation, and analysis of digital traces, and then follow appropriately tailored procedures for the extraction and processing of data. This forms part of the overall methodologies for digital investigations (the idea of digital forensics), the end results of which should be the production of evidence that can be presented to and accepted by the courts (Clough, 2010).

A computer forensics investigator must be equipped with the appropriate kits to collect, store, preserve, and transport forensic evidence. The tools the investigator uses will depend on the operating system (e.g., Windows or BlackBerry) and the type of electronic device (e.g., computer or mobile phone) to be examined (Clough, 2010). Therefore, choosing the right tools with which to examine computer system components and electronic devices for evidence is extremely important. Before examining the evidence with the chosen forensics tool, an investigator must ask himself or herself if the chosen software is appropriate for the computer system or electronic device in question (Maras, 2015).

According to a manual written by the Technical Working Group for Electronic Crime Scene Investigation, each investigator of a cybercrime is expected to carry a forensic toolkit that contains at least the following items:

1. documentation tools (e.g., cable tags and stick-on labels),
2. disassembly and removal tools (e.g., screwdrivers, pliers, and tweezers),
3. package and transport supplies (e.g., evidence tape, antistatic bags, and packaging materials),
4. and other essential items (e.g., flashlight, seizure disk, magnifying glass, and gloves).

Clough (2010) notes that the majority of forensic tools available to investigators, be they commercial products or open source tools, offer the same kinds of functionalities, including:

i. the creation of a bit-for-bit image – an exact copy – of the original data;
ii. the preservation of the data collected;
iii. time and date stamping;
iv. the recovery of files, directories, or data destroyed or hidden, and of the logs of actions or transactions;
v. search based on a number of criteria (key words, types of access request, file types, types of programme, amongst others);
vi. search for passwords;
vii. file descriptions (size, location, date of creation, date of last access, etc.) •presentation of results; and
viii. possible analysis of encrypted files or of metadata.

Some of the tools commonly deployed by computer forensics investigators for gathering, analysis and interpreting digital evidence are discussed below:

a. *Encase:* this is a computer forensics tool that is widely used by law enforcement agencies. It allows users to create an image of a drive without altering its contents and calculates the hash value for further authentication. It can locate hidden drives or partitions within a drive, as well as other hidden files or media that some other programs would not be able to discover. Encase can search multiple file locations and devices simultaneously. In doing so, it creates an index of what is found on the computer, such as emails and deleted files. Overall, it is an incredibly useful tool for investigations and for law Encase has been used by law enforcement agencies worldwide. The proven, powerful, and trusted EnCase Forensic solution, lets examiners acquire data from a wide variety of devices, unearth potential evidence with disk level forensic analysis, and craft comprehensive reports on their findings, all while maintaining the integrity of their evidence.

b. *ILook:* this tool is usually used to forensically examine computer media. Its capabilities include imaging, advanced email analysis, and data salvaging (to recover files that have been deleted by the user). This tool is used by the Criminal Investigation Division (CID) of the Internal Revenue Service (IRS), a bureau of the U.S. Department of Treasury. It is not available to the general public, but rather is provided to law enforcement agencies, government intelligence agencies, military agencies, and government, state, and other regulatory agencies with law enforcement missions (Maras, 2015).

c. *E-fense Helix and Live Response:* this tool offers cybersecurity and computer forensics software such as Helix3Pro and Live Response. E-fense Helix3Pro software can be used on multiple operating systems (Windows, Macintosh, and Linux). This tool is carefully designed to ensure that data is not altered during the imaging process. Local, state, and federal law enforcement agencies, along with private practitioners, have used this computer forensics tool. E-fense Live Response is a Universal Serial Bus (USB) key that is designed to be used by first responders, investigators, information technology professionals, and security professionals to collect nonvolatile and volatile data (which will be lost if the computer is shut down) from live running systems.

d. *Forensic Toolkit:* this product is sold by Access-Data. It is recognized around the world as the standard in computer forensics software. This court-accepted digital investigation platform is built for speed, analytics and enterprise-class scalability. Known for its intuitive interface, email analysis, customizable data views and stability, FTK lays the framework for seamless expansion, so your computer forensics solution can grow with your organization's needs (Clough, 2010). This software has many capabilities, including the ability to create images of hard drives, analyze the registry, scan slack space for file fragments, inspect emails, and identify steganography. Unlike other computer forensics tools on the market, FTK can crack passwords. This tool can also be used to decrypt files. Indeed, FTK was used to decrypt files seized from a safe haven of a Bolivian terrorist organization that had assassinated four U.S. Marines (Clough, 2010). Furthermore, this tool is quite beneficial because even if a computer crashes while using FTK software, the information will not be lost.

e. *Vogon Forensic Software*: this tool comprises a range of imaging, processing and investigation software tools designed for the professional computer forensic investigator. The software has been developed by Vogon over the past decade to offer very high performance, extensive investigation facilities and comprehensive auditing and anti-repudiation techniques.

f. *Forensic E-mail Analysis Software*: this is typically used to forensically examine the most popular e-mail formats such as America Online (AOL), Outlook Exchange (PST), Eudora, and many others. Paraben's E-mail Examiner is one of the most comprehensive forensically sound e-mail examination tools available. E-mail Examiner quickly recovers deleted messages and folders. E-mail Examiner doesn't just recover e-mail in the deleted folders; it also recovers e-mail deleted from deleted items (deleted/deleted).

g. *Live View developed by CERT, Software Engineering Institute*: this is a Java-based graphical forensics tool that creates a VMware virtual machine out of a raw (dd-style) disk image or physical disk. This allows the forensic examiner to «boot up» the image or disk and gain an interactive, user-level perspective of the environment, all without modifying the underlying image or disk. Because all changes made to the disk are written to a separate file, the examiner can instantly revert all of his or her changes back to the original pristine state of the disk. The end result is that one need not create extra [throw away] copies of the disk or image to create the virtual machine (Ghernaouti, 2013).

4.0. CONCLUSION

Forensic investigations tools are essential in computer forensics, and every potential electronic or digital piece of evidence requires a set of dedicated tools that will facilitate the easy generation of relevant evidence, devoid of damage, alteration, and manipulation. Students should understand that forensic evidence is important to cybercrime investigation. Hence, the choice of forensic tool is very important as the use wrong of tools can lead to a loss or damage of potential electronic evidence.

5.0 SUMMARY

In this unit, efforts have been devoted to the major computer forensic tools commonly deployed for generating electronic evidence on the field. Also, the major functionalities of forensics tools were also discussed.

6.0 TUTOR-MARKED ASSIGNMENT

1. With relevant examples, discuss the major functionalities of forensic tools
2. Identify and discuss three major forensic tools commonly deployed by computer forensics investigators

7.0 REFERENCES/FURTHER READING

Clough, J. (2010). *Principles of Cybercrime*. Cambridge University Press.

Ghernaouti, S. (2013). Cyber Power: Crime, Conflict and Security in Cyberspace. EPFL Press.

Maras, M. (2015). *Computer Forensics: Cybercriminals, Laws and Evidence (Second Edition)*. Jones & Bartlett Learning.

