COURSE GUIDE

CYB 203
CYBERCRIME, LAW, AND COUNTERMEASURES

Course Team NOUNL (Course Developer)
Engr. Dr. Isah Abdulkadir O. (Course Writer)- NOUN
Prof. Afolayan A. Obiniyi (Course Editor)- NOUN

NATIONAL OPEN UNIVERSITY OF NIGERIA

National Open University of Nigeria
Headquarters
University Village
Plot 91, Cadastral Zone
Nnamdi Azikiwe Expressway
Jabi, Abuja

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

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

Printed 2011, 2024

ISBN: 978-978-786-273-5

CONTENTS

INTRODUCTION

Welcome **to CYB 203: Title.** CYB Cybercrime, Law, and Countermeasures are a two-credit unit course with a minimum duration of one semester. It is a compulsory course for graduate students in BSc Cybersecurity at the National Open University of Nigeria. The course guides you through understanding cybercrime and its negative impact on cyberspace. It will also explain cyber law and some necessary countermeasures against cybercrime.

COURSE COMPETENCIES

- Develop detailed security awareness training programs fashioned for companies, organisations, and their employees.
- Demonstrate competence in knowledge of cybercrime methods and inclinations to efficiently execute strategies for defence and mitigation.
- Get information on reputable and ethical resources for learning about cybercrime prevention, legal frameworks, and best practices.

COURSE OBJECTIVES

- To equip you with techniques to analysis cybercrime activities
- To understand what is required to develop robust cybercrime-free systems
- To investigate cybercrime attacks that leads to legal prosecution.

WORKING THROUGH THIS COURSE

To successfully complete this course, read the study units, listen to the audios and videos, do all assessments, open the links and read, participate in discussion forums, read the recommended books and other materials provided, prepare your portfolios, and participate in the online facilitation.

Each study unit has an introduction, intended learning outcomes, the main content, and conclusion, summary and references/further readings. The introduction will tell you the expectations in the study unit. Read and note the intended learning outcomes (ILOs). The intended learning outcomes tell you what you should be able to do after each study unit. So, you can evaluate your learning at the end of each unit to ensure you have achieved the intended learning outcomes. To meet the intended learning outcomes, knowledge is presented in texts, videos and links arranged into modules and units. Click on the links as may be directed but where you are reading the text offline, you will have to copy and

paste the link address into a browser. You can download the audios and videos to view offline. You can also print or download the texts and save in your computer or external drive. The conclusion gives you the theme of the knowledge you are taking away from the unit. Unit summaries are presented in downloadable audios and videos.

There are two main forms of assessments: formative and summative. Formative assessments help you monitor your learning. They are presented as in-text questions, discussion forums, and Self-Assessment Exercises.

The summative assessments would be used by the university to evaluate your academic performance. This will be given as a computer-based test (CBT) which serves as a continuous assessment and final examination. A minimum of three computer-based tests will be given with only one final examination at the end of the semester. You are required to take all the computer-based tests and the final examination.

There are 13 study units in this course divided into four modules. The modules and units are presented as follows:

STUDY UNITS

Module 1 Cybercrime

Unit 1 General Introduction to Cybercrime
Unit 2 Types and Categories of Cybercrime
Unit 3 Threats and Types of Attacks and Defences
Unit 4 Cybercrime as a Threat to the National Critical Infrastructure

Module 2 Investigation Process of Cybercrime

Unit 1 Procedures for Cybercrime
Unit 2 Strategies of Cybercrime Perpetrators
Unit 3 Successful Use of Online Social Networks for Cybercrime Investigation
Unit 4 Cyber Terrorism

Module 3 Computer Cybercrime Investigations

Unit 1 Computer Network and Forensic Investigations
Unit 2 Digital Evidence Collection and Evaluation

Module 4 Cyber Law and Countermeasures

Unit 1 Introduction to Cyber Law
Unit 2 Cyber Law Applications
Unit 3 Cyber Law Framework in Nigeria
Unit 4 Challenges and Opportunities for Cyber Law and Countermeasure Enforcement in Nigeria

REFERENCES/FURTHER READINGS/WEB RESOURCES

(PDF) Cybercrime and Cybercriminals: A Comprehensive Study. Available from: https://www.researchgate.net/publication/304822458_Cybercrime_and_Cybercriminals_A_Comprehensive_Study [accessed Jul 19, 2024].

Adeyemi O. O. (2023). *Cybercrime, Digital Forensics, and Jurisdiction in Nigeria,* University Press of Nigeria Publication

Britz, M. (2013). Computer Forensics and Cyber Crime‖. Third Edition. Upper Saddle River: Pearson.

Chawki, M. et al. (2015). *Cybercrime, Digital Forensics and Jurisdiction*‖. New York: Springer International Publishing.

Chawki, M., Darwish, A., Khan, M. A., & Tyagi, S. (2015). *Cybercrime, Digital Forensics, and Jurisdiction*. Springer. https://doi.org/10.1007/978-3-319-15150-2

Gibson, D. (2011). CompTIA Security+: Get Certified get ahead‖. Charleston, S.C.

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2023). *Cybercrime and digital forensics: An introduction* (3rd ed.). Routledge.

ISACA (2013). Advanced Persistent Threats: How to Manage the Risk to Your Business‖ (pp 11-46). Rolling Meadows, Illinois.[10] International Telecommunication Union ITU (2014). Understanding cybercrime: phenomena challenges and legal response‖(pp. 12-42). Edited by Marco Gercke. Geneva, Switzerland. <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/CybercrimelegislationEV6.pdf>

Sibe, R. T., & Kaunert, C. (2024). *Cybercrime, Digital Forensic Readin ess, and Financial Crime Investigation in Nigeria*. Springer.

PRESENTATION SCHEDULE

The presentation schedule gives you the important dates for the completion of your computer-based tests, participation in forum discussions and participation at facilitation. Remember, you are to submit all your assignments at the appropriate time. You should guard against delays and plagiarisms in your work. Plagiarism is a criminal offence in academics and is highly penalized.

ASSESSMENT

There are two main forms of assessments in this course that will be scored. The Continuous Assessments and the final examination. The continuous assessment shall be in three-fold. There will be two Computer Based Assessment. The computer-based assessments will be given in accordance to university academic calendar. The timing must be strictly adhered to. The Computer Based Assessments shall be scored a maximum of 10% each, while your participation in discussion forums and your portfolio presentation shall be scored maximum of 10% if you meet 75% participation. Therefore, the maximum score for continuous assessment shall be 30% which shall form part of the final grade.

The final examination for CYB Cybercrime, Law and Countermeasures will be maximum of two hours and it takes 70 percent of the total course grade. The examination will consist of 70 multiple choice questions that reflect cognitive reasoning.

Note: You will earn 10% score if you meet a minimum of 75% participation in the course forum discussions and in your portfolios otherwise you will lose the 10% in your total score. You will be required to upload your portfolio using google Doc. What are you expected to do in your portfolio? Your portfolio should be note or jottings you made on each study unit and activities. This will include the time you spent on each unit or activity.

HOW TO GET THE MOST FROM THE COURSE

To get the most in this course, you need to have a personal laptop and internet facility. This will give you adequate opportunity to learn anywhere you are in the world. Use the Intended Learning Outcomes (ILOs) to guide your self-study in the course. At the end of every unit, examine yourself with the ILOs and see if you have achieved what you need to achieve.

Carefully work through each unit and make your notes. Join the online real time facilitation as scheduled. Where you missed the scheduled

online real time facilitation, go through the recorded facilitation session at your own free time. Each real time facilitation session will be video recorded and posted on the platform.

In addition to the real time facilitation, watch the video and audio recorded summary in each unit. The video/audio summaries are directed to salient part in each unit. You can assess the audio and videos by clicking on the links in the text or through the course page.

Work through all self-assessment exercises. Finally, obey the rules in the class.

FACILITATION

You will receive online facilitation. The facilitation is learner centred. The mode of facilitation shall be asynchronous and synchronous. For the asynchronous facilitation, your facilitator will:

- Present the theme for the week.
- Direct and summarise forum discussions.
- Coordinate activities in the platform.
- Score and grade activities when need be.
- Upload scores into the university recommended platform.
- Support you to learn. In this regard personal mails may be sent.
- Send you videos and audio lectures, and podcast

For the synchronous:

- There will be eight hours of online real time contact in the course. This will be through video conferencing in the Learning Management System. The eight hours shall be of one-hour contact for eight times.
- At the end of each one-hour video conferencing, the video will be uploaded for view at your pace.
- The facilitator will concentrate on main themes that are must-know in the course.
- The facilitator is to present the online real time video facilitation timetable at the beginning of the course.
- The facilitator will take you through the course guide in the first lecture at the start date of facilitation

Do not hesitate to contact your facilitator. Contact your facilitator if you:

- do not understand any part of the study units or the assignment.
- have difficulty with the self-assessment exercises
- have a question or problem with an assignment or with your tutor’s comments on an assignment.

Also, use the contact provided for technical support.

Read all the comments and notes of your facilitator, especially on your assignments. Participate in the forums and discussions. This allows you to socialize with others in the programme. You can raise any problem encountered during your study. To benefit from course facilitation, prepare a list of questions before the discussion session. You will learn a lot from participating actively in the discussions.

Finally, respond to the questionnaire. This will help the university to know your areas of challenges and how to improve them for reviewing the course materials and lectures.

COURSE BLUB

This course covers a general introduction to cybercrime, computer cybercrime investigations, cyber law and countermeasures, computer cybercrime investigations

ICE BREAKER

You are welcome to CYB 203: Cybercrime, Law, and Countermeasures, a two-unit course. Please upload your profile on your wall, including your picture, workplace address, GSM number, and other details. What are your expectations in this course? I am sure you are going to enjoy it. Please fasten your seat belt as you take off. Once again, you are welcome.

MAIN COURSE

CONTENTS

MODULE 1 OVERVIEW OF CYBERCRIME

Module Introduction

The advancement in digital and information technology presented us with the conveniences of information sharing and all other online activities. This convenience has, however, created new avenues and tools for committing traditional crimes and new forms of crimes. This module will introduce you to the cybercrime concept, general introduction, the definition of cybercrime, different types and categories of cybercrime, and types of threats, attacks, and defences. Detections of cybercrime threats to national critical infrastructures and countermeasures.

Unit 1 General Introduction to Cybercrime
Unit 2 Types and Categories of Cybercrime
Unit 3 Threats and Types of Attacks and Defences
Unit 4 Cybercrime as Threat to the National Critical Infrastructure

In each unit, I will explore a particular topic in detail and highlight self-assessment exercises at the end of the unit. Finally, I highlight resources for further reading at the end of each unit.

Unit 1 General Introduction to Cybercrime

Unit Structure

1.1 Introduction
1.2 Learning Outcomes
1.3 General Introduction to Cybercrime
  1.3.1 What is cybercrime?
  1.3.2 Definitions of cybercrime
1.4 History of cybercrime
  1.4.1 Cybercrime by Decades
  1.4.2 Cybercrime in Nigeria
  1.4.3 Causes of Cybercrime in Nigeria
  1.4.4 Motivation for cybercrime
1.5 Summary
1.6 References/Further Readings/Web Resources
1.7 Possible Answers to Self-Assessment Exercise(s)

1.1 Introduction

You will learn from this unit the definition, terminologies and concepts of cybercrime. After studying the unit, you will be equipped with skills to define cybercrime and identify cybercrime attacks. You will also have the required background knowledge for the analysis of cybercrime.

1.2 Learning Outcome

By the end of this unit, you will be able to:

- recognise how studying cybercrime can help you understand the threats in the digital world and equip you to protect yourself and others.

1.3 General Introduction to Cybercrime

1.3.1 What is cybercrime?

The "cyber" environment includes all forms of digital activities, regardless of whether they are conducted through networks and without borders. This extends the previous term "computer crime" to encompass crimes committed using the Internet, all digital crimes, and crimes involving telecommunications networks.

Cybercrime is any illegal activity that involves a computer, computer network, or digital device. This can encompass a wide range of activities, including:

Theft: Criminals can steal data, such as financial information or personal records. They can also steal digital assets, like cryptocurrency.
Fraud: Cybercriminals can trick people into giving them money or personal information. This can be done through phishing scams, where emails or websites are designed to look legitimate, or by creating fake online stores.

Extortion: In this type of cybercrime, criminals threaten to release sensitive information or damage a computer system unless a ransom is paid. This is often done through ransomware attacks, which encrypt a victim's files and demand payment to decrypt them.

Disruption: Cybercriminals may launch denial-of-service attacks, which flood a website or server with traffic to take it offline. They may also deface websites or tamper with data.

Cybercrime is a growing problem as more and more of our lives move online. It's important to be aware of the risks and take steps to protect yourself, such as using strong passwords, being careful about what information you share online, and keeping your software up to date.

Self-Assessment Exercise 1

1	What is cybercrime?

1.3.2 Definitions of Cybercrime

The term "cybercrime" was introduced after the latest evolution in the computer industry and networks

- Cybercrime can be defined as “The illegal usage of any communication device to commit or facilitate in committing any illegal act”.
- A cybercrime is explained as a type of crime that targets or uses a computer or a group of computers under one network for harm.

Cybercrimes are committed using computers and computer networks. They can be targeting individuals, business groups, or even governments.

1.4 History of cybercrime

The first cyber-attack took place in France in 1834, long before the Internet was invented. Attackers managed to steal financial market information by hacking into the French telegraph system. However, cybercrime didn't become a significant issue until the late 20th century. With the rise of the digital revolution, cybercriminals were quick to adopt new technologies and use their intelligence to come up with clever ways to steal data and money from individuals and organisations. Since then, cybercrime has grown rapidly, with attackers constantly evolving their tactics for malicious purposes.

Today, cybercrime has developed into a complex ecosystem, with leak sites, "as-a-service" models, and profitable attack methods like business email compromise (BEC). The global impact of cybercrime continues to increase, costing organisations more money each year. If there were a hall of fame for cybercrime, it would feature the names and faces of

infamous attacks and attackers who have caught the attention of law enforcement and the admiration of other hackers.

1.4.1 Cybercrime by Decades

1960s

In the 1960s, the history of cybercrime began with Allen Scherr launching a cyber-attack on MIT computer networks, stealing passwords from their database using punch cards.

1970s

In the 1970s, the first computer virus, known as the Creeper Virus, was created by Bob Thomas for research purposes at Bolt, Beranek, and Newman (BBN) Technologies. This virus was detected on the ARPANET in 1971, showing the potential for future viruses to cause significant damage to computer systems.

1980s

The 1980s saw the first appearance of ransomware with the Acquired Immunodeficiency Syndrome (AIDS)Trojan, also called PC Cyborg Trojan. Trojan. This ransomware was easy to remove and appeared on floppy disks distributed by cybercriminals at the World Health Organisation's AIDS conference.

1990s

In the 1990s, the Melissa Virus became known to the general public. This virus spread through Microsoft Word and Outlook, causing an estimated $80 million in damages and expanding beyond America Online (AOL).

2000

In the year 2000, the ILOVEYOU virus infected over 10 million endpoints worldwide, causing billions of dollars in damages. It pretends to be a love letter attachment but overwrites and destroys millions of users' files worldwide. The worm spread through spam emails and exploited a flaw in Windows.

2010

In 2010, Operation Aurora, a nation-state attack by Chinese military hackers, targeted over 20 technology companies, with Google publicly announcing the seizure of its intellectual property.

2020

By 2020, alleged Russian cyber-attacks on U.S. governmental institutions increased, with a major data breach involving the Solar

Winds programme compromising an estimated 18,000 private and government networks, exposing sensitive information like financial data, source code, and passwords. Looking ahead to 2023, the landscape of cybercrime continues to evolve.

2023

The breach of Metro-Goldwyn-Mayer (MGM) Resorts systems, which resulted in $100 million in lost bookings and an additional $10 million for breach cleanup, was caused by social engineering. MGM Resorts Systems Company's integrated technology and IT infrastructure assists processes such as hotel reservations, casino management, and guest services. The attack was carried out by the ransomware gang Scattered Spider.

1.4.2 Cybercrime in Nigeria

Cybercrime is a growing trend as the Internet becomes more prevalent in society, and its future is unpredictable. It is often difficult to trace these crimes. Cybercrime can be categorized into two types: crimes that directly affect computer networks and devices, such as malicious code and viruses, and crimes facilitated by computer networks or devices that target individuals, such as cyberstalking, fraud, identity theft, phishing scams, and information warfare.

In recent times, Nigerian society has increasingly relied on the Internet and other information technology tools to engage in personal communication and conduct business activities among other several benefits. While these developments allow for enormous gains in productivity, efficiency, and communication they also create loopholes that are becoming worrisome and posing a serious threat to Nigeria as a nation.

Automation and AI lead to a rise in attempted cyberattacks as cybercriminals use them more commonly.

Self-Assessment Exercise 2

1	What are the major causes of cybercrime rise in Nigeria?

1.4.3 Causes of Cybercrime in Nigeria

Here are some of the reasons behind cybercrime:

1. Unemployment is a major factor contributing to cybercrime in Nigeria. With over 20 million graduates in the country unable to find jobs, many turn to criminal activities to survive.

2. The desire for wealth is another driving force behind cybercrime in Nigeria. Many young people are impatient and want to quickly attain wealth, leading them to engage in cybercrimes to keep up with their wealthy peers.

3. The lack of strong cybercrime laws in Nigeria also plays a major role in encouraging criminals, as they feel they can get away with their actions. The government must establish and enforce strict laws to ensure that criminals face consequences for their actions.

4. Inadequate security measures on personal computers also contribute to cybercrime. Computers without proper security controls are vulnerable to criminal activities, making it easier for information to be stolen.

1.4.4 Motivation for cybercrime

Political or Ideological Beliefs: Some cybercriminals are motivated by political or ideological reasons. They may target government agencies, corporations, or individuals who they believe go against their beliefs. These cyberattacks can be aimed at disrupting operations, stealing sensitive information, or spreading propaganda.

Revenge: In some cases, cybercriminals seek revenge against a person, organisation, or entity that they feel has wronged them. This could be a former employer, a romantic partner, or even a competitor in business. They may use cyberattacks to cause harm or damage to the target as a form of retaliation.

Thrill-Seeking: For some individuals, the excitement and challenge of hacking into systems and networks is what drives them to engage in cybercrime. These thrill-seekers may not have any specific motive other than the adrenaline rush they get from successfully carrying out illegal activities online.

State-Sponsored Attacks: Governments and nation-states may also engage in cybercrime for political, economic, or military purposes.
One key aspect of understanding the motivations of cybercriminals is recognising that they often operate in a complex ecosystem where various factors can contribute to their decision-making. For example, financial gain may be a primary motivator for some individuals, while others may be driven by a desire for power or recognition within online communities.

Additionally, the anonymity and perceived low risk associated with cybercrime can make it an attractive option for those seeking to exploit

vulnerabilities in digital systems. This lack of accountability can embolden individuals to engage in illegal activities without fear of consequences.

By addressing the underlying reasons why individuals turn to cybercrime, such as lack of opportunity or peer pressure, we can work towards creating a more secure and resilient digital environment. This includes investing in education and training programmes that provide alternative pathways for at-risk individuals, as well as implementing stronger cybersecurity measures to deter potential offenders.

Ultimately, by understanding the motivations behind cybercriminal behaviour, we can better equip ourselves to prevent and respond to threats in a proactive and effective manner

Discussion

1. After reading unit 1 from module 1 of this course material, can you explain with understanding the origin and trend of cybercrime globally and in Nigeria? Cybercrime can pose a serious threat to individuals, organisations and government establishments. Start your response by defining cybercrime with some examples and then support your view with skill and theories from your experience.

2. Discuss the most significant challenges law enforcement faces in combating cybercrime and explain how the rapid evolution of technology impacts the effectiveness of legal frameworks and countermeasures.

1.5 Summary

By the end of this unit, you will have learned about the definition and origins of cybercrime, as well as the challenges it presents in the world of ICT. You will also understand how cybercrime can pose serious security risks to computers and networks. In the next unit, you will be introduced to the various types and categories of cybercrime.

You have learned from this unit that cybercrime is a widespread and constantly changing threat that presents significant challenges to people, businesses, and governments around the world. The fast-paced development of technology has opened up new possibilities for legal and illegal activities, making it harder to outsmart cybercriminals.

1.6 References/Further Readings/Web Resources

Adeyemi, O. O. (2023), Cybercrime in Nigeria: A Comprehensive Guide, University Press of Nigeria Publication.

Kaur, M., Kaur, G., & Raina, C. K. (2017). Cyber-crime and its preventive measures. Int J Adv Res CCE, 6(3), 920-925.

Nwafor, I. (2022). *Cybercrime and the law: Issues and developments in Nigeria.* CLDS Publishing.

Schultz, C. B. (2016). Cybercrime: an analysis of the current legislation in South Africa (Master's thesis, University of Pretoria (South Africa).

Shah, M. H., Jones, P., & Choudrie, J. (2019). Cybercrimes prevention: promising organisational practices. Information Technology & People, 32(5), 1125-1129.

1.7 Possible Answer to Self-Assessment Exercise(s)

1. What is cybercrime?

Answer:
Cybercrime refers to any criminal activity involving a computer or computer network, such as data theft or denial-of-service attacks.

2. When did cybercrime begin?

Answer:
The origins of cybercrime can be traced back to the 19th century when telegraph messages were manipulated, even though the term itself is more modern.

3. Why is cybercrime such a big problem?

Answer:
Cybercrime is a significant issue due to the potential for financial loss, identity theft, and damage to critical infrastructure. It is also challenging to combat because it is constantly evolving.

4. What are the major challenges of fighting cybercrime?

Answer:
One major challenge in fighting cybercrime is its international nature, as cybercriminals can operate from anywhere in the world, making it difficult to track and prosecute them.

5. What was the first major cybercrime incident?

Answer:
There is a debate about the first major cybercrime incident. One strong contender is the Morris Worm incident in 1988, which infected a large portion of early Internet-connected machines and caused widespread disruption.

6. How did cybercrime evolve with the Internet?

Answer:
The rise of the Internet in the 1990s created a vast new landscape for cybercrime. Hackers exploited vulnerabilities in early web technologies and software, leading to data breaches, malware attacks, and online scams.

7. *How has cybercrime become more sophisticated*?

Answer:
Cybercriminals have become more organised and now use advanced techniques. They target critical infrastructure, develop complex malware, and employ social engineering tactics to trick victims.

8. What are some of the biggest cybercrime threats today?

Answer:
Today's cybercrime landscape is vast. Major threats include ransomware attacks that extort money, large-scale data breaches, and supply chain attacks that compromise trusted systems.

Unit 2 Types and Categories of Cybercrime

Unit Structure

2.1 Introduction

You will learn from this unit the different types of cybercrimes. After studying the unit, you will be equipped with the skills to recognise the different types of cybercrimes.

2.2 Learning Outcome

By the end of this unit, you will be able to:

- identify the different types of cybercrimes.

2.3 Categorizing Cybercrime

When it comes to cybercrime, there are a variety of different types that can be categorized based on the nature of the offense. Some common categories include hacking, phishing, identity theft, malware, and denial of service attacks.

Hacking involves illegally accessing computer systems or networks with malicious intent.

Phishing is a deceptive practice where cybercriminals attempt to steal personal information by posing as legitimate entities.

Identity theft is when someone's personal information is stolen for fraudulent purposes.

Malware refers to malicious software designed to disrupt or damage computer systems.

Lastly, denial of service attacks involves overwhelming a network or server with traffic to make it inaccessible to users. Understanding these different categories can help individuals and organisations better protect themselves from falling victim to cybercriminal activities. Cybercrime categorization is shown in figure 3.1.

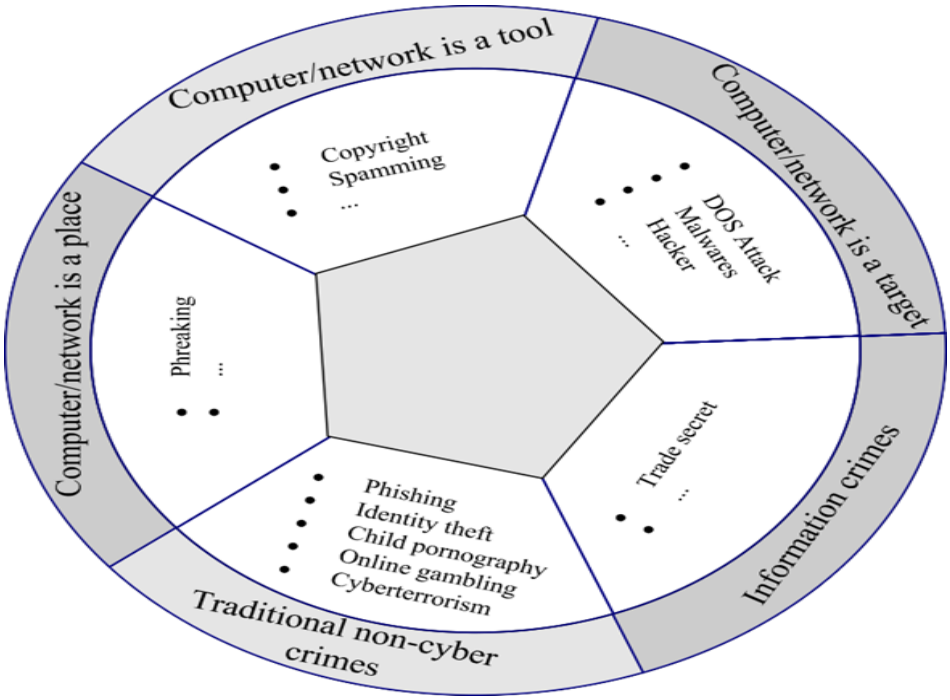


Fig. 3.1: Categorizing cybercrime (Zhang et al, 2012).

Self-Assessment Exercise 1

1.	How is Cybercrime Categorised?

2.3.1 Main Categories of Cybercrime

There are three main categories of cybercrime - property, individual, and government.
The methods used and difficulty levels vary depending on the category.

Property cybercrime: is like someone illegally obtaining a person's bank or credit card information to access funds or run scams. Hackers may use malicious software to access confidential information on websites. Individual cybercrime: involves one person distributing harmful or illegal information online, such as cyberstalking or trafficking.

Government cybercrime: is the most serious offense, including activities like hacking government websites or spreading propaganda. These criminals are often enemies or terrorists of other nations.