UNIT 4 MOBILE DEVICES IN COMPUTER FORENSIC INVESTIGATION

CONTENTS

1.0. Introduction
2.0. Objectives
3.0. Main Content
3.1 Mobile Devices in Computer Forensics Investigation
4.0. Conclusion
5.0. Summary
6.0. Tutor -Marked Assignment
7.0. Reference/Further Reading

1.0 INTRODUCTION

Mobile device forensics is the branch of forensics investigation relating to the recovery of electronic/digital evidence or data from a mobile device forensically. In every forensics investigation involving a mobile device(s), the forensic expert needs to first identify the type of the mobile device(s) i.e., PDAs smartphone, tablet, etc. to determine how to proceed with such investigation. Mobile devices forensics are important to forensic investigation because due mobile phones and PDAs have capacity to store and disseminate information.

2.0 OBJECTIVES

At the end of this Unit, you should be able to:

- know the importance of mobile devices in forensic investigations
- list the types of information that can be accessed from mobile devices
- describe the forensic tool kits suitable for mobile devices.

3.0 MAIN CONTENT

3.1 Mobile Devices in Computer Forensics Investigation

Mobile devices have over time played important roles in criminal investigations. These devices have been the targets of crimes, have been used to commit crimes, and have stored evidence of crimes. Mobile devices can be used to make phone calls and send and receive text messages. Many of these devices also have GPS navigation systems. In many ways, mobile devices behave can be used to store files, create and save images, browse the Internet, send emails, and record videos. Therefore, mobile devices hold a wealth of data that may be used as evidence in an investigation (Maras, 2015).

Mobile devices are important gadgets on which forensics investigations are frequently conducted to gather evidence of a crime or incident. Today's mobile devices have vast storage capacities which potential reservoirs of valuable information to an investigation (Maras, 2015). The type of information normally retrieved from PDAs and mobile phones for use in an investigation include, but are not limited to:

a. Personal information manager (PIM) information such as:

- a memo pad, personal notes, diary, and/or a journal
- a calendar, datebook, and/or events list that contain appointments and reminders
- a "to-do list," which records tasks that a user needs to accomplish
- the numbers dialed, the numbers from which calls were received, missed calls, and the dates and times of these calls
- contacts listed in the phone book: this data may include names, email addresses, home addresses, and phone numbers (work, home, and/or mobile).
- text messages (such as Short Message Service (SIM); Multimedia Messaging Services (MMS); Enhanced Multimedia Messages (EMS).

b. Email and Internet data: Information regarding e-mails sent and received can be stored and found in mobile phones and PDAs. Also, draft emails of suspects may also be found.

c. Information on websites accessed can be obtained from these sources as well.

d. Memory Card Data: these cards allow users "to store additional files beyond the device's built-in capacity and provide another avenue for sharing data between compatible devices. Some of the commonly sourced data on memory cards are photographs, audio recordings, and video clips. Given that the majority of PDAs and mobile phones have digital picture and video capabilities, images or recordings of a crime, evidence, victims, or accomplices can be stored on memory cards.

e. Computer Applications: such as programs used to view and create documents, spreadsheets, and presentations.

f. Subscriber identifiers: these identifiers are used to authenticate the user to the network and to verify the services tied to the account

g. The personal identification number (PIN) and financial information (e.g., credit and debit card numbers) of the mobile phone or PDA user can also be retrieved, including data from the user's voice mail account.

h. Location data can also be retrieved from mobile devices: mobile phones are capable of identifying a user's location to within a few meters, requiring only that the phone is switched on to identify this site. Additionally, the GPS functionality included in most mobile phones and PDAs enables the pinpointing of the location of the user to within a few feet. GPS navigation systems can record the user's home address, work address, and other areas to which the individual traveled. Moreover, Google offers mapping capabilities that allow the user of a mobile phone to pinpoint the locations of his or her friends. This capability could prove extremely useful in missing children cases, as long as the child's phone remains on long enough for law enforcement authorities to identify the location of the child (Maras, 2015).

Phone records may sometimes be employed to prove or disprove a suspect's testimony or alibi. Cell phones are constantly communicating with whichever signal tower is closest to them. Telecommunication providers do keep track of which phone numbers are communicating with every signal tower at any given time. Thus, this information can then be used to plot out the course and subsequent locations of a mobile device (Maras, 2015). Evidence of this type has been used in many criminal investigations. Some of the remarkable cases where mobile phone data have proven critical in resolving crime incidents are highlighted below as presented by Maras (2015):

a. The murder of Veronica Guerin.

Veronica Guerin was a well-known Irish journalist who reported on gangs and drug dealers in Dublin. In 1996, she was murdered in her car by individuals who drove up alongside her vehicle in a motorcycle and shot her multiple times. In this particular case, mobile phone call data proved critical in the criminal prosecutions of those responsible for Guerin's murder.

b. Omagh bombing

On August 15, 1998, the Real Irish Republican Army (Real IRA), a splinter terrorist group from the Provisional IRA, executed an attack in Omagh, Northern Ireland, that killed 29 individuals and injured 220. The information retrieved from mobile phone data led to the criminal prosecutions of the perpetrators of the Omagh bombing.

c. Soham murders

In 2002, two 10-year-old girls, Holly Wells and Jessica Chapman, were murdered in Soham, United Kingdom. Authorities were able to use mobile phone records to track the location of Jessica and Holly. The records indicated that right before Jessica's mobile phone was turned off on the night the pair was killed, she was close to the home of Ian Huntley, who was charged in the murders. Mobile phone records were also used to discredit the testimony of Huntley and his girlfriend, Maxine Carr. Huntley and Carr had stated that they were together, but mobile phone records revealed that Carr was actually miles away from Huntley on the night of the murders.

d. Murder of Avis Banks and her unborn child

Keyton Pittman was engaged to Avis Banks, who was pregnant with his child. However, Pittman was also having an affair with Carla Hughes, a fellow teacher at his school. In November 2006, Hughes went to Banks' home, where she stabbed and shot Banks and her unborn child. Her mobile phone records helped place Hughes at the crime scene during the murder. This, along with the other evidence, proved critical in her conviction for two counts of capital murder.

In some instances, mobile phones have been used to detonate explosives, as in the following cases:

a. Bali bombings

On October 12, 2002, a terrorist attack was executed in Bali by a militant Islamic group based in Southeast Asia, known as Jemaah Islamiyah. Two nightclubs were targeted in the Bali areas that were very popular with Australian tourists, Paddy's Pub and Sari Club. The two nightclubs were located opposite each other. The first bomb was detonated in Paddy's Pub by a suicide bomber wearing a vest filled with explosives. Nine people were killed by this bomb. Survivors of the bomb frantically exited Paddy's Pub, only to encounter a second bomb that had been placed in a vehicle parked in front of the Sari Club. This bomb was triggered by a mobile phone 15 seconds after the initial blast.

b. Madrid bombings

On March 11, 2004, bombs detonated on four commuter trains in Madrid, Spain, killing 191 people and injuring more than 1,800 individuals. The terrorists responsible for this attack detonated the bombs with mobile phones. This event represented the first coordinated terrorist attack conducted by Islamic extremists on European soil. These terrorists were inspired by al-Qaeda's cause, rather than explicitly directed by al-Qaeda personnel.

c. London bombings

On July 7, 2005, during morning rush hour in London, three suicide bombers (Shehzad Tanweer, Mohammad Sidique Khan, and Jermaine Lindsay) detonated bombs on their persons (within one minute of one another) on three separate subway trains heading in different directions. Approximately one hour later, another suicide bomber (Hasib Hussain) detonated his explosive device on a bus. It was believed that mobile phones were used to set off these bombs. Like the Madrid bombers, these terrorists were inspired by al-Qaeda's cause, but not directed by this group. This event was the first coordinated suicide bombing by Islamic extremists on European soil (Maras, 2015).

d. Bombing in a Saudi Arabian palace

On August 28, 2009, an al-Qaeda suicide bomber, Abdullah Asieri, detonated explosives hidden in his rectum in an attempt to kill the head of Saudi Arabia's counterterrorism operations, Prince Mohammed Bin Nayef. Asieri had passed through two airport security checkpoints and had spent more than 30 hours with Saudi Arabian secret service agents before reaching the Prince. Once in the Prince's company, Aiseri informed him that more senior members of al-Qaeda wanted to surrender and convinced the Prince to speak with them on his mobile phone. The bomb is believed to have been triggered by a text message that was sent to Asieri's phone.