2.3.2 Types of Cybercrimes

Cybercrime is a broad term encompassing a wide range of illegal activities conducted through digital means. Here are some of the most common types:

- **Denial of Service Attack (DoS)**

This is an act by the criminal, who floods the bandwidth of the victim network or fills his e-mail box with spam mail depriving him of the services he is entitled to access or provide short for denial-of-service attack, a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic. Many DoS attacks, such as the Ping of Death and Teardrop attacks, exploit limitations in the TCP/IP protocols. For all known DoS attacks, there are software fixes that system administrators can install to limit the damage caused by the attacks. But, like Virus, new DoS attacks are constantly being dreamed up by Hacker.

- **Virus Dissemination**

Malicious software that attaches itself to other software. Viruses, worms, Trojan Horse, Time bomb, Logic Bomb, Rabbit and Bacterium are the malicious codes.

- **Software Piracy**

Theft of software through the illegal copying of genuine programmes or the counterfeiting and distribution of products intended to pass for the original.

- **Net Extortion**

This is the process of seizing, getting, or copying data of high value or secrecy in order to threaten its damage, exposure, or reputation tarnishing for a huge sum of money.

- **Phishing**

The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organisation already has. The Web site, however, is bogus and set up only to steal the user's information. Phishing is also referred to as brand spoofing or carding.

- **Cyber trespassing**

This type of crime includes following a victim online. Cyber Criminals send a programme to the victim's machine, which after getting downloaded in stealth or hidden capture all the information from the victim's machine and send it to the criminal. The information collected by the cybercriminal is then used against the victim for harassing, black mailing etc.

- **Cyber Contraband**

Selling of illegal items by use of computer system, preferably having internet connectivity.

- **Cyber terrorism**

Terrorist use technology to spread terrorism across the world. Some websites provide unwarranted information about making ammunitions, hacking techniques, spreading arms and ammunitions by using secret codes.

- **Cyber laundering**

Cyber criminals lure the victim by sending email's assuring them that they have won a lottery and asking the victim to pay token amount to get the lottery amount. They ask personal information from the victim such as Name, Age, Address, Bank Account, Occupation etc. This information collected is then used against the victim for committing the

crime. The lottery amount is never received by the victim, nor is the token amount returned back.

- **Cyber Theft**

This type of crime involves stealing Internet time.

- **Cyber Pornography**

This is one of the most prominent crimes taking place on the Internet. Cyber criminals make websites which promote nudity on the Internet. There are many websites on the Internet which promote this heinous crime. Another way by which criminals promote pornography on the Internet is by cutting and pasting two or more photographs from pornographic sites and merging with the photograph of the victim. This is called as morphing. Special care has to be taken by individuals, groups while putting photographs on the websites. Whenever photographs are put on the Internet features such as cut, copy, paste and print screen should be disabled.

- **Email Bombing**

This kind of activity refers to sending large numbers of mail to the victim, which may be an individual or a company or even mail servers there by ultimately resulting into crashing.

- **Data Diddling**

This kind of an attack involves altering raw data just before a computer processes it and then changing it back after the processing is completed. The electricity board faced similar problem of data diddling while the department was being computerized.

- **Salami Attacks**

This kind of crime is normally prevalent in the financial institutions or for the purpose of committing financial crimes. An important feature of this type of offence is that the alteration is so small that it would normally go unnoticed. E.g. the Ziegler case wherein a logic bomb was introduced in the bank's system, which deducted 10 cents from every account and deposited it in a particular account.

- **Denial of Service Attack**

The computer of the victim is flooded with more requests than it can handle which cause it to crash. A Distributed Denial of Service (DDoS) attack is also a type of denial of service attack, in which the offenders are wide in number and widespread. E.g. Amazon, Yahoo.

- **Logic Bombs**

These are event dependent programmes. This implies that these programmes are created to do something only when a certain event (known as a trigger event) occurs. E.g. even some viruses may be termed logic bombs because they lie dormant all through the year and become active only on a particular date (like the Chernobyl virus).

- **Trojan Attacks**

This term has its origin in the word 'Trojan horse'. In software field this means an unauthorised programmeme, which passively gains control over another's system by representing itself as an authorised programmeme. The most common form of installing a Trojan is through e-mail.

- **Web Jacking**

This term is derived from the term hijacking. In these kinds of offences, the hacker gains access and control over the web site of another. Hacker is someone gains unauthorised access to computer system or confidential information. Web jacker may even mutilate or change the information on the site. This may be done for fulfilling political objectives or for money. Of recent many sites were web jacked. Out of uncounted number was the site of Bombay crime branch which was also web jacked. Another case of web jacking is that of the 'gold fish' case. In this case the site was hacked and the information pertaining to gold fish was changed. Further a ransom of US $ 1 million was demanded. Thus, web jacking is a process whereby control over the site of another is made backed by some consideration for it.

2.4 System Target/Focused Cybercrime

System target/focused cybercrime refers to a category of cyber-attacks where the primary objective is to compromise or exploit specific systems or networks for malicious purposes. Unlike indiscriminate attacks that target a wide range of victims, these attacks are highly targeted and often involve extensive reconnaissance and planning.

2.4.1 Viruses

This type of malicious code requires you to actually do something before it infects your computer. This action could be opening an email attachment or going to a particular web page.

2.4.2 Worms

Worms propagate without user intervention. They typically start by exploiting a software vulnerability (a flaw that allows the software's intended security policy to be violated), then once the victim computer has been infected the worm will attempt to find and infect other computers. Like viruses, worms can propagate via email, web sites, or network-based software. The automated self-propagation of worms distinguishes them from viruses.

2.4.3 Trojan Horses

A Trojan horse programme is software that claims to be one thing while in fact doing something different behind the scenes. For example, a programme that claims it will speed up your computer may be sending confidential information to a remote intruder.

2.4.4 Physical Destroying the System in other to Destroy Evidence

Even in the traditional law today, for a criminal court to set upon any lawsuit there must be genuine evidence or witnesses

Self-Assessment Exercise 2

1. Give one example of cybercrime you know.

 **Discussion**

After reading this unit, think about how you could differentiate between common cybercrimes. Create a group with a minimum of three members and provide a response based on your knowledge and experience of cybercrime fundamentals that you have learnt so far.

2.5 Summary

At the end of this unit, you have learnt the different types of malwares that are used for cybercrime. In the next unit, you will be introduced to the different ways in which a malware can be detected in a computer or over a network.

You have learnt from this unit that cybercrime can be categorized into three main headings which are: property, individual, and government. Therefore, it is important that you can categorize cybercrime and recognise the types that fall under a particular heading.

2.5 References/Further Readings/Web Resources

Adeyemi, O. O. (2023). *Cybercrime in Nigeria: A Comprehensive Guide*. University Press of Nigeria.

Cascavilla, G., Tamburri, D. A., & Van Den Heuvel, W. J. (2021). Cybercrime threat intelligence: A systematic multi-vocal literature review. Computers & Security, 105, 102258.

Ejemeyovwi, J. O., & Okolie-Osemene, J. (2023). *Cybercrime and Data Protection in Nigeria: Legal Implications and Safeguarding Measures*. University of Benin Press.

Saunders, J. (2017). Tackling cybercrime–the UK response. Journal of cyber policy, 2(1), 4-15.

Sibe, R. T., & Kaunert, C. (2024). Cybercrime, Digital Forensic Readine ss, and Financial Crime Investigation in Nigeria. Springer.

Watson, K., & Payne, T. (2023). The human side of cybercrime. Cyber Security: A Peer-Reviewed Journal, 6(4), 356-365.

2.7 Possible Answers to Self-Assessment Exercise(s)

Answers to Self-Assessment

1. Define Cybercrime

Answer:
Cybercrime is any criminal activity that involves computers and networks. This includes everything from stealing personal information to causing damage to computer systems.

2. What are the three main categories of cybercrime?

Answer:
Property, Individual, and Government

3. What are some types of cybercrime?

Answer:
Some types of cybercrime include:

i. Denial-of-service (DoS) attacks: These attacks overload a computer system or network, making it inaccessible to legitimate users.
ii. Data breaches: This occurs when sensitive information is stolen from a computer system.
iii. Online fraud: This includes scams like fake online stores or lottery scams.
iv. Copyright infringement: This involves illegally copying or distributing copyrighted material.

4. How can I protect myself from cybercrime?

There are several things you can do to protect yourself from cybercrime.

- Be cautious of suspicious emails and links.
- Use strong, unique passwords for your online accounts.
- Keep your software and operating system up-to-date.
- Use antivirus and anti-malware software.
- Back up your important files regularly.

5. *Give one example of cybercrime you know.*

One example of cybercrime is Phishing: Phishing is a common type of cybercrime. This involves sending fraudulent emails or messages that appear to come from legitimate sources, like banks or social media platforms, to trick people into revealing personal information such as passwords, credit card numbers, or social security numbers.

Unit 3 Threats and Types of Attacks and Defences

Unit Structure

3.1 Introduction

You will learn from this unit, threats and attack types and how to defend them. After studying this unit, you will be able to use some defence strategies to tackle cybercrimes.

3.2 Learning Outcome

By the end of this unit, you will be able to:

- defend against various types of cyberattacks.

3.3 Threats and Types of Attacks and Defences

Cybercrime threats are a serious issue in today's digital age, with hackers constantly finding new ways to infiltrate systems and steal sensitive information. There are common types of cyber threats targeting individuals, organisations, and government establishments like phishing scams, ransomware attacks, and DDoS (Distributed Denial of Service) attacks.

To defend against these threats, individuals and organisations can employ tactics such as using strong passwords, keeping software

updated, installing antivirus programmes, and educating themselves about potential risks online. Vigilance and caution are key in guarding against cybercrime in today's interconnected world.

3.3.1 Cyber Threats

In simple terms, a cybersecurity threat, also known as a cyber threat, is a sign that a hacker or malicious actor is trying to access a network without permission to launch a cyberattack.

Cyber threats can vary from obvious scams like email promising money in exchange for bank details, to sneaky malicious code that bypasses defenses and remains undetected on a network for a long time before causing a costly data breach. The more knowledge security teams and employees have about different types of cybersecurity threats, the better they can prevent, prepare for, and respond to cyberattacks.
Figure 3.1 *shows various top cyber threats.*

Fig. 3.1: Top cyber threats. (Prajwal, 2023)

3.3.2 Cyber Attacks

Cyber threats are constantly evolving, with tactics and attack methods improving daily. Cyber criminals gain access to computers or network servers through various paths in order to cause harm, a process known as an attack vector.

- **How Cybercriminals Gain Access to a Computer**

i. Web or email attacks can pose a threat to your organisation.
ii. Be cautious of removable media like flash drives.
iii. Unauthorised use of your organisation's system privileges should be avoided
iv. Keeps an eye out for loss or theft of devices containing confidential information.
v. Watch out for brute force attacks that attempt to decode encrypted data through trial and error.
vi. Remember to be cautious of removable media like flash drives.

Self-Assessment Exercise 2

1.	List three examples of cyber threats.

3.3.3 Cyber Defences

Cyber threats are a serious issue for individuals, organisations, and government establishments. These threats are complex, destructive, and increasing in frequency.

Cyberspace is constantly under attack, with malicious events happening daily, ranging from simple to highly advanced attacks.

Self-Assessment Exercise 2

1.	What is the concern of cyber security experts in cyber defence?

3.4 Cyber Defence in Depth

Cyber defence in depth is a strategy that uses multiple security measures to safeguard an organisation's assets. The idea is that if one defense is breached, there are additional layers in place to stop threats. This approach tackles security weaknesses in hardware, software, and people, as human error is a common cause of security breaches

3.4.1 Elements of Defense-in-Depth

In the past, most businesses relied on defense-in-depth strategies that were based on traditional perimeter security models to protect their on-premises IT infrastructure. A typical defense-in-depth security setup includes the following components:

- Endpoint security solutions: such as antivirus software and endpoint detection and response (EDR) tools to defend against threats from PCs, Macs, servers, and mobile devices. Additionally, endpoint privilege management solutions are used to control access to privileged endpoint accounts.

- Patch management tools: these are used to ensure that endpoint operating systems and applications are kept up to date and to address common vulnerabilities and exposures (CVEs).

- Network security solutions: including firewalls, VPNs, VLANs, etc., are used to protect traditional enterprise networks and on-premises IT systems.

- Intrusion detection/prevention (IDS/IPS) tools: these are used to detect malicious activity and prevent attacks on traditional on-premises IT infrastructure. - User identity and access management solutions: these include single sign-on, multi-factor authentication, and lifecycle management tools for authenticating and authorising users.

3.4.2 Strategies of Defence-in-Depth in the Digital Era

Traditional IT security models based on perimeter control, designed to regulate access to trusted enterprise networks, are not effective in the digital age. Nowadays, businesses create and implement applications in various locations such as corporate data centers, private clouds, public clouds (AWS, Azure, GCP), and SaaS solutions (Microsoft 365, Google Workspace, Box). Most businesses are updating their defense strategies to safeguard cloud workloads and combat new attack methods that come with digital transformation.

Regardless of whether applications are on-premises or in the cloud, history has shown that skilled attackers can infiltrate networks and remain undetected for extended periods. For instance, the SolarWinds supply chain attack in 2020 went unnoticed for nine months, impacting more than 18,000 organisations. As a response, many enterprises are embracing a Zero Trust approach, assuming breaches can happen, and adjusting their security tactics. They are using a mix of preventive measures and detection tools to pinpoint attackers and prevent them from achieving their objectives if they manage to breach a network.