When conducting a criminal investigation on a mobile device, the following are expected of a forensic scientist:

a. *The investigator must first locate and document all the relevant evidence to the case:* he or she must document the location, make, model, serial number, identifying marks (if any), and condition of the electronic device (on, off, standby) to be seized. In addition, if the device is on, the investigator must write down all the information projected on the display of the electronic device and its current battery charge in his or her notebook. The screen of the mobile device (if on) and other related evidence should also be photographed. Forensic protocol dictates that if mobile devices (mobile phones, smartphones, and PDAs) are discovered during an investigation, they must be left in the state that they were found. If the device is off, it should remain off. If the device is turned on, the data in it may be modified. If the device is found on, the device should remain on (Maras, 2015). These devices are powered by battery; they must be charged to ensure that they remain on. As such, an investigator should ensure that the "on" state is maintained by powering the devices with, for example, a battery pack. Although other electronic devices such as computers must be powered down before transport, PDAs, mobile phones, and smartphones should remain on if they were found in this state.

b. When collecting mobile phone, PDA, or smartphone evidence, investigators should look for memory and SIM cards. The suspect may have hidden such items. Given their small size, these cards may be easily overlooked by investigators. In addition to those items, the cradle and all synchronization and power cables associated with the mobile device should be seized, labeled, packaged, and transported back to the forensic laboratory (if available). All peripheral devices, cloning equipment, and instruction and informational manuals related to the electronic devices (if present) should also be seized.

c. All of the seized devices must be handled very carefully to avoid any destruction or tampering of the evidence. Investigators should take special care when examining a mobile phone for evidence. Care must also be taken to ensure that a forensic tool does not alter the data in the device. Highly specialized tools are required to recover data from PDAs and their memory cards. In addition, specialized tools are required for recovering data from mobile phones, smartphones, and SIM cards. The tools used depend on the operating system of the mobile device. The investigator must ensure that the forensic tool that is used is documented in his or her notebook. The evidence stored on the mobile device (PDAs, mobile phones, and smartphones) will depend on its make and model. All storage devices can have deleted files or fragments recovered using a forensic procedure. Recovery depends on the time a manufacturer allotted for the retention of this information on a specific device (Maras, 2015).

d. The analyst must ensure that the mobile device is properly connected to a forensic workstation (i.e., computer) before acquiring data from it. For example, to acquire data from a PDA, the investigator must make sure that the device is powered on, in the appropriate cradle, and properly connected to the computer via a USB or serial port. The most important thing for an investigator to remember is to make sure that no matter which device is involved (e.g., PDA, mobile phone, smartphone), he or she must create a bit-by-bit copy of the contents of the device. The investigator must then verify that this bit-by-bit image is an exact copy of the contents of the device.

e. The investigator must also make sure that no modifications are made to the original contents of the device because doing so may render the evidence inadmissible in court of law. For example, a device could be used to copy the SIM card while simultaneously preventing it from connecting to the mobile phone network. A search can then be performed securely (i.e., without threat of modification of the data) on the contents of the device and pertinent data to the investigation can be retrieved (if any). An investigator may also use software, such as Forensic SIM, to clone a mobile phone’s or smartphone’s SIM card. This cloned card can then be used to examine the contents of the device without worrying about the possibility of modifying any potential evidence. Criminals have been known to destroy mobile devices to prevent investigators from retrieving data stored on them by breaking, burning, and submerging the device in water. However, even in these instances, an investigator can retrieve the data stored by the suspect’s service provider (Maras, 2015).

Mobile Devices Forensic Tools

Typically, some specialized forensic tools are required for the successful investigations of mobile devices. However, the selection of forensics tool that is used on mobile devices to obtain evidence is largely dependent on the make and model of the device and its operating system. This is essentially due to the fact that these devices require different tools than those used on computer systems.

The NIST states that PDA forensics tools are chosen for use in an investigation based on their ability to successfully meet the following demands:

a. acquire the contents of the device
b. retrieve information associated with PIM applications (e.g., calendar, “to-do list”)
c. locate graphic, text, video, and audio files
d. identify websites visited and obtain emails exchanged
e. find and display fields acquired from the device
f. locate data in compressed, archived, and formatted files
g. recover deleted, misnamed, and hidden files
h. retrieve files from a removable memory card
i. acquire data after a hard reset is performed
j. obtain the user’s password to acquire the contents of the device in question.

The following are some of the forensics tools commonly deployed in mobile devices investigations:

a. Encase

Encase is one of the most popular forensics tools, but is incompatible with PDAs running Pocket PC (Maras, 2015). It is usually used to acquire data from PDAs with Palm operating systems (OS). This tool also facilitates investigations of Linux-based PDAs. With Encase, "a complete physical bit-stream image of Palm OS devices is created and this bit-stream image is checked with the already obtained existing CRC (Cyclical Redundancy Checksum) values (Maras, 2015). Encase images the device and provides a hash value for it. Accordingly, the evidence file that is created by this tool can be reviewed for potential evidence. A report of the analyses performed and the results of these analyses can also be provided using this tool. Furthermore, Encase has organizing and bookmarking capabilities; the latter may be used to highlight and store certain data for future reference.

b. Palm dd

The Palm dd (pdd) tool is used to acquire data from a Palm device with a Palm operating system that is running in console mode. This tool does not have report, bookmarking, and search capabilities. The files that are "created from pdd can be imported into a forensic tool, such as [Encase], to aid analysis; otherwise the default tool is a hex editor."45 Although this tool can image the memory of the device, it does not provide hash values for the data that are acquired; as such, a separate procedure must be used to ensure the integrity of the data collection process.46 As of January 2003, this forensics tool was no longer being updated, although Paraben has included a pdd engine in its PDA Seizure software (Maras, 2015).

c. PDA Seizure

The PDA Seizure tool can be used to extract data from PDAs running the Windows CE, Pocket PC, or Palm operating systems. This tool can image RAM and ROM and works in a Windows environment. Unlike the pdd, PDA Seizure can provide hash values for acquired information. This toolkit is oriented toward PDAs without mobile phone functions, as it does not include features such as the ability to acquire SIM data. An investigator can use this tool to evaluate the contents of the PDA and provide a report on the results of his or her analyses. PDA Seizure tool also has organizing and bookmarking capabilities (Maras, 2015).

4.0 CONCLUSION

This unit established that mobile devices do not only play important roles in the generation of electronic evidence needed for cybercrime investigation, but are also necessary for the prosecution of cybercriminals. Students should also note that mobile devices are important to cybercrime investigations because they are used to store and disseminate information. Students should also be aware of the technical and evidential challenges in mobile devices forensic examination.

5.0 SUMMARY

Effort was made in this unit to explain the significance of mobile devices in computer forensics investigations, the procedures and steps required for electronic evidence sourcing from mobile digital devices, as well as the major problems usually associated with forensic investigations of mobile devices.