3.4.3 Principle of Modern Defence-in-Depth Strategies

Protect privileged access: This is by using privileged access management solutions to monitor and secure access to privileged

accounts, such as super user accounts, local and domain administrator accounts, and application administrative accounts, by both human and non-human identities like applications, scripts, and bots.

- Lockdown critical endpoints: This is with advanced endpoint privilege management solutions to restrict privilege across all endpoints, prevent lateral movement, and defend against ransomware and other malware.
- Implement adaptive multifactor authentication: by using contextual information like location, time of day, IP address, and device type, along with business rules to determine which authentication factors to apply to a specific user in a particular situation.

- Secure developer tools: This is by using secrets management solutions to protect, manage, rotate, and monitor secrets and other credentials used by applications, automation scripts, and other non-human identities. Enterprises typically combine privileged access management solutions, endpoint privilege management solutions, adaptive multifactor authentication solutions, and secrets management solutions with traditional enterprise security solutions like EDRs, firewalls, and IDS/IPS as part of a comprehensive, modern defense-in-depth strategy.

Discussion

Considering the evolving landscape of cyber threats, what are the most prevalent types of cyberattacks today, and discuss how modern defense mechanisms can effectively counter these threats, particularly in the context of legal and technological challenges.

3.5 Summary

At the end of this unit, you have learnt how and when to use the defence strategies. In the next unit, you wil be learning about threats to the national critical infrastructures.

You have learnt from this unit the different types of threats and how to take steps to protect your information resources. You have also learnt some defence strategies and analysis of the threats.

3.6 References/Further Readings/Web Resources

Adeyemi, O. O. (2023). *Cybercrime, Digital Forensics, and Jurisdiction in Nigeria*. University Press of Nigeria.

Chakraborty, A., Alam, M., Dey, V., Chattopadhyay, A., & Mukhopadhyay, D. (2018). Adversarial attacks and defences: A survey. arXiv preprint arXiv:1810.00069.

Diogenes, Y., & Ozkaya, E. (2022). Cybersecurity – Attack and Defense Strategies (Third Edition). Packt Publishing .

Okoye, K. (2022). *Cybersecurity in Nigeria: Threats, Vulnerabilities, and Defense Mechanisms*. Lagos: CyberDefence Publishing.

Rodríguez-Barroso, N., Jiménez-López, D., Luzón, M. V., Herrera, F., & Martínez-Cámara, E. (2023). Survey on federated learning threats: Concepts, taxonomy on attacks and defences, experimental study and challenges. Information Fusion, 90, 148-173.

Rot, A., & Olszewski, B. (2017, September). Advanced Persistent Threats Attacks in Cyberspace. Threats, Vulnerabilities, Methods of Protection. In FedCSIS (Position Papers) (pp. 113-117).

Zlomislić, V., Fertalj, K., & Sruk, V. (2017). Denial of service attacks, defences, and research challenges. Cluster Computing, 20, 661-671.

3.7 Possible Answers to Self-Assessment Exercise(s)

Answers to SAEs

1. What is a cyber threat?

Answer:
A cyber threat is any potential danger to computer systems, networks, or data. These threats can come from individuals, groups, or even governments and can result in data loss, system damage, or financial loss.

2. Mention three common types of cyber threats.

Answer:
Three common types of cyber threats are; Malware, Phishing and Ransomware

3. List three basic solutions to protect systems from cyber threats.

Answer:
The three basic solutions are: Strong passwords, software updates and backup data.

4. List three examples of cyber threats.

Answer:
Example of free of cyber threats are Ransomware Attacks, Internet of Things (IoT) Vulnerabilities, Phishing Attacks.

5. What is the concern of cyber security experts in cyber defence?

Answer:
Cyber security experts are having serious concern in cyber defence because of the growing complexity of cybercriminals, state-sponsored hackers, and other threat actors, along with the quick speed at which cyberattacks can happen, makes it challenging to respond and minimise damage

Unit 4 Cybercrime as Threat to the National Critical Infrastructure

Unit Structure

4.1 Introduction

You will learn from this unit the threats to the national critical infrastructures. After studying this unit, you will be able to identify all forms of cyber threats that target critical infrastructures. You will be able to know the different sectors of critical infrastructures in the remaining sections of the unit.

4.2 Learning Outcome

By the end of this unit, you will be able to:

- identify and analyse threats to critical infrastures and profer solutions.

4.3 Cybercrime as Threat to the National Critical Infrastructure

4.3.1 National Critical Infrastructure

National Critical Infrastructure (NCI) includes the essential systems, facilities, and networks that are crucial for a country and its economy to function properly. Examples of CNI are the water supply, which provides the water we need, the energy sector that powers our homes

and industries, and the telecommunication networks that allow us to communicate and connect with each other. Additionally, CNI also covers assets that may not be necessary for daily life but require protection due to their potential danger, such as nuclear power stations or chemical plants that could pose a serious public health risk if attacked or damaged.

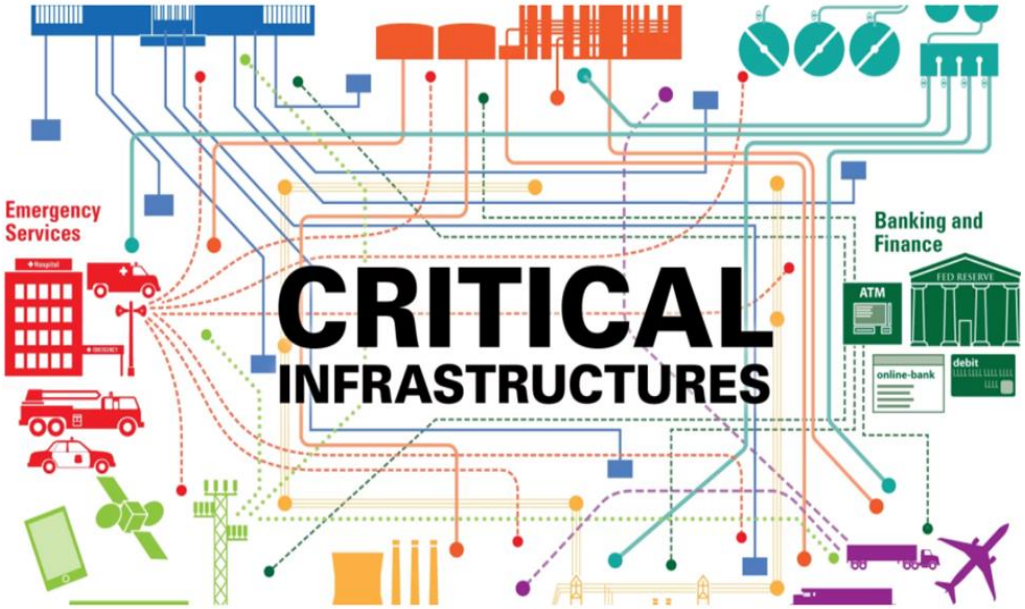


Fig. 3.1: The sectors that depict National Critical Infrastructure. *(Young, 2024)*

4.3.2 Sectors of National Critical Infrastructure

These sectors are all interconnected and crucial for modern society. If one sector experiences a disruption, it can have a domino effect on the others. For instance, if there is a cyberattack on the energy sector, it could result in power outages that impact transportation, communication, healthcare, water, financial systems, and other important services. The sectors are listed below:

- Defence Industrial Base: Manufacturing and supply chain for defence equipment.
- Energy: Power generation, transmission, and distribution.
- Water and Wastewater: Treatment, distribution, and disposal.
- Transportation: Roads, bridges, airports, railways, and ports.
- Government Facilities: Federal, state, and local government buildings and operations.
- Banking and Finance: Financial institutions and markets.
- Healthcare and Public Health: Hospitals, clinics, and public health systems
- Dams: Hydropower generation and flood control.

- Food and Agriculture: Production, processing, and distribution.
- Nuclear Reactors, Materials, and Waste: Nuclear power plants and related facilities.
- Chemical: Manufacturing, storage, and transportation of chemicals.
- Information Technology: IT systems and infrastructure.
- Communications: Telecommunications, internet, and broadcasting.
- Commercial Facilities: Large commercial buildings and complexes.

4.3.3 Importance of National Critical Infrastructure (NCI)

This is also called the Ghosting or Gold Standard (GS) approach. It involves backing up data of an infected hard drive and transferring the data on to a new hard drive, reinstalls all user applications and settings. The re-imaging process may require 6-8 hours to be done right which may be very expensive for small businesses who only have that computer for usage which is been cleaned up. If any of the National Critical Infrastructures is disrupted, it can significantly impact a nation and its citizens' daily lives.

The re-imaging approach is most appropriate for enterprise installation that involves hundreds of computer systems that all imaged from the same hard drive without locally installed programmes and data on them. However, re-imaging is not what most users want because it may lead to catastrophic problems in terms of data loss when it comes to small business and home users. Furthermore, a computer will never look the same after a re-imaging process.

- **National Security**

NCI plays a crucial role in supporting national defense and security operations. If NCI fails, the UK could become vulnerable to attacks from hostile actors or nation-states, including cyberattacks.

- **Public Safety**

NCI provides essential services like water, electricity, healthcare, and transportation. Any disruption to these services could have a serious impact on the safety and well-being of the population.

- **Economic Stability**

In today's digital economy, communication and transportation networks are crucial for business operations, supply chains, and overall economic stability. Disruptions to NCI can result in significant financial losses for organisations and the economy as a whole.

- **Disaster Resilience**

NCI helps nations prevent and withstand terrorist attacks, cyberattacks, and natural disasters. In the event of such incidents, emergency response services play a critical role in coordinating recovery efforts.

- **Sector Interdependence**

Since a nation's critical infrastructure is highly interdependent, disruptions in one sector can have a ripple effect on others. For example, if essential IT networks fail, it could disrupt the control and coordination of energy supplies.

Self-Assessment Exercise 1

1.	Why is a comprehensive approach necessary to safeguard critical infrastructure assets?

4.3.4 Threat to National Critical Infrastructure

In today's uncertain world, the country's National Critical Infrastructure is at risk from a range of threats, both natural and man-made. These threats include the followings:

- **Vandalism**

NCI may face vandalism, terrorism, or sabotage from internal staff or external malicious actors.

- **Natural Disasters**

Such as floods, storms, wildfires, and climate change effects can impact NCI assets like transportation, power, and water supplies.

- **Regional Conflicts**

Regional conflicts, global power shifts, trade disruptions, sanctions, and cyberattacks can directly affect NCI due to geopolitical challenges posed by states and non-state actors.

- **Risks of Supply Chain**

NCI assets relying on global supply chains for essential components are at risk of shortages if the supply chain is disrupted.

- **Emerging Technologies**

Emerging technologies like artificial intelligence and quantum computing may introduce new threats to NCI, necessitating continuous research and protective measures.
The interconnected nature of NCI assets itself poses a threat, as disruptions in one sector can quickly spread to others. Therefore, safeguarding the country's critical assets requires a comprehensive approach.

Self-Assessment Exercise 2

1.	Conducting regular risk assessments and vulnerability studies to identify potential weaknesses protect national critical infrastructure?

 **Discussion**

If a health system computer has been compromised by cyber attackers, discuss your solution as a student.

 **4.4 Summary**

At the end of this unit, you have learnt the infrastructures that constitute National Critical Infrastructure. You also learned that there could be a devastating consequence on national security if there is any cyberattack on National critical infrastructures. In the next module, you will learn the Investigation Process of Cybercrime.

You have learnt from this unit, that cybercrime poses a significant threat to national critical infrastructure, compromising the reliability, integrity,

and security of essential systems and services. You have also learnt that effective mitigation requires a multi-faceted approach, combining robust cybersecurity measures, international cooperation, and continuous monitoring to stay ahead of evolving threats. In the next unit, I will be discussing the investigation process of cybercrime threats.

4.5 References/Further Readings/Web Resources

Adeyemi, O. O. (2023). *Cybercrime and National Critical Infrastructure in Nigeria*. University Press of Nigeria.

Destiny Young (2024), Critical Infrastructure Protection: Why the Nigerian Government Must Invest in Cybersecurity. https://youngdestinya.ng/tag/critical-infrastructure

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2018). *Cybercrime and Digital Forensics: An Introduction* (3rd ed.). Routledge.

Lewis, J. A. (2022). " Cyber Threats to Our Nation's Critical Infrastructure". Centre for Strategic and International Studies (CSIS).

Rudner, M. (2013). Cyber-threats to critical national infrastructure: An intelligence challenge. *International Journal of Intelligence and Counter Intelligence, 26(3), 453-481.*

Sibe, R. T., & Kaunert, C. (2024). Cybercrime, Digital Forensic Readi ness, and Financial Crime Investigation in Nigeria. Springer.

Wilson, C. (2014). *Cyber threats to critical information infrastructure. In Cyberterrorism: Understanding, Assessment, and Response* (pp. 123-136). New York, NY: Springer New York.

4.6 Possible Answers to Self-Assessment Exercise(s)

Answers to SAEs

1. What is the primary goal of protecting national critical infrastructures?

a. To ensure economic growth
b. To protect against cyber threats only
c. To prevent disruptions to essential services
d. To reduce costs

Answer: 'c' To prevent disruptions to essential services

2. Which of the following is a key component of protecting national critical infrastructures?

a. Regular risk assessments
b. Only physical security measures
c. Only cybersecurity measures
d. None of the above

Answer: 'a' Regular risk assessments

3. What can be a consequence of a successful attack on national critical infrastructures?

a. Minor disruptions
b. No impact on society
c. Cascading failures across multiple sectors
d. Only financial losses

Answer: 'c' Cascading failures across multiple sectors

4. Which of the following sectors is an example of national critical infrastructure?

a. Entertainment
b. Education
c. Energy
d. Retail

Answer: 'c' Energy

5. Why is a comprehensive approach necessary to protect national critical infrastructures?

a. Because each sector is independent
b. Because threats only come from outside the country
c. Because of the interconnected nature of critical infrastructures
d. Because it's too expensive to protect

Answer: 'c' Because of the interconnected nature of critical infrastructures

6. Why is a comprehensive approach necessary to safeguard critical infrastructure assets?

Answer:
A comprehensive approach is necessary because the interconnected nature of critical infrastructure assets poses a threat, where disruptions in one sector can quickly spread to others, and a coordinated effort can help mitigate this risk and prevent cascading failures.

7. Conducting regular risk assessments and vulnerability studies to identify potential weaknesses protect national critical infrastructure?

Answer:
Yes, conducting regular risk assessments and vulnerability studies can help protect national critical infrastructure (NCI) by:

1. Identifying potential weaknesses and vulnerabilities before they can be exploited.
2. Allowing for proactive measures to mitigate or address identified risks.

MODULE 2 INVESTIGATION PROCESS OF CYBERCRIME

Module Introduction

In module 1, you have learned the basics of cybercrime like definitions, history, evolution, and causes of cybercrime. I also discussed in detail, the incursion of cybercrime in Nigeria, as well as the motivation for the cybercrime. In this module 2. I will take you through the Investigation processes of cybercrime and its unique challenges that require a distinct approach. I will discuss different aspects of the investigation processes in each unit. There will be 4 units to consider four main topics. Topics include the procedures for cybercrime, strategies of cybercrime perpetrators, Successful Use of Online Social Networks for Cybercrime Investigation and Cyber-Terrorism.

Unit 1 Procedures for Cybercrime
Unit 2 Strategies of Cybercrime Perpetrators
Unit 3 Successful Use of Online Social Networks for Cybercrime Investigation
Unit 4 Cyber Terrorism

In each unit, I will explore a particular topic in detail and highlight self-assessment exercises at the end of the unit. Finally, I highlight resources for further reading at the end of each unit.

Unit 1 Procedures for Cybercrime

Unit Structures

1.1 Introduction
1.2 Learning Outcomes
1.3 Procedures for Cybercrime
  1.3.1 Computer Cybercrime Investigations
  1.3.2 Cybercrime Mode of Operation
  1.3.3 Stage Setting for Cybercrime
1.4 Summary
1.5 References/Further Readings/Web Resources
1.6 Possible Answers to Self-Assessment Exercise(s)

1.1 Introduction

You will learn from this unit the various processes of investigating cybercrime. You will also learn the modus operandi of cybercriminals

and how to guard against them. After studying this unit, you will be able to acquaint yourself with the knowledge of the stages cybercriminals follow before attacking.

1.2 Learning Outcomes

By the end of this unit, you will be able to:

- use some of the investigation techniques
- predict that an attack is imminent.

1.3 Procedures for Cybercrime

1.3.1 Computer Cybercrime Investigations

Investigating computer crimes involves finding and stopping illegal activities that occur on computers and digital devices. This process requires special tools and methods to analyse crimes such as hacking, phishing, malware, data breaches, and identity theft. Professionals who perform this task are known as computer crime investigators.

They meticulously search for evidence that can help law enforcement apprehend individuals involved in these unlawful activities. Investigating computer crimes is crucial for individuals and businesses to safeguard themselves against the growing threats posed by these crimes and to ensure justice for victims. The continuous evolution of these crimes highlights the importance of investigating them, as they can have severe consequences for everyone, including governments and businesses.

- **Description of Criminals**

Cyber Terrorists: Individuals or groups who carry out attacks over the Internet for political reasons, often with the goal of causing societal disruption. Many of these actors are motivated by political ideologies.

Insiders Attackers: These can be employees or part-time workers who exploit their access to a company's network to steal data, damage property, or commit other illegal activities.
Organised Attack Groups: These are organised gangs that commit cybercrimes for profit and are skilled at covering their tracks.

Cyber Cracker/Hackers: These individuals are skilled in computers and break into unauthorised systems to steal information or cause damage. Some do it for financial gain, while others do it to test their skills or because of their beliefs.

State-Sponsored: Some nations attack the computer systems of other countries to gain secret information, disrupt operations, or gain a competitive advantage.

- **Investigation Techniques of Cybercrime**

Various technical and non-technical strategies are employed in cybercrime investigation.

1 Digital forensics is one of the most popular investigation techniques. it involves preserving, collecting, and analysing digital evidence. It may include recovering deleted files, examining data details, or investigating network traffic logs. Special software like EnCase, FTK, and Autopsy is used

2 Aside from digital forensics, cybercrime investigators have alternative methods to gather evidence and pinpoint suspects. These methods include interviewing witnesses, analysing surveillance camera footage, and tracing the flow of money. Investigators may also pose as victims or create fake profiles on social media to deceive suspects into disclosing information. This tactic is known as social engineering.

3 In investigating computer crimes, there should be synergy between the various agencies and organisations. Cybercrime Investigators should exchange information with law enforcement, government entities, or private cybersecurity firms to combine resources. Working together in partnership will help them to identify patterns, pursue suspects, and benefit from each other's successful strategies.

1.3.2 Cybercrime Mode of Operation

Most cybercrimes are preceded by careful preparation and planning by hackers or crackers in order to ensure success. Hacking goes beyond simply gaining access and fixing vulnerabilities. Established techniques are utilized to guide the criminal through the hacking process and ensure they reach their intended target. Due to their advanced computer skills, cyber-criminals must develop a methodology that aligns with their hacking objectives.

Self-Assessment Exercise(s) 1

1.	What do hackers aim to do with security vulnerabilities?

1.3.3 Stage Setting for Cybercrime

Advancement in cybersecurity discipline has given rise to technologies and task automation tools. As useful as these tools to cybersecurity solutions, cyber criminals (Hackers) have taken advantage of these tool to fast track their malicious activities. These tools allow criminals to focus on the tests rather than the methods. These tools gather small pieces of information and put them together. Criminals start with a goal in mind, hack their way through many steps, and eventually find security vulnerabilities at a point in the system. The goals and methods used can varies. Hackers will try to identify all security vulnerabilities and figure out how to exploit them. Attackers can target any system from any angle, not just from the network perimeter or the Internet. They test every possible entry point, including partner, vendor, and customer networks, as well as home users and connectable devices. Figure 3.3 shows the stage setting for Cybercrime.

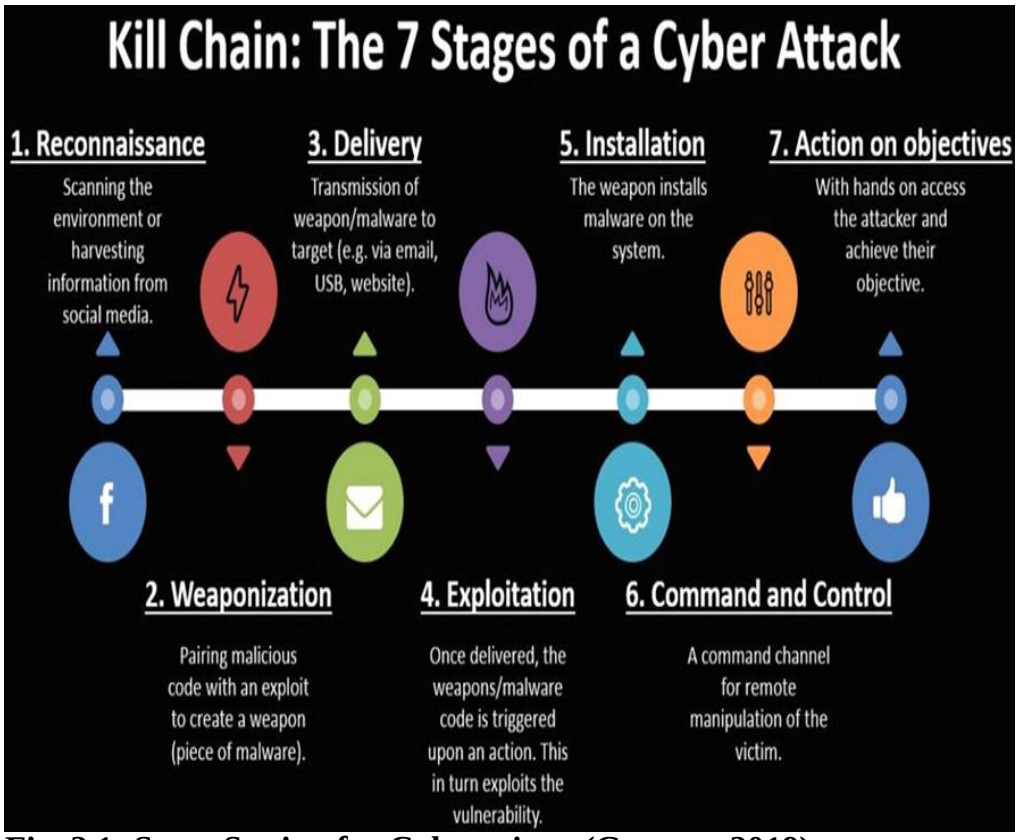


Fig. 2.1: Stage Setting for Cybercrime. (Gonapa, 2019).

- **Preparing to Attack**

The initial phase of a cyber-attack is known as reconnaissance. During this stage, attackers collect information about their target by gathering publicly available data from websites, social media, physical locations, and details about key employees in the organisation. Attackers also utilize open-source intelligence (OSINT) tools and information from the dark web to find credentials and vulnerabilities related to the organisation. After gathering this information, attackers move on to resource development. This involves creating tools to use against the organisation and acquiring additional capabilities, such as purchasing or renting physical or cloud servers, domains, or third-party web servers to compromise the organisation's infrastructure and service accounts.

- **Initiating the Attack**

Once all necessary resources are prepared, cyber attackers will gain initial access to your system through methods such as phishing attacks, compromising your supply chain, or exploiting public-facing assets. Once inside, the attackers will escalate their activities by executing malicious code, exploiting native APIs, containers, services, scheduled jobs, or shared modules. During the persistence stage, the attackers will maintain a presence in your system. They will then move on to privilege escalation, allowing them to perform actions typically reserved for administrators or root users.

- **Evasion**

Avoiding Detection to remain undetected in your system, attackers will practice evasion techniques. This includes using methods already in use within your system, such as "living off the land". For example, if your system uses PowerShell scripts, attackers will also use PowerShell commands to disguise their activities. By evading detection, attackers can move on to obtaining credential access by stealing account names and passwords. This allows them to map out the target environment and identify additional systems for lateral movement.

- **Gathering Information**

At this stage, attackers will begin collecting valuable data, such as trade secrets and personally identifiable information (PII). They may also install command and control malware to communicate and manipulate compromised systems using encrypted channels and exploited application protocols.

- **Final Stage of the Attack**

The final stage of a cyber-attack is the impact stage, where attackers may destroy information, modify configurations, or disrupt services.

- **Covering Tracks**

Some attackers will attempt to cover their tracks to avoid detection for extended periods, potentially months or even years.

Self-Assessment Exercise(s) 2

1.	What is the motivation behind attackers covering their tracks after a cyber-attack?

Discussion

After reading this unit, explain investigation techniques. Propose the best approach to discourage the information-gathering stage of the attack.

1.4 Summary

At the end of this unit, you have learnt the technique of cyber attackers. In the next unit, you learn about Strategies of Cybercrime Perpetrators.

You have learnt from this unit how to establishing standardized procedures for cybercrime investigation and response is crucial for effective detection, containment, and prosecution of cyber offenses. You have also learnt that, by adopting a comprehensive and coordinated approach, law enforcement agencies and organisations would help to disrupt and dismantle cybercriminal networks. I will discuss the strategies of cybercrime perpetuators.

1.5 References/Further Readings/Web Resources

Adeyemi, O. O. (2023). *Cybercrime Investigations: A Nigerian Perspective*. University Press of Nigeria.

Alkaabi, A., Mohay, G., McCullagh, A., & Chantler, N. (2011). Dealing with the problem of cybercrime. In Digital Forensics and Cyber Crime: Second International ICST Conference, ICDF2C 2010, Abu Dhabi, United Arab Emirates, October 4-6, 2010, Revised Selected Papers 2 (pp. 1-18). Springer Berlin Heidelberg.

Dragan, A. T. (2015). Procedural Aspects of Cybercrime Investigation. Journal of Legal Studies "Vasile Goldiş", 16(30), 55-66.

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2018). *Cybercrime and Digital Forensics: An Introduction* (3rd ed.). Routledge.

Oerlemans, J. J. (2017). Investigating cybercrime (No. s 51). Amsterdam University Press.