6.0 TUTOR-MARKED ASSIGNMENT

1. Mobile devices are important reservoirs of electronic evidence. Discuss.
2. State the steps required of a forensic expert conducting criminal investigations on a mobile device.
3. Identify and explain the use of any three major forensic tools used in mobile device investigations.

7.0 REFERENCE/FURTHER READING

Maras, M. (2015). *Computer Forensics: Cybercriminals, Laws and Evidence (Second Edition)*. Jones & Bartlett Learning.

UNIT 5 CHALLENGES ASSOCIATED WITH COMPUTER FORENSIC INVESTIGATIONS

CONTENTS

1.0. Introduction
2.0. Objectives
3.0. Main Content
3.1 Challenges associated with Computer Forensic Investigations
4.0. Conclusion
5.0. Summary
6.0. Tutor- Marked Assignment
7.0. References/Further Reading

1.0. INTRODUCTION

During investigation of computer-based crimes, forensic experts usually encounter series of challenges with regard to the collection, retention and examination of potential electronic evidence. These challenges usually stem from the technical, administrative, and legal frameworks. The technical challenges often border on electronic evidences retrieval and documentation, while administrative/legal challenges usually concern procedural/jurisdictional/privacy issues. Also, resource challenges often mainly center on the volume of data, time needed to acquire and analyze forensic media data.

2.0 OBJECTIVES

At the end of this Unit, you should be able to:

- highlight and discuss the major challenges that are usually associated with computer forensics investigations.

3.0 MAIN CONTENT

3.1 Challenges associated with Computer Forensic Investigations

Generally, criminals are conscious of the illegality of their conducts and the possibility of being detected via the data contained on their digital devices. Thus, they always make extra effort to cover their criminality tracks. Criminals use different techniques with which to communicate undetected online. They may also seek to avoid detection by changing their IP or email addresses. In other cases, criminals may use proxy servers to hide or mask their IP addresses (Maras, 2015). If an individual uses a proxy server (i.e., a server that acts as an intermediary for client requests for resources from other servers when accessing a website), the user’s identity is not revealed because the proxy server provides its own identity when it retrieves the website for the user.

Criminals may also use anonymous remailers to communicate undetected. These services allow an individual to send an email without revealing the sender's identity to the receiver (Maras, 2015). Moreover, a criminal may intentionally bounce (or route) his or her communication through numerous intermediate computers all over the world before arriving to the target computer. Therefore, to find the criminal, the investigator will have to identify each router or bounce point through which the message traveled to eventually find the email's point of origin. This is likely to be a slow process, as investigators may have to retrieve data from each point pursuant to a subpoena, court order, or search warrant (depending on which location in the world the message bounced to) to trace the message back to the computer from which it originated.

Criminals may also attempt to evade detection by setting up a foreign POP3 or IMAP email account and then accessing this account by using certain webbased systems such mail2web.com. With this approach, the mail is stored in and accessed from a foreign account, so that the criminal never uses publicly available electronic communications services or public communications networks. Investigators may run into significant obstacles when attempting to obtain emails retained on foreign servers (Maras, 2015). Moreover, criminals may attempt to avoid detection by accessing the Internet from Internet cafés. Criminals have also been known to use library computers to commit crimes, believing that the anonymity afforded to them in these venues will shield them from detection by authorities. This, however, is not always the case.

Another challenge to the utilization of computer forensics investigation is that the availability of several tools online that allow terrorists and other criminals to hide their messages. For instance, spam mimic is a program that turns email messages into spam. This program is designed to encode the email to appear as spam. The spam is then decoded by the recipient to reveal the original message (Maras, 2015). Another technique that is usually used to avoid surveillance is blocking moves. In this case, individuals "physically block access to the communication or, if unable or unwilling to do that, to render it (or aspects of it such as the identity, appearance, or location of the communicator) unusable." Individuals may encrypt messages by transforming the plaintext message (or parts of it, such as any personal information of the sender) into a cipher text message. The cipher text message is gibberish; thus, if eavesdroppers get their hands on this cipher text, they will not be able to determine what the message means. The intended recipient of the message should have the decryption key— the means for transforming the cipher text back into the plaintext message (Maras, 2015).

Furthermore, criminals also do find different creative ways to inhibit law enforcement efforts by using privacy-enhancing technology. An example of such technology is Tor—an anonymous Internet communication system that, among other things, provides individuals (and organizations) with the ability to share information and communicate over public networks without compromising their privacy (Clough, 2010). Tor works by distributing a user's transaction over several places on the Internet, so no single point can link [a user] to [his or her] destination…. Instead of taking a direct route from source to destination, data packets on the Tor network take a random pathway through several relays that cover your tracks so no observer at any single point can tell where the data came from or where it [is] going. Nevertheless, criminals are not the only people who seek to use privacy enhancing technologies, such as Tor. Some individuals also do use these technologies to retain anonymity, wherein an individual seeks and finds freedom from identification and surveillance in public or while engaging in public activities (this can include Internet activities) (UNODC, 2013).

Additionally, digital evidence is even more difficult to obtain when it is scattered across systems located in different countries. In such cases, success depends entirely on the effectiveness of international cooperation between legal authorities and the speed with which action is taken (Maras, 2015). Effective use of such evidence to identify individuals depends on the speed with which requests are treated: if treatment is slow, identification is next to impossible. In most countries there is a significant mismatch between the skills of the criminals who commit high-technology crimes and the resources available to the law enforcement and justice authorities to prosecute them. The use of computer technologies by those authorities, whether at the national or international level, remains weak and varies greatly from one country to another. In most cases, the police and judicial authorities rely on the conventional investigation methods used for ordinary crime to identify cybercriminals and build up cases against them (UNODC, 2013).

4.0 CONCLUSION

It was clearly demonstrated in this unit that computer forensics investigators usually encounter series of challenges in the course of extracting electronic evidence. Despite the multiple challenges embedded in computer forensics investigations, professional experts working with them have the chance to generate important evidence by deploying appropriate technical tools and techniques.

5.0 SUMMARY

This unit has documented the major challenges which computer forensic investigators usually face in the process of collection, examination, retention, and analysis of potential electronic evidence. However, these challenges are avoidable if computer forensic investigators follow the earlier discussed standard phases in computer forensics investigations.

6.0 TUTOR-MARKED ASSIGNMENT

1. Computer forensic investigations are usually associated with multidimensional challenges. Discuss
2. With relevant examples, explain the steps that can be taken by forensic scientists to overcome the challenges that are associated with computer forensics investigations.

7.0 REFERENCES/FURTHER READING

Clough, J. (2010). *Principles of Cybercrime*. Cambridge University Press.

Maras, M. (2015). *Computer Forensics: Cybercriminals, Laws and Evidence (Second Edition)*. Jones & Bartlett Learning.

United Nations Office on Drugs and Crime (2013). Comprehensive Study on Cybercrime. UNODC, Vienna.

MODULE 7 CYBERCRIME AND CRIMINOLOGICAL THEORIES

Unit 1 Anomie-Strain Theory and Differential Association Theory
Unit 2 Social Learning Theory and Situational Crime Prevention Perspective
Unit 3 Routine Activity Theory and Lifestyle Exposure Theory
Unit 4 Space Transition Theory and Digital Drift Theory

UNIT 1 ANOMIE-STRAIN THEORY AND DIFFERENTIAL ASSOCIATION THEORY

CONTENTS

1.0. Introduction
2.0. Objectives
3.0. Main Content
3.1 Anomie-Strain Theory
4.0. Conclusion
5.0. Summary
6.0. Tutor -Marked Assignment
7.0. References/Further Reading

1.0 INTRODUCTION

The majority of traditional criminological theories were postulated to explain the factors underlying the occurrence of offline crimes, the victims of such crimes, as well as how such crimes can be prevented. Thus, the emergence of cybercrime has generated series of debates among criminologists as regards the applicability of traditional criminological theories on this relatively new form of crime. These initial debates were largely informed by both the novel nature of the Internet at that time and the increasingly ubiquitous presence of technology in daily life (Holt & Bossler, 2015). For instance, on the one hand, David Wall stated that the development of crimes like computer hacking and computer intrusion via malicious software, are totally dependent on the advent of computer technology and the Internet. Therefore, these offenses may constitute “new wine in new bottles,” meaning that both the offense and the space where they operate are unique (Wall, 1998). On the other hand, Peter Grabosky (2001) and scholars belonging to same school of thought countered Wall’s argument by focusing on the motivations of offenders. The suggested that the larger body of traditional criminological theories should have utility to account for cybercrimes. Regardless of these divergent views, attempts shall be made in this unit to demonstrate how some selected ‘old’ and ‘new’ criminological theories can be employed to provide explanation on the phenomenon of cybercrime, its characteristics, the factors motivating cybercriminals to engage in the act, as well as the reasons why victims of cybercrime fall prey to the antics of cybercriminals.

Crime is a product of society, and it is ingrained in shared human relationships. As such, cybercrime has become popular with an exponential increase in the number of cybercriminals due to the premium which contemporary society places on financial success and the limited opportunity available to achieve such institutionalised goal. This situation inadvertently ferments a condition which breeds different forms of criminality, which also includes cybercrime. Moreover, cybercrime behaviour is learnable, and can be transmitted in the process of interaction with other cybercriminals. Through this association, potential cybercriminals learn from established cybercriminals, the techniques for perpetrating certain cybercrime, the specific rationale, motives, and gains of committing such the crime. Today, cybercrimes are national, transnational, and international in nature and scope.

2.0 OBJECTIVES

At the end of this Unit, you should be able to:

- discuss the basic tenets of anomie-strain theory and differential association theory
- explain the problem of cybercrime in society.

3.0. Main Content

3.1 Anomie-Strain Theory

Robert K. Merton proposed Anomie-strain theory after reviewing Emile Durkheim’s theory of anomie. Durkheim had analysed the concept of anomie as a breakdown in the ability of society to regulate the natural appetites of individuals. Merton, in an article published in 1938, pointed out that many of the appetites of individuals are not necessarily “natural” but rather, are “culturally induced”. He argued that social structure could limit the ability of certain groups to satisfy these appetites. This would then mean that the social structure itself might exert a definite pressure on certain persons in the society to engage in non-conformist rather than conformist conduct (Vold and Bernard, 1986).

Merton’s theory is a theory of deviance; it does not focus on criminality. His conception of deviance is relatively large (Williams III and McShane, 1999). He opined that the culture of any society defines certain goals it deems “worth striving for”, and that there are many such goals in every society, and they vary from culture to culture. Cultures also specify the approved norms or institutionalised means all individuals are expected to follow in pursuing the culture goals. These means are based on values in the culture, and generally, they will rule out many of the technically most efficient methods of achieving the goal (Vold and Bernard, 1986).

Robert Merton noted that certain goals are too strongly emphasised throughout society (he uses the example of financial success), and society also emphasises certain means such as hard work, education, starting at the bottom and working one's way up to reach those goals. When these goals are too strongly stressed, as Merton said financial success was, in the United States of America, the stage is set for anomie. This is due to the fact that everyone does not have equal access to the achievement of the legitimate financial success, and as a result, these people may search for other, perhaps illegitimate, ways of succeeding. Due to social inequality, the approved means to reach the success goals are not readily available to certain groups in the society even though the goals are said to apply equally to all. Certain groups of people, the lower social class and minorities, for instance, may be at a disadvantage in gaining business positions that would allow them to pursue the goal of financial success (Williams III and McShane, 1999).

According to Merton, when this inequality exists because of the way society is structured, the social structure is anomic (Williams and McShane, 1999). The individuals caught in these anomic conditions (largely the lower classes) are then faced with the strain of being unable to reconcile their aspirations with their limited opportunities. He, however, presents five ways by which an individual can respond to this problem of anomie, depending on his attitude towards the cultural goals and the institutionalised means. These options are: conformity, innovation, ritualism, retreatism, and rebellion (Vold and Bernard, 1986).

To the extent that a society is stable, most persons in it will choose 'conformity', which entails acceptance of both the cultural goals and institutionalised means. These persons try to achieve wealth through the approved methods of middle-class values and will continue to do so whether or not they succeed. Most crimes that exist in society will probably take the form of 'innovation'. Persons who innovate retain their allegiance to the cultural goal of acquiring wealth (since this is so heavily emphasised), but they find that they cannot succeed at this through the institutionalised means. Therefore, they figure out new methods by which wealth can be acquired (i.e. pursing culture goals through unapproved means).

A third possible adaptation is ritualism, it involves rejecting the possibility of ever achieving wealth, but retaining allegiance to the norms of hard work and honesty. This is the adaptation of those persons who wish to "play it safe". They will not be disappointed by failure to achieve their goals, since they have abandoned them. At the same time, they will never find themselves in trouble since they abide by all the cultural norms. These persons have achieved a minimum level of success through the institutionalised means, but have no real hope of achieving anything more. The fear of losing even this minimum level locks them into their adaptation. The fourth adaptation, retreatism, involves a rejection of both goals and means. Retreatists are those individuals who opt not to be innovative, and, at the same time, need to resolve their inability to reach the important goals in life. Their solution is that they simply quit trying to get ahead. This pattern is best seen as dropping out of society and is exemplified by vagrants, alcoholics, and drug addicts (Williams III and McShane, 1999).

Merton’s typology of adaptations to anomie

	Culture goals	Institutionalised means
Conformity	+	+
Innovation	+	_
Ritualism	_	+
Retreatism	_	_
Rebellion	±	±

(+) signifies “acceptance,” (-) signifies “rejection”, and (+) signifies “rejection and substitution of new goals and standards”.

The final mode of adaptation, ‘rebellion,’ is of a different type from the others. It focuses on the substitution of new goals and means for the original ones. Merton’s conception suggests that rebellion “leads men outside the environing social structure to envisage and seek to bring into being, a new, that is to say, a greatly modified social structure. It presupposes alienation from reigning goals and standards” (Merton, 1968). The basic point is that this person ceases to function as a member of the existing society and begins to live within an alternate culture.

Therefore, from the perspective of anomie-strain theory, people who engage in cybercrime belong to the category of innovators. These groups of individuals take to cybercrime because they have accepted the culturally prescribed goal of wealth accumulation, but rejected the institutionalised means (engaging in hard work and legitimate business) of reaching the cultural goal. Hence, innovators respond to the existing anomic situation in society by taking to cyber criminality as a way of fulfilling societal prescribed cultural goal.