Sibe, R. T., & Kaunert, C. (2024). Cybercrime, Digital Forensic Readine ss, and Financial Crime Investigation in Nigeria. Springer.

Tsakalidis, G., & Vergidis, K. (2017). A systematic approach toward description and classification of cybercrime incidents. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 49(4), 710-729.

1.6 Possible Answers to Self-Assessment Exercise(s)

Answers to SAEs

1. What type of data do attackers collect during the information-gathering stage of a cyber-attack?

a) Only personally identifiable information (PII)
b) Only trade secrets
c) Valuable data, including trade secrets and personally identifiable information (PII)
d) None of the above

Answer: 'c' Valuable data, including trade secrets and personally identifiable information (PII)

2. What is the primary goal of the final stage of a cyber-attack?

a) To gather information
b) To cover tracks

c) To impact the system by destroying information, modifying configurations, or disrupting services
d) To install malware

Answer: 'c' To impact the system by destroying information, modifying configurations, or disrupting services

3. Why do some attackers attempt to cover their tracks after a cyber-attack?

a) To speed up detection
b) To increase their chances of getting caught
c) To avoid detection for extended periods
d) To delete their malware

Answer: 'c' To avoid detection for extended periods

4. What do hackers aim to do with security vulnerabilities?

Answer: Hackers try to identify all security vulnerabilities and figure out how to exploit them.

5. What is the motivation behind attackers covering their tracks after a cyber-attack?

Answer: To remain undetected for a long time, possibly months or years.

Unit 2 Strategies of Cybercrime Perpetrators

Unit Structure

2.1 Introduction

It is important to understand the strategies used by cybercriminals in order to protect digital assets. These criminals use a variety of tactics, such as advanced malware and social engineering techniques, to take advantage of weaknesses and infiltrate systems. In this unit, you will be introduced to the various strategies that cybercriminals employ to perpetrate their crimes.

2.2 Learning Outcome

By the end of this unit, you will be able to:

- discuss the strtategies of cybercrimals and the countermeasures to curtail their activities.

2.3 Strategies of Cybercrime Perpetrators

2.4 Techniques of Cybercrime Perpetrators

Cybercriminals have become more sophisticated due to advanced technology and strong motivation.

These criminals carry out attacks by using one or more computers to target a single device or a network of devices. They infiltrate IT security systems and the Internet of Things (IoT) through malicious methods such as malware, phishing, ransom ware, denial-of-service attacks, artificial intelligence, and data manipulation.

A cyber-attack is when cybercriminals use one or more computers to launch an assault against a single device or multiple devices within a network. They employ various techniques like malware, phishing, ransom ware, and denial of service to carry out these attacks.

2.5 Phishing Attack Technique

Spear phishing is the most dangerous form of phishing. Unlike generic, template-based attacks, spear phishing involves finding out information about the target in order to customize the phishing message to make it more likely to work.

A spear phishing attack begins with the cyber criminal finding information about the target, then using that target to build a connection, and thirdly using that connection to make the target perform an action. Read on to learn more about the bait, hook, and catch: the three stages of a spear phishing attack.

Step 1: The Information (Bait)

The first of the three steps of a phishing attack is preparing the bait. This involves finding out details about the target, which can be as simple as knowing that they use a particular service or work at a particular business. This is one of the reasons why data breaches where no ‘sensitive’ information is compromised can be so dangerous: if a service leaks a list of just email addresses of its users, criminals will be able to know that all the owners of those email addresses use that service and can target them with emails that pretend to be from that service.

In more sophisticated spear phishing attacks, cyber criminals can harvest details from your social media profiles in order to build a highly

customized spear phishing message that is highly likely to convince you of its genuineness.

Step 2: The Promise (Hook)

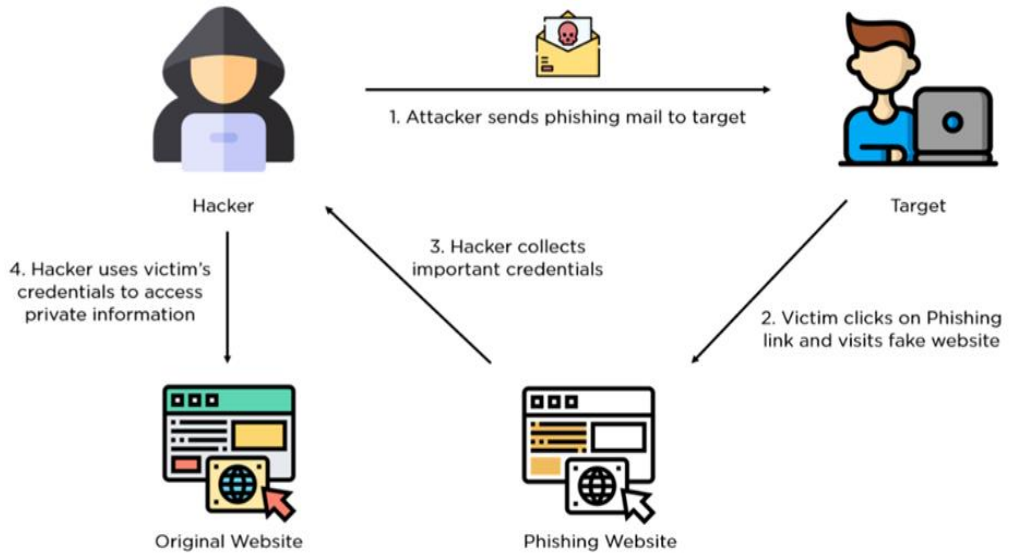
Once the attacker has acquired the necessary information to use as bait, they then need to lay out the hook. In order to actually make the target perform an action, the attacker needs to promise something or scare them into action.

In many scams, the hook involves making the target believe that one of their accounts has been compromised, creating a sense of urgency and making the target act quickly - perhaps without thinking. The attacker can then redirect the target to follow a link to a page where they can harvest the victim's details.

Step 3: The Attack (Catch)

The third phase of phishing is the actual attack. The cyber criminal sends out the email and prepares for the prey to fall for the bait.

What the attacker's next action will be will depend on the nature of the scam. For example, if they used a landing page to gain the victim's email password, they can then log in to the victim's email account in order to harvest more information and start sending further phishing emails to the victim's contacts. Figure 3.1 Shows the phases of phishing



attack.

Fig. 2.1 Phishing attack. (Jena, 2023)

2.5.1 Types of Fishing Attack

There are four major types of phishing attacks:

- **Pharming:** Pharming attacks involve hackers purchasing domain names similar to popular websites (e.g., www.gogle.com or www.facebuk.com) hoping that a target will type the URL quickly. When the target reaches the fake website, they may unknowingly submit their login credentials without verifying its authenticity.
- **Deceptive Phishing:** Deceptive phishing involves sending a single phishing email to many people, often without much research. The hacker is counting on a small percentage of recipients to click on a malicious link and provide their private information on a fake website.
- **Spear Phishing:** In spear phishing, hackers conduct research to increase their attacks' success rate. For example, if a person frequently orders from Dominos, a phishing email pretending to be from Dominos is more likely to be opened by the target compared to a random survey or newsletter.
- **Whaling:** Whaling targets high-profile individuals like CEOs and managers with carefully planned phishing attacks. Hackers invest time in researching the target to determine the best approach and timing for the attack.

2.5.2 Malware Attack Technique

Just like other hacking techniques, hackers who use malware have various ways to access data or steal money from their victims. These methods depend on the type of malware used, the malware's purpose, and how it is installed on the victim's computer.

The most common methods of malware attacks involve using viruses, worms, botnets, or ransomware to infect the victim's computer.

Infection can occur through tactics like phishing, drive-by downloads, social media links, or remotely accessing the computer to manually install the software.

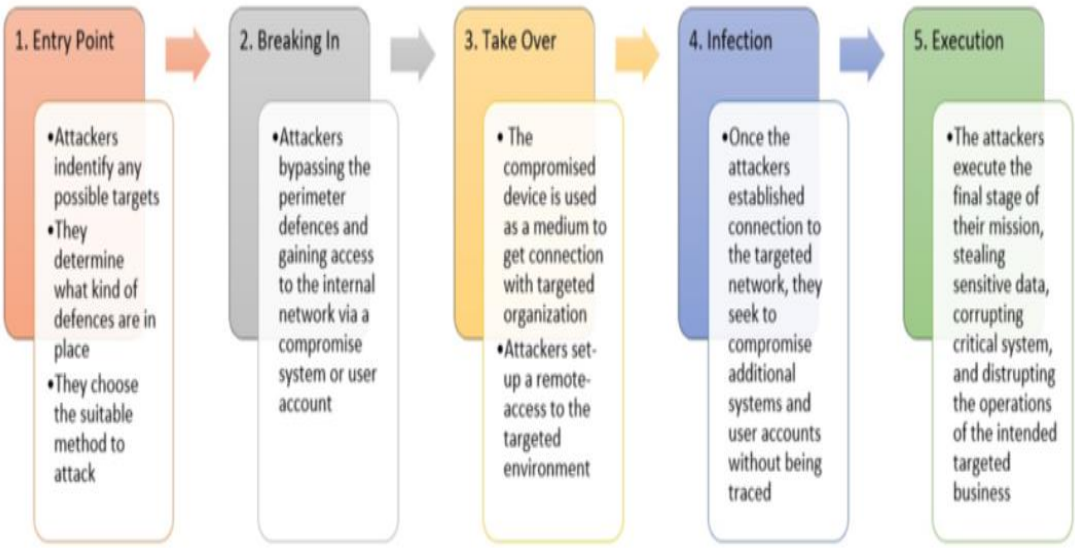


Fig. 2.2: Malware attack stages technique (Gorment et al, 2023)

2.5.3 Types of Malware

There are many major types of malware but for this course, I shall discuss just the four common types:

- **Botnet:** These are programs that infiltrate computers and create a network of compromised devices controlled by a central command server. They are often used to launch DDoS attacks.
- **Ransomware:** Ransomware locks the victim's computer, demanding payment to regain access. These are typically used for financial gain.
- **Computer Virus:** A computer virus behaves similarly to a virus in our bodies. The software duplicates itself and spreads quickly by attaching to other commonly used programs on the computer.
- **Worm:** Worms can also duplicate themselves and spread, but they contain themselves in their own containers and limit their harmful activities to the application they are in.

2.5.4 Botnet

Botnet attacks operate using a command and control system that enables hackers to control infected devices, also known as 'zombie bots', from a remote location. The more devices that are infected with the attacker's malware, the more powerful the attack is likely to be.

Botnet Attack Techniques:
Botnet attacks can be conducted by an individual or a team. In either case, a group of zombie bots is controlled by the bot herder, who is the

person or group leading the attack. The bot herder can create their botnet or rent one from other malicious actors (known as "malware-as-a-service," or MaaS). Once infected, zombie bots are controlled anonymously through a centralised client-server model or a decentralised peer-to-peer (P2P) model.

Centralised Model: A centralised botnet attack is carried out by a single server acting as the bot herder while in a decentralised botnet attack, the responsibility for giving instructions is distributed among all the bots in the botnet. If the attacker can communicate with any of them, the malware can still spread through the other compromised devices. The P2P framework makes it more challenging to identify the person or people in control, which is why the decentralised model is more commonly used. Three steps are majorly employed by the botnet attackers.

Finding a Vulnerability: Any weakness in a website or application can create an opportunity for botnet attackers. Sometimes, unintentional user actions can lead to these vulnerabilities. Regardless of how the vulnerability arises, the attackers aim to exploit it.

Infecting User Devices: This is the stage where unsuspecting users are unknowingly turned into zombie bots through the delivery of malware. For example, attackers may use methods like spamming and social engineering to trick users into downloading malware, such as a Trojan virus.

There are various delivery methods that attackers may use, some more aggressive than others. However, their main objective is to compromise your security by targeting a few users.

Mobilising the Botnet: Once a few devices are infected, the botnet attacker connects them to control them remotely. Their ultimate aim is to infect as many devices as possible to cause maximum damage.

2.5.5 Computer Virus

Computer viruses are created to disrupt systems, cause operational problems, and lead to data loss and leaks. It is important to understand that computer viruses are meant to spread through programs and systems. Usually, computer viruses attach themselves to executable host files, allowing their viral codes to activate when the file is opened.

Computer Virus Attack Techniques

Viruses can be transmitted through hard disks and USB devices, but they are more commonly spread between devices over the Internet.
Computer viruses can be transmitted through email, with some even able to take over email software to spread themselves. Others may attach themselves to legitimate software, and software packages, or infect code. Some viruses can also be downloaded from compromised app stores and infected code repositories.

A crucial aspect of any computer virus is that it needs a victim to run its code or payload, which requires the host application to be active. The code then spreads from the original document or software through networks, drives, file-sharing programs, or infected email attachments.

- The following are some signs of a computer virus attack: mass emails being sent from the user's email account, crashing of the device, changes of the computer homepage, pop-up windows, accounts being logged out, slowness in system speed, and programs self-executing.

- Types of Computer viruses are Web scripting viruses, Direct action, Network Viruses, Overwrite viruses, Resident viruses, Browser hijackers, File infectors, Multipartite viruses, and Boot Sector Viruses.

2.5.6 Ransomware

Ransomware is a harmful software that infects a person's computer or network, encrypting their files or blocking access to their system. The attacker then asks for a payment from the victim to unlock the data or system.