Differential Association Theory

Differential association theory was first propounded by Edwin Sutherland in 1939, but he later modified it in 1947. He created a general theory of criminal behaviour by insisting that behaviour is learned in a social environment. In fact, all behaviour is in what is learned, rather than how it is learned. By the “differential association”, Sutherland meant that “the contents of the patterns presented in association would be from individual to individual (Sutherland, 1939). Crime is viewed as a consequence of conflicting values; that is, the individual followed culturally approved behaviour that was disapproved by the larger society. Hence, systematic criminal behaviour is due to differential association in a situation in which cultural conflicts exist, and ultimately lead to the social disorganization in the situation.

The core assumption of the theory is that all human behaviors are learned within a social environment. It essentially submits that criminal behavior is learned in association with others via communication. Generally, the two basic things that people learn through association and communication are the techniques for committing criminal behavior and the definitions (values, motives, drives, rationalisations, attitudes) supporting such behavior (Vold & Bernard, 1985).

Also, Sutherland posits that the key factor determining people's propensity towards law violation is not the social or psychological conditions they experience, but the way they define those conditions. In essence, differential association theory argues that people tend to violate the law when "definitions favorable to law violation" outweighs "definitions" unfavorable to law violation". Specifically, the major tenets of differential association theory as contained in Sutherland's 1947 edition include:

(1) criminal behavior is learned;

(2) criminal behavior is learned in interaction with other persons in a process of communication;

(3) the principal part of the learning of criminal behavior occurs within intimate personal groups;

(4) when criminal behavior is learned, the learning includes (a) the techniques for committing a crime, which are sometimes very complicated, and sometimes very simple; (b) the specific direction of the motives, drives, rationalisations, and attitudes;

(5) the specific directions of the motives and drives is learned from definitions of the legal codes as favorable or unfavorable;

(6) a person becomes delinquent because of an excess of definitions favorable to violation of law. This is the principle of differential association;

(7) differential association may vary in frequency, duration, priority, and intensity;

(8) the process of learning criminal behavior by association with criminal and anti-criminal patterns involves all of the mechanisms that are involved in any other learning;

(9) while criminal behavior is an expression of general needs and values, it is not explained by those general rules and values, since non-criminal behavior is an expression of the same needs and values.

Generally, differential association theory says that criminal behaviour is learned in association with others by communicating with those of others. Two basic things are learned. The technique for committing criminal behaviour and the definitions (values, motives, drives, rationalizations, attitudes) supporting such behaviour. Criminal behaviour occurs according to Sutherland, when there is an excess of definitions, favouring conventional behaviour. Therefore, once certain definitions exist, an individual tends to be more susceptible to similar behavioural definitions will be opened to criminal definitions. Moreover, the individual will be less receptive to anti-criminal definition. Thus, differential association theory posits that an individual learnt criminal behaviour through his or her interaction with other people that are involved in crime.

Using the point of view of differential association theory to explain cybercrime, it can then be said that individuals engaging in cyber criminality take to the act because of their excess of interactions with already established cybercriminals from whom they learnt the techniques for committing cybercrime, and the specific direction of the motives, drives, rationalisations, and attitude favourable to the perpetration of cybercrime.

4.0 CONCLUSION

This unit carefully explicated the conditions and social structures that promote the emergence of cybercrime and subculture of cybercriminals. The social strains and social relationships that created the problem of cybercrime were also discussed.

5.0 SUMMARY

This detailed discussion of the anomie-strain theory and differential association theory has provided student with the explanation on how existing strains in society and human social relationships are promoting the phenomenon of cybercrime.

6.0 TUTOR-MARKED ASSIGNMENT

1. Critically explain the phenomenon of cybercrime from the viewpoint of anomie-strain theory
2. How valid are the propositions of differential association theory for understanding the emergence of the *yahoo yahoo* sub-culture in Nigeria?

7.0 REFERENCES/FURTHER READING

Grabosky, P.N. (2001). Virtual criminality: Old wine in new bottles? Social and Legal Studies, 10, 243–249.

Sutherland, E. 1947. Principles of Criminology (4th ed.). New York. Harper and Row.

Vold, G. & Bernard, T. 1986. *Theoretical criminology* (3rd Ed). Oxford University Press.

Wall, D.S. (1998). Catching cybercriminals: Policing the Internet. International Review of Law, Computers & Technology, 12, 201–218.

Williams III, F. & McShane, M. 1999. *Criminological theory.* Prentice Hall, Upper Saddle River, New Jersey.

UNIT 2 SOCIAL LEARNING THEORY AND SITUATIONAL CRIME PREVENTION PERSPECTIVE

CONTENTS

1.0. Introduction
2.0. Objectives
3.0. Main Content
3.1 Social Learning Theory
4.0. Conclusion
5.0. Summary
6.0. Tutor -Marked Assignment
7.0. References/Further Reading

1.0. INTRODUCTION

Social learning theory asserts that people learn from people around them. This happens in two ways – through differential association- people learn values and behaviors associated with crimes, and through differential reinforcement- people learn the rewards and punishments associated with a behaviour. On its own part, situational crime prevention perspective focuses on the settings for criminal acts rather than on the characteristics of offenders. According to the theory, offenders choose to commit a crime when there are available opportunities that are rewarding.

2.0 OBJECTIVES

At the end of this Unit, you should be able to:

- explain the propositions of social learning theory and situational crime prevention perspective
- show how it can aid our understanding of the occurrence of cybercrime in society.

3.0 MAIN CONTENT

3.1 Social Learning Theory

Social learning theory is among the primary theories generally applied by criminologists to a wide variety of criminal and deviant behaviors over the last 50 years. This theory was proposed in the 1960s as an expansion of Sutherland’s (1947) differential association theory which argued that criminal behavior was learned through interactions and communication with others, with the most important influences derived from time spent with intimate personal groups. Through social engagement with others, some individuals were exposed to beliefs and attitudes that supported rule-breaking behavior as well as techniques of offending. The more frequently an individual was exposed to definitions supporting the violation of law, defined as rationalizations and attitudes supporting criminality, relative to definitions that did not support law violation, the more likely that individual would engage in crime. Akers initially expanded this theory to include aspects of operant conditioning and reinforcements for behavior, though it has subsequently been reformulated into a processual theory of offending. Specifically, Akers's (1998) social learning theory argues that the learning process of any behavior, including crime, includes at least four principal components: (1) differential association; (2) definitions; (3) differential reinforcement; and (4) imitation. The process begins with differential associations with deviant others which expose individuals to models of offending as well as definitions supportive of criminal or deviant behavior and justifications that neutralize the possible negative consequences of deviance. Social learning theory argues that the more beliefs and attitudes an individual has that are supportive of deviant behavior, the more likely they will be to engage in those activities. Exposure to delinquent peers and definitions supporting criminality are critical sources of imitation for first-time offenders. Future offending behavior is dependent, however, on the ways that individuals experience reinforcements for their actions. The experience of reinforcements through economic gain, emotional fulfillment, or social acceptance as well as experiences with punishments is all critical in influencing whether behaviors persist or desist over time. Therefore, from the purview of social learning theory, cybercriminals take to the crime by imitating their significant others (family members or friends) who are positively reinforced and favorably disposed towards indulging in cybercrime.

Situational Crime Prevention Perspective

Situational crime prevention perspective seeks to develop crime and situation specific methods for limiting and eliminating criminal opportunities (Reyns, 2010). The theory posits that the probability of a criminal activity can be reduced by changing the features of a given social situation or of the surrounding environment (Cornish and Clarke, 2003; Cornish and Clarke, 1987). According to the theory, society plays a role in inadvertently creating crime through the manufacturing of "criminogenic goods", through leaky systems, and poor management/design of facilities (Clarke, 1992). Therefore, situational crime prevention involves measures directed at highly specific forms of crime that involve the management, design or manipulation of the immediate environment in a systematic and permanent way (Clarke, 1992). Generally, situational crime prevention perspective suggests five major crime prevention strategies that can further be broken into 25 techniques: (a) increasing the effort (this involves physically separating the offender from his/her target through target hardening, controlling access, screening exits, deflecting offenders and controlling tools); (b) increasing the risk (this suggests the manipulation of the environment in as permanent a way as possible to limit criminal opportunities by extending guardianship, assisting natural surveillance, reducing anonymity, utilising place managers and strengthening formal surveillance); (c) reducing rewards (this entails concealing targets, removing targets, identifying property, disrupting markets and denying benefits); (d) reducing provocation (this involves understanding and reducing the immediate triggers of criminal events by reducing frustrations and stress, avoiding disputes, reducing emotional arousal, neutralising peer pressure and discouraging imitation); and (e) removing excuses (this connotes setting rules, posting instructions, alerting conscience, assisting compliance, and controlling drugs and alcohol). Therefore, within this context, the occurrence of cybercrime may be attributed to the failure of society and law enforcement officials to practically manage and deal with some specific situational and contextual conditions the occurrence of this 'new' of crime.

4.0 CONCLUSION

This unit was designed to familiarize students with the major tenets of the social learning theory and situational crime prevention perspective. It also showed how these two criminological theories can be adopted to understand the phenomenon of cybercrime in society.

5.0 SUMMARY

In this unit, the propositions of social learning theory and situational crime prevention perspective were discussed and utilised to conceptualize the occurrence of cybercrime in society.

6.0 TUTOR-MARKED ASSIGNMENT

1. Justify the relevance of social learning theory to the understanding of cybercrime
2. Critically contextualise the phenomenon of cybercrime from the lens of situational crime prevention perspective.

7.0 REFERENCES/FURTHER READING

Akers, R.L. (1998). Social Learning and Social Structure: A General Theory of Crime and Deviance. Boston: Northeastern University Press.

Cornish, D.B., & Clarke, R.V. (1987). Understanding crime displacement: An application of rational choice theory. Criminology, 25, 933–948.

Cornish, D. B., & Clarke, R.V. (2003). Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention. Crime Prevention Studies, 16, 41–96.

Reyns, B. W. (2010) A situational crime prevention approach to cyberstalking victimization: Prevention tactics for Internet users and online place managers. Crime Prevention and Community Safety 12: 999-118.

Sutherland, E. 1947. Principles of Criminology (4th ed.). New York. Harper and Row.

UNIT 3 ROUTINE ACTIVITY THEORY AND LIFESTYLE EXPOSURE THEORY

CONTENTS

1.0. Introduction
2.0. Objectives
3.0. Main Content
3.1 Routine Activity Theory
4.0. Conclusion
5.0. Summary
6.0. Tutor -Marked Assignment
7.0. References/Further Reading

1.0. INTRODUCTION

Routine activity theory is among the most popular crime opportunity and victimization theories. According to the proponents of the theory, the combination of a motivated offender, a suitable target, and the absence of a capable guardian will make a crime to occur. On its part, lifestyle exposure theory posits that persons with certain demographic profiles are more prone to experience criminal victimization because their lifestyles expose them to risky situations that promote crime. Also, lifestyles increase people's exposure to would-be offenders without effective restraints that can prevent the occurrence of a crime.

2.0 OBJECTIVES

At the end of this Unit, you should be able to:

- discuss the major tenets of routine activity theory (RAT) and lifestyle exposure theory
- provide an understanding of the occurrence of cybercrime, online criminal activities of cybercriminals
- explain action or inaction of victims falling prey to the antics of cybercriminals.

3.0 MAIN CONTENT

3.1 Routine Activity Theory

Routine activity theory was postulated by Larry Cohen and Marcus Felson (1979). The theory opines that the risk of criminal victimisation varies dramatically among the circumstances and locations in which people place themselves and their property (Schmalleger and Volk, 2018). Its major proposition is that a criminal activity is organised around routine activities of a population, and that crime is likely to occur as a result of the interplay of these three principal elements- motivated offender, a suitable target and the absence of a capable guardian (when a motivated offender and suitable target come together in the absence of a capable guardian, criminal opportunity occurs).

Target suitability refers to qualities such as the value of a person or property, access to them, and resistance capability. Motivation of offender refers to both criminal inclinations and the ability to carry out those inclinations, while capable guardians may either be formal or informal third parties with a capacity for intervention (Cohen and Felson, 1979). According to routine activity theory, although there will always be a substantial number of motivated offenders, however, suitable targets (either vulnerable people or unattended valuables) and capable guardians (watchful friends and neighbours, the police, security personnel) vary with the place and over time.

Early cybercrime scholars recognized that routine activities theory had great potential to account for cybercrime victimization (Grabosky & Smith, 2001; Newman & Clarke, 2003). Each component of the theory logically connects to individuals, entities, or behaviors in online environments. Motivated offenders are plentiful online, and are fueled by various motives including economic gain (Hutchings & Holt, 2015), personal desires (Holt & Bossler, 2009) or sexual proclivities (Holt, Blevins, & Burkert, 2010; Jenkins, 2001). Suitable targets in cyberspace may be individuals, computers, data, or various other items depending on the type of crime being examined. Their suitability or attractiveness may vary based on the interests, motivations, and preferences of the offender. Various guardians are also present online, and can be conceptualized as physical (e.g. antivirus software and password protection), social (e.g. peers), and personal (e.g. computer skills).

Lifestyle Exposure Theory

Lifestyle exposure theory was originally proposed to account for differences in the risks of violent victimization across social groups, but it has been extended to include property crime, and it forms the basis for more elaborate theories of target-selection processes (Meier and Miethe, 1993). This theory posits that the patterned activities and lifestyles of individuals (both work and leisure) lead to differential victimization rates (Williams and McShane, 1999). Specifically, the demographic differences in the likelihood of victimization are attributed to differences in the personal lifestyles of victims. In essence, variations in lifestyles are important because they are related to the differential exposure to dangerous places, times, and other situations where there are high risks of victimization (Meier and Miethe, 1993). According to the theory, lifestyles are essentially influenced by three basic elements: (i) the social roles played by people in society based on the expectations of others (people conduct themselves in certain ways and construct lifestyles more or less conducive to victimization); (ii) the social structure (the higher one’s position, the lower the risk of victimization-largely because of the kind of activities in which one engages and the places one frequents); and (iii) rational component in which decisions are made about which behaviours are desirable (based on one’s social role and structural position, decisions can be made to restrict routine behaviours to relatively safe ones or to accept risk) (Williams and McShane, 1999). When lifestyle variations are taken into account, victimization experience and potential victimizations are relatively predictable. Therefore, for those whose social and structural background creates greater interaction with offenders and places conducive to crime, there is indeed a great risk of victimization (Williams and McShane, 1999). In this particular context, people's exposure to cybercrime victimization will be explained as being primarily influenced by the frequency of their presence on the cyberspace, type of activities they engage in on the cyberspace, the type of websites they usually visit, the potency of the precautions they normally take to protect themselves and their digital device when online, amongst others.

4.0 CONCLUSION

This unit essentially explains the circumstances and situations that usually expose people to the criminal antics of cybercriminals on the cyberspace through the perspectives of routine activity theory and lifestyle exposure theory.