Ransomware Attack Techniques

- Ransomware Spread: Ransomware usually spreads through social engineering tactics or software vulnerabilities. Attackers commonly use phishing emails containing harmful attachments or links to infect victims' devices. These emails may seem legitimate, appearing to be from trusted sources like banks or delivery companies. Once the victim interacts with the attachment or link, the malware is installed on their computer. Ransomware can also spread through unpatched software vulnerabilities, like remote desktop protocols (RDP), insecure websites, or outdated software.

- Encrypting Data: After infecting the victim's computer, the malware begins encrypting files and folders on the hard drive, making them inaccessible. Ransomware often uses a strong encryption algorithm that requires a unique decryption key to unlock the data. Some ransomware types can also encrypt files on network drives or cloud storage, making data recovery even more challenging.

- Demands for Ransom: Those responsible for ransomware attacks typically demand payment in exchange for providing the decryption key to unlock the encrypted data. The ransom amount can vary, ranging from a few hundred dollars to tens of thousands of dollars, and is often requested in cryptocurrencies like Bitcoin, which are hard to trace. If the ransom is not paid within a specified time frame, attackers may threaten to delete or publish the victim's data. The ransom note usually includes detailed instructions on how to make the payment and obtain the decryption key.

Types of Ransomware

- Double extortion ransomware: This combines data encryption with the threat of data theft. Attackers first encrypt the victim's data and then threaten to publish it online if the ransom is not paid. This type of ransomware often targets businesses, as the publication of sensitive data can have serious financial and reputational consequences.

- Crypto ransomware: It works by encrypting the victim's files and then asking for a ransom payment in exchange for the decryption key. This type of ransomware is usually spread through email attachments or downloads from compromised websites. The encryption used by crypto-ransomware is very strong, making it hard to recover data without the decryption key.

- Locker ransomware: This is also known as screen locker, blocks access to the victim's system or specific files instead of encrypting them. It typically displays a message on the victim's screen demanding payment in exchange for restoring access. Locker ransomware can be distributed through infected websites or phishing emails.

2.5.7 Worm

A worm is malicious software that can quickly replicate and spread through devices on a network. It consumes bandwidth as it spreads,

which can overload infected systems and make them unreliable or inaccessible. Worms can also modify or delete files, as well as introduce other types of malware. Worms can be more dangerous than viruses due to their self-replicating nature. If a worm infects a vulnerable system, it will automatically spread across different devices.

Worm Attack Techniques

Software vulnerabilities create opportunities for worms to infect computers. Spam emails and instant message attachments are common delivery methods for worms. These messages often use social engineering tactics to trick users into opening malicious files. Worms can also spread through removable drives, such as USB drives, by taking advantage of automatic file-sending and receiving features on network computers. Once a computer is infected, the worm installs itself in the device's memory and can spread to other machines. The following outlines how criminals commonly exploit in their attacks.

- Vulnerability Exploitation: The first step of a worm attack occurs when the worm is installed on a device that has a vulnerability. This vulnerability could have been exploited through software, a malicious email or attachment, or a compromised removable drive.

- Self-Replication: Once the worm is on a vulnerable device, it starts replicating itself automatically. As it spreads through the network, it consumes bandwidth and storage space, impacting the performance of devices and systems.

- Payload Delivery: In the final stage of a worm attack, the attacker aims to increase their access to the targeted system. They may gain administrator-level access, allowing them to steal data and potentially access other systems.

- Continuous Spread: After infecting a device, the worm continues to spread by exploiting vulnerabilities in other connected systems. This allows attackers to gain access to multiple systems and potentially create a botnet for malicious activities like spamming and data theft.

Empower your users to help prevent cyber incidents. Learn how unsecured helps businesses drive secure behavior with intelligently-automated cyber security awareness training.

2.6 Countermeasures

Cybersecurity strategies and cybercrime prevention strategies are often used interchangeably, but they are not the same. While they complement each other and have some overlap, they are distinct concepts. Cybercrime prevention strategies involve efforts to address cybercrime directly and indirectly. This includes law enforcement responses and promoting cooperation between governments, businesses, academic institutions, organisations, and the public to control and reduce cybercrime.

- **Keep software updated**

Your operating system controls all the functions of your computer, making it a target for cybercriminals. Built-in features in operating systems help prevent attacks, but cyber risks are always changing. Operating system vendors release updates regularly to stay ahead of evolving threats from cybercriminals.

- **Use Next-Generation Firewalls (NGFW)**

NGFW is a network security device that offers more capabilities than a standard firewall. It can block modern threats like advanced malware and application-layer attacks through access control. NGFW includes features such as:

- **Conduct regular cybersecurity audits**

These audits provide a comprehensive assessment of your company's security, identifying vulnerabilities, risks, and threats to network security, physical security, data security, system security, and operational security.

- **Implement Two-Factor Authentication (2FA)**

2FA requires two forms of identification to access something, preventing unauthorised users from using a stolen password. Password breaches can happen when users use the same password on multiple websites or download software or click on email links. 2FA enhances online account security.

- **Educate staff and employees**

Provide appropriate training to staff to raise awareness of cybersecurity threats. Some departments, like Finance and HR, are more likely targets

due to their access to confidential information. Training can prevent disastrous consequences if a senior executive falls for a scam.

- **Install Spam Filters and Anti-Malware Software**

Spam filters block unsolicited and virus-infected emails, while anti-malware software defends against malicious programs. These tools scan for malware to prevent, detect, and remove it.

- **Encrypt Backup Data**

Encrypting backups adds an extra layer of security to protect data if it's stolen or compromised. Symmetric and Asymmetric encryption are common types used based on cryptography algorithms.

- **Consider Cyber Security Insurance**

Cyber insurance covers losses from cyber incidents like data theft, hacking, denial of service attacks, and legal claims. It can help with legal defense, customer reparations, data recovery, and other expenses not typically covered by standard insurance policies.

- **Protect Confidential Data**

Data confidentiality ensures that information is only accessible to authorised individuals through mechanisms like file encryption and data access management.

- **Use Endpoint Detection & Response (EDR)**

EDR is an endpoint security system that monitors and collects data from endpoints to detect and respond to security threats. It automates threat removal, alerts security professionals, and uses forensics and analysis tools to investigate threats.

- **Security Awareness Training**

Cybersecurity awareness training is created to teach people and organisations about the significance of cybersecurity, how to identify cyber threats, and safeguard sensitive data. The goal is to increase awareness about the importance of IT security. With cybersecurity threats increasing, the expenses of data breaches can be substantial. Cybersecurity training assists individuals and companies in reducing risks, securing sensitive data, and avoiding security incidents.

Self-Assessment Exercise(s) 1

1.	Identify one major difference between a virus and a worm.

Discussion

Apart from replication and propagation under this unit, can you discuss other differences between viruses and worms? You can choose to respond individually or as a group of three (3) members at maximum.

2.7 Summary

So far, you have learned that cybercrime perpetrators use advanced technology and motivation to carry out sophisticated attacks. They target devices or networks using malicious methods like malware and phishing.

Cyber-attacks involve using one or more computers to launch an assault on a device or network. Spear phishing is a dangerous form of phishing that involves customizing messages to targets. It involves three stages: preparing the bait (gathering information), building a connection, and making the target perform an action. Therefore, in the next unit you will be introduced to Cyber Terrorism and its overall impacts on the world security.

You have learned from this unit, the cybercrime perpetrators' strategies. You have also learned some preventive strategies to guard against the attack strategies discussed so far.

2.8 References/Further Readings/Web Resources

Adeyemi, O. O. (2023). *Cybercrime Strategies and Tactics: A Nigerian Perspective*. University Press of Nigeria.

Aransiola, J. O., & Asindemade, S. O. (2011). Understanding cybercrime perpetrators and the strategies they employ in Nigeria. Cyberpsychology, Behavior, and Social Networking, 14(12), 759-763.

Aransiola, J. O., & Asindemade, S. O. (2023). Understanding Cybercrime Perpetrators and the Strategies They Employ in Niger ia. Cyberpsychology, Behavior, and Social Networking.

Brenner, S. W. (2013). Cybercrime: Re-thinking crime control strategies. In Crime online (pp. 12-28). Willan.

Hawdon, J. (2021). Cybercrime: Victimization, perpetration, and techniques. American Journal of Criminal Justice, 46(6), 837-842.

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2018). *Cybercrime and Digital Forensics: An Introduction* (3rd ed.). Routledge.

Sarkar, G., & Shukla, S. K. (2023). Behavioral analysis of cybercrime: Paving the way for effective policing strategies. Journal of Economic Criminology, 100034.

2.9 Possible Answers to Self-Assessment Exercise(s)

Answers to SEAs

1. Do cybercrime perpetrators often use social engineering tactics to trick victims into revealing sensitive information?

Answer: Yes

2. Do cybercrime perpetrators typically use easily traceable communication channels to coordinate their attacks?

Answer: No

3. Do cybercrime perpetrators often exploit vulnerabilities in software or operating systems to gain unauthorised access to systems?

Answer: Yes

4. Identify one major difference between a virus and a worm.

The major difference between a virus and a worm is:

Replication and Propagation

- A virus requires human interaction (e.g., opening an infected email attachment or executing an infected program) to replicate and spread.

- A worm, on the other hand, can replicate and spread automatically without human interaction, often by exploiting vulnerabilities in operating systems or networks.

Unit 3 Successful Use of Online Social Networks for Cybercrime Investigation

Unit Structures

3.1 Introduction

In the previous units, cybercrime was discussed generally, however, in this unit, Online Social Networks and Cybercrime investigation will be discussed. Online social networks are an integral aspect of modern communication, linking people worldwide through platforms like Facebook, Instagram, and Twitter. Online Social Networks (OSNs) are online platforms that allow user communications and content distribution.

Cybercrime on the other hand is the illegal activities done through these networks, including identity theft, phishing, and cyberbullying, highlighting the vulnerabilities and security challenges inherent in online social interactions. This unit shall look at the method of Successful Use of Online Social Networks for Cybercrime Investigation.

3.2 Learning Outcome

By the end of this unit, you will be able to:

- successfully use online social networks for cybercrime investigation.

3.3 Successful Use of Online Social Networks for Cybercrime Investigation

3.4 Introduction to Online Social Networks and Cybercrime

Online Social Networks (OSNs), though, useful, and inevitable these days, have become tools for cyber criminals and crime investigations alike. OSNs have become tools for cybercrime investigation because they offer investigators a wealth of publicly shared information that can be analysed for criminal activity. Through observing posts, messages, and interactions, authorities can trace doubtful conduct, identify patterns, and uncover digital evidence tied to cybercrimes like fraud, identity theft, and illegal online transactions.

These networks allow law enforcement agents to track the digital footprints of suspects and build cases through data-driven insights, often showing hidden contacts that traditional investigative methods might miss. Hence, OSNs, are very important in modern cybercrime detection and prevention.

3.4.1 Definition of Online Social Networks (OSNs)

Different definitions can be given to OSNs depending on the angle through which they are viewed. OSNs can be defined as web-based platforms where individuals generate profiles, interact with friends, share content like posts, photos, and videos, and partake in online groups. Examples comprise Facebook, where users share life updates, and Instagram, where people share photos and videos.

OSNs can also be defined as relationship-building tools which can be platforms created for building and preserving social relationships by linking people with similar interests, allowing communication and information exchange. For example, LinkedIn is used for professional networking, and Twitter is a microblogging platform that connects people through brief status updates.

In terms of Content Creation and Sharing, OSNs can be defined as platforms that allow users to create and share content such as text, images, videos, or links to other websites, encouraging interaction through comments, likes, or shares. YouTube is an example where users create and share videos, while TikTok focuses on short video content creation and engagement.

When discussing Data-Driven Platforms, OSNs function as schemes where large amounts of data are created, analysed, and utilized for diverse purposes like advertising, market analysis, or even cybercrime investigation. For example, Reddit is an online community where users share discussions and content on a wide range of topics, generating valuable data insights. Snapchat provides real-time communication through short-lived multimedia messages.

3.4.2 Overview of Cybercrime

There are lot of cybercrimes that take place using the social network platforms. Some of them are cyber stalking**,** where individuals use platforms to harass or threaten others, and identity theft, where personal information shared online is exploited to steal identities. Furthermore, there are issues of online fraud which include scams such as phishing schemes, while coordinated cyber-attacks such as Distributed Denial of Service (DDoS) attacks are arranged through social platforms, as seen in real-world cases of social media-driven scams or in case of cyberbullying that cause harm to victims.

3.5 Investigative Techniques in Social Networks

Investigators can monitor social media activity to track suspects, gather evidence, and identify potential networks of criminal collaborators.

The behavior, locations, and relationships of cyber criminals can significantly aid law enforcement efforts in identifying and apprehending individuals involved in illicit activities.

Social networks allow investigators to analyse patterns in communication and interactions that might signal criminal intent or involvement. Advanced tools, such as social media analytics, and Maltego can help sift through vast amounts of data to pinpoint suspicious activities and trace digital footprints.

Steps in Investigation

Investigators start by finding a suspect's social media accounts using basic search techniques and specialized investigative tools such as

Maltego. They then analyse posts, connections, and activity to uncover potential evidence, such as incriminating messages, photos, or geo-tagged locations. For example, in a fraud case, investigators might examine a suspect's social media posts for signs of a luxurious lifestyle that is inconsistent with their reported income. By monitoring social networks, law enforcement can gather evidence, track suspects, and build a case against cybercriminals.

The following URL is the video on the basics of cybercrime investigation: https://www.youtube.com/watch?v=pM8yX-cr6S8.

3.5.1 Open-Source Intelligence (OSINT) Techniques

Maltego is an open-source intelligence (OSINT) and forensics-free tool for cybercrime investigation that allows investigators to collect and analyse data from various online sources, including social media, domain names, email addresses, and more. It helps create visual link diagrams that can reveal connections between entities, making it easier to identify relationships in cybercrime investigations.

.

How to Use Maltego

1. Download and install Maltego from the official website (community edition is free).
2. Set up an account and log in to access the tool's interface.
3. Choose a "Transform" to search for a specific entity, such as a domain, email address, or social media profile.
4. Run the transform, and Maltego will gather and display related information such as IP addresses, associated domains, or linked social media accounts.
5. Analyse the results using Maltego's graph-based visualization to identify connections between different entities, which can lead to discovering key evidence in the investigation.

The knowledge of how to use Maltego assists in mapping out a suspect's digital footprint and uncovering potential criminal activities.

3.5.2 Tracking Digital Footprints

This is a technique of observing and analysing the traces of data that people leave behind when they engage in online activities. These "footprints" comprise things such as the websites visited, social media interactions, login information, online purchases, and more.

Digital footprint can be used for many purposes such as improving cybersecurity or helping law enforcement in investigations. For instance, when analysing posts, messages, geolocation data, and media shared by suspects, it is important to start by explaining the concept of digital footprints, that is, the traces left behind by users through their online activities.

Investigators can gather vital evidence by examining posts, messages, and media shared on social media platforms. A vital part of this analysis is metadata which involves details such as the time and date of posts, the type of device used, and in some cases, IP addresses that can help locate the suspect. For instance, geotagging in photos (metadata that embeds the location where the picture was taken) can reveal the exact geographical coordinates.

> *The following video introduces what is Geotagging: (https://www.youtube.com/watch?v=THB8XdLj7Wk) while the next video explains Geotagging and Tracking Using an Android Phone (https://www.youtube.com/watch?v=swBB2hNvUNY).*

3.5.3 Preserving Evidence

This is a meticulous process of collecting and safeguarding digital data to guarantee it remains intact and legally admissible in court. This method stresses following strict legal steps, comprising taking screenshots of related posts or messages, gathering metadata (e.g., time stamps, location data), and using specialized software to maintain a clear chain-of-custody, that is, the documented trail revealing who handled the evidence, when, and how.

This chain guarantees that the data hasn't been tampered with. Tools such as X1 Social Discovery are vital to preserving social media evidence, as they permit investigators to capture, analyse, and store online content in a way that retains its integrity and is compliant with legal standards, ensuring the evidence can be used in legal proceedings.

> *The following video introduces X1 Social Discovery tutorial (https://www.youtube.com/watch?v=cT1wZhVRHmc)*

3.6 Common Tools for Social Network Investigation

Many tools are used for social network investigation. In this study, the discussion will be on the following social network investigation tool. These are Maltego, Hunchly, Social-Analyser, and GeoFeedia.

- **Maltego**

Maltego is a data mining and link analysis tool used in cybercrime investigations and intelligence collection. It assists in visualizing relationships between entities such as people, phone numbers, email addresses, and social media accounts, for easy online interaction tracking.

For instance, if investigators want to trace how a cluster of cybercriminals are linked through emails or domains, Maltego can create a graph that visually signifies these connections, permitting investigators to recognize key players or concealed connections within a network.

- **Hunchly**

Hunchly tool assists investigators in capturing and documenting web pages when browsing, guaranteeing that online evidence is gathered and conserved for legal purposes. It automatically saves every page visited, making it easier to track online activities and verify the authenticity of the data gathered.

For instance, if someone is investigating a suspect's social media activity, Hunchly archives the pages visited, captures screenshots, and stores metadata, guaranteeing the evidence can be presented in court.

- **Social-Analyser**

Social Analyser is an open-source tool that assists investigators in analysing and observing social media profiles transversing several platforms. It explores public profiles founded on usernames, giving insights into online conduct and relations.

For instance, if you want to track a user's existence across diverse social networks, Social Analyser assists you collect data on their actions, making it a useful tool for law enforcement and digital investigators.

- **GeoFeedia**

Geofeedia is a position-based social media observing tool that assists users track, analysing, and recording social media content based on geographic locations. It permits investigators to observe social media posts from precise areas, which can be supportive through events or for tracking events in targeted regions.

For instance, throughout a public protest or an emergency, Geofeedia can capture life posts from that area, giving treasured insights into on-the-ground situations for law enforcement or journalists.

3.7 Case Study and Practical Demonstration

A case study is a comprehensive scrutiny of a specific real-world scenario, individual, or organisation to prove a concept, analyse outcomes, or derive lessons. A practical demonstration, on the other hand, entails displaying how something works or applying a concept in a real-life setting, often through hands-on activities or simulations, to strengthen knowledge of the subject matter.

- **Case Study Examples**

On 19th January 2022, the Nigerian Police Force (NPF) arrested 11 alleged members of a prolific cybercrime network as part of a national police operation coordinated with INTERPOL.

Arrested by officers of the NPF Cybercrime Police Unit and INTERPOL's National Central Bureau (NCB) in Nigeria, many of the suspects are thought to be members of 'SilverTerrier', a network known for Business Email Compromise (BEC) scams that have harmed thousands of companies globally (https://www.interpol.int/en/News-and-Events/News/2022/Nigerian-cybercrime-fraud-11-suspects-arrested-syndicate-busted).

On 25th May 2022, the cybercrime unit of the Nigeria Police Force in conjunction with INTERPOL arrested a 37-year-old Nigerian man for purportedly running an immense cybercrime maneuver that used phishing campaigns and business email compromise systems to scam companies and individual victims (https://cyberscoop.com/silverterrier-interpol-nigeria-bec/).

- **Practical Demonstration**

Start Maltego OSINT by entering the suspect's email address or username into the search engine for associated social media accounts. Maltego will map out links to other accounts, showing relationships and interactions across platforms. Once accounts are identified, analyse the suspect's posts, friends, and activities to infer patterns or intentions.

To collect geolocation data, analyse posts with embedded metadata or tagged positions. Maltego will picture these links on a map, for easy tracing of the suspect's digital footprint across various locations.

The use of Maltego is outlined in this video, https://www.youtube.com/watch?v=onHHXNDnkrs

Discussion

Provide examples of successful investigations where social media played a pivotal role and discuss the impact of laws like the General Data Protection Regulation (GDPR) on these practices.

3.8 Summary

Online Social Networks (OSNs) serve as vital platforms where cybercrimes such as identity theft, cyberstalking, and online fraud occur. Through the application of Open-Source Intelligence (OSINT) methods and tools such as Maltego, Hunchly, and GeoFeedia, investigators analyse suspect activity and collect valuable information. Appropriately conserving evidence from social networks, employing legal procedures and tools, guarantees that it remains admissible in court, supporting more efficient cybercrime investigations.

In this unit, the students have learned how online social networks can assist as tools for cybercrime investigations, involving methods for tracking digital footprints, preserving evidence, and utilizing specialized investigative tools.

3.9 References/Further Readings/Web Resources

Bokolo, B. G., & Liu, Q. (2024). Artificial Intelligence in Social Media Forensics: A Comprehensive Survey and Analysis. Electronics, 1 3(9), 1671. https://doi.org/10.3390/electronics13091671

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2023). Cybercrime and Digital Forensics: An Introduction (4th ed.). Routledge.
https://cyberscoop.com/silverterrier-interpol-nigeria-bec/
https://www.interpol.int/en/News-and-Events/News/2022/Nigerian-cybercrime-fraud-11-suspects-arrested-syndicate-busted

Kumar, A., Singh, R., & Singh, R. K. (2019). Social media analytics for cybercrime investigation: A review. International Journal of Engineering and Advanced Technology, 8(5), 3457-3463.

Maras, M.-H. (2016). *Computer forensics: Cybercriminals, laws, and evidence* (2nd ed.). Jones & Bartlett Learning. Link to the book:https://www.elsevier.com/books/investigating-with-maltego/roth/978-1-59749-627-7

Roth, D. (2019). *Investigating with Maltego: The open-source intelligence and forensics tool for networks and beyond*. Syngress. Link to the book: https://www.elsevier.com/books/investigating-with-maltego/roth/978-1-59749-627-7

3.10 Possible Answers to Self-Assessment Exercise(s)

Answers to SAEs

1. What are Online Social Networks (OSNs), and why are they significant in the context of cybercrime investigations?

Answer
Online Social Networks (OSNs) are platforms where users create profiles, share content, and interact with others. Examples include Facebook, Twitter, and Instagram. They are significant in cybercrime investigations because they offer a wealth of publicly accessible information, which can be used to track digital footprints, identify connections between suspects, and analyse suspicious activities, thereby aiding law enforcement in solving cybercrimes like cyberstalking, fraud, and identity theft.

2. What is Open-Source Intelligence (OSINT), and how is it utilized in cybercrime investigations?

Answer
Open-Source Intelligence (OSINT) involves collecting data from publicly available sources like social media profiles, websites, and forums. In cybercrime investigations, OSINT techniques help gather relevant data about suspects, such as geolocation, email addresses, and their online behavior. Tools like Maltego and Hunchly are often used to map out connections and visualize the information found during the investigation.

3. Why is tracking digital footprints important in cybercrime investigations, and what tools can assist in this process?

Answer
Tracking digital footprints is crucial because it allows investigators to trace a suspect's online activities, interactions, and locations, helping to establish patterns or connections to criminal behavior. Tools such as Maltego and GeoFeedia assist in tracking these footprints by collecting data from various platforms and visualizing relationships between online entities, making it easier to follow the digital trail.

4. What is the importance of preserving evidence in social network investigations, and how can tools like Hunchly help in this process?

Answer
Preserving evidence ensures that data collected from social networks is admissible in court. Capturing screenshots, collecting metadata, and using software to maintain the chain of custody are key steps in this process. Hunchly helps investigators capture and preserve webpages in a legally sound manner, automatically saving screenshots and metadata, which is essential for maintaining the integrity of the evidence.

5. How do tools like Maltego and Social-Analyser assist in OSINT investigations related to social networks?

Answer
Maltego maps relationships and connections between online accounts, helping investigators visualize and trace social media interactions. Social-Analyser helps automate the collection of social media profiles and activity for further analysis. Both tools are essential in efficiently identifying patterns and connections during an investigation, providing insights that may not be immediately visible through manual searches.

Unit 4 Cyber Terrorism

Unit Structures

4.1 Introduction

So far, the focus of our discussion has been on cybercrime generally. I have also discussed the strategies of cybercrime perpetrators in the unit before this very one.

Cyber terrorism refers to the use of computer networks and Internet technologies to disrupt, damage, or destroy critical infrastructure, computer systems, or electronic data, with the intention of intimidating or coercing individuals, organisations, or governments for political, ideological, or religious purposes. It combines traditional terrorism with cybercrime, posing a significant threat to national security, global stability, and digital safety.

4.2 Learning Outcome

By the end of this unit, you will be able to:

- discuss the motives and the global impacts of cyber terrorism.

4.3 Cyber Terrorism

4.3.1 What is Cyber Terrorism?

Cyber Terrorism is typically described as a planned attack with political motives against information systems, programs, and data that either threatens violence or leads to violence. This can involve cyber-attacks that instill fear in the population of a country, state, or city by damaging or disrupting critical infrastructure necessary for social, economic, political, and business functions.

These Cyber Terrorist acts are carried out using computer servers, devices, and networks that are accessible on the public Internet. Government networks and other restricted networks are often targeted. Other potential targets include the banking industry, military installations, power plants, air traffic control centers, and water systems.

The U.S. Federal Bureau of Investigation (FBI) defines cyberterrorism as a planned, politically motivated attack against information, computer systems, programs, and data that results in violence against noncombatant targets by subnational groups or clandestine agents. According to the FBI, a cyberterrorist attack is a form of cybercrime specifically intended to cause physical harm.

Some organisations and experts consider less harmful attacks as acts of cyberterrorism, particularly when they are meant to disrupt or advance the attacker's political goals. The North Atlantic Treaty Organisation (NATO) defines cyberterrorism as a cyberattack that utilizes computer or communication networks to cause enough destruction or disruption to instill fear or intimidate a society towards an ideological objective.

- **Terrorist Tactics Worldwide**

Terrorist groups use six main types of tactics: hijackings, kidnappings, bombings, assassinations, armed assaults, and barricade-hostage incidents. The tactics chosen depend on the group's objectives and organisational capabilities.

- **Methods Used for Cyber Terrorism**

Cyber Terrorist groups aim to create chaos, disrupt critical infrastructure, support political activism, or cause physical harm. They use methods like Advanced Persistent Threat (APT) attacks to gain network access and steal data from organisations in industries like

defense, manufacturing, healthcare, and finance. They also use computer viruses, worms, and malware to target IT control systems in utilities, transportation, power grids, government departments, and military systems.

4.3.2 Examples of Cyber Terrorism

As I have explained earlier, cyber terrorist attacks system by unauthorised gaining (hacking) of access into computer systems or devices. These attackers often go after critical infrastructure and governments