5.0 SUMMARY

In this unit, students were introduced to the basic tenets of routine activity theory (RAT) and lifestyle exposure theory. The perpetrator-victim(s) interactions and contacts leading to victimization on the cyberspace was analysed from the perspectives of the two theories.

6.0 TUTOR-MARKED ASSIGNMENT

1. Using routine activity theory and lifestyle exposure theory, critically discuss the circumstances exposing people to the antics of cybercriminals on the cyberspace.

7.0 REFERENCES/FURTHER READING

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

Grabosky, P.N., & Smith, R. (2001). Telecommunication fraud in the digital age: The convergence of technologies. In D. Wall (Ed.), Crime and the Internet (pp. 29–43). New York: Routledge.

Holt, T.J., & Bossler, A.M. (2014). An assessment of the current state of cybercrime scholarship. Deviant Behavior, 35, 20–40.

Hutchings, A., & Holt, T.J. (2015). Crime script analysis and online black markets. British Journal of Criminology, 55, 596–614.

Jenkins, P. (2001). Beyond Tolerance: Child Pornography on the Internet. New York: New York University Press.

Meier, R. F. & Miethe, T. D. (1993). Understanding theories of criminal victimisation. Crime and Justice, 17: 459-499.

Newman, G., & Clarke, R. (2003). Superhighway Robbery: Preventing e-Commerce Crime. Cullompton: Willan.

Schmalleger, F. & Volk, R. (2018). *Canadian criminology today: Theories and applications (sixth edition)*. Pearson.

Williams III, F. and McShane, M. 1999. *Criminological theory*. Prentice Hall, Upper Saddle River, New Jersey.

UNIT 4 SPACE TRANSITION THEORY AND DIGITAL DRIFT THEORY

CONTENTS

1.0 Introduction
2.0 Objectives
3.0 Main Content
3.1 Space Transition Theory
4.0 Conclusion
5.0 Summary
6.0 Tutor -Marked Assignment
7.0 References/Further Reading

1.0. INTRODUCTION

The space transition theory argues that people behave differently when they move from one space to another. It posits that people who are not criminal in the physical space do find it easy to commit crime on the cyberspace due to convenience, anonymity, and reward it presents. In similar terms, the digital drift theory attempt to explain how technology provides an avenue for criminals to engage and disengage from criminal behavior online with the help of the Internet that help to shield criminals' actual identity. This theory leads to criminal motivational behaviours online that are different from physical or traditional crimes.

2.0 OBJECTIVES

At the end of this Unit, you should be able to:

- discuss the tenets of space transition theory and digital drift theory
- explain how these theories were used to explain the online activities of cybercriminals.

3.0 MAIN CONTENT

3.1 Space Transition Theory

Space transition is among the recently propounded criminological theories specifically developed to explicate the issue of cybercrime. This theory was postulated by Karuppannan Jaishankar in 2008. It operates on the basic argument that people behave differently while online than they otherwise would in physical space, leading to different behavioural patterns in online environments. Specifically, Jaishankar presents seven basic propositions to explain people's behavior both online and off-line:

1. individuals who repress their desire to engage in crime in the real world due to either status or position have a propensity to engage in crimes online
2. offenders may be more likely to engage in cybercrime because of the ability to utilize various identities, hide their location, and the lack of deterrence in online spaces
3. crime in online spaces is likely to move into physical space, and vice versa.
4. cybercriminals may have the opportunity to desist because of the temporary nature of the Internet and its spatio-temporal disconnect from the real world
5. the nature of technology allows strangers to come together in cyberspace in order to plan and commit offenses in the real world, and those who know one another in the real world may partner in order to engage in cybercrimes
6. closed societies may produce greater levels of cybercrime than open societies due to the repressive nature of government regimes
7. the disconnect between norms and values of a society in the real world and those of the Internet may lead some individuals to engage in cybercrime.

Digital Drift Theory

Digital drift theory was proposed in 2015 by Andrew Goldsmith and Russell Brewer. Using the tenets of drift, they present the concept of digital drift. Goldsmith and Brewer (2015) state that they do not intend to account for hacking and other forms of cybercrime, but rather for the ways that technology creates opportunities to engage and disengage from criminal communities on and offline. Access to and use of the Internet for personal communications exposes individuals to environments where they are disconnected from their actual identity. Anonymity frees individuals from a sense of responsibility, and may encourage or embolden individuals to act in ways they would otherwise not in the real world (Goldsmith & Brewer, 2015). The escapism provided by online games, chat, and other media also relaxes the need to conform to social norms and mores, which may encourage deviance. According to the theory, the asynchronous, faceless nature of online communications leads individuals to feel that behavioural norms are meaningless because they are disconnected from themselves and others. Therefore, the absence of moral or social controls leads individuals to feel that they can behave in whatever way they see fit, and appears to have some association with digital piracy and trolling behaviors. In this respect, Goldsmith and Brewer (2015) argue that the Internet facilitates the two conditions necessary for drift to occur: affinity (immediate rewards, awareness of others) and affiliation (means of hooking-up, deepening of deviant associations, skills, etc.). With respect to affinity, the content of the websites and other forms of CMC may surprise youth and expose them to criminal beliefs, behaviors, and justifications that can make criminality attractive. The same is true for social relationships cultivated on and off-line. For instance, increasing rates of viewing pornography and digital piracy among various age groups may present the notion that crime online is socially acceptable, and increase willingness to engage in other forms of online deviance as well. Regarding affiliation, the more time individuals spend online, the more likely they are to be exposed to criminogenic pathways that may entice individuals to engage in various behaviors. Time spent on social media sites may expose individuals to new people they do not know off-line, who may be engaged in various forms of deviance on or off-line. The ability to access new social networks may increase exposure to criminal others and facilitate entry into deviant peer groups. In turn, these relationships may provide individuals with knowledge to justify and neutralize any sense of wrongdoing in criminal activity, creating what Matza (1964) argued were sources of reassurance that crime will neither be detected nor resolved. Since online relationships may or may not spill over into the real world, individuals can slip in and out of wrongdoing depending on their attitudes and perceptions of offending.

4.0 CONCLUSION

This unit focused on two relatively new theories – space transition theory and digital drift theory specifically propounded to explain why people take to crime on the cyberspace. Digital drift theory explains why people behave differently when they move from physical space to cyberspace to commit crime due to convenience, anonymity, and reward, while digital drift theory explained how technology and internet power provides opportunity for criminals to engage and disengage from criminal behavior online.

5.0 SUMMARY

This unit exposed students to the propositions of space transition theory and digital drift theory on the factors motivating people to engage in criminal behaviour on the cyberspace even if they do not normally indulge in such a behaviour in the physical space.

6.0 TUTOR-MARKED ASSIGNMENT

1. Critically interrogate the relevance of the propositions of space transition theory and digital drift theory to the *yahoo yahoo* sub-culture in Nigeria.

7.0 REFERENCES/FURTHER READING

Goldsmith, A., & Brewer, R. (2015). Digital drift and the criminal interaction order. *Theoretical Criminology*, 19: 112–130.

Jaishankar, K. (2008). Space transition theory of cybercrimes. In F. Schmalleger & M. Pittaro (Eds.), Crimes of the Internet (pp. 283–301). Upper Saddle River, NJ: Prentice Hill.

Matza, D. (1969). Becoming Deviant. Englewood Cliffs: Prentice Hall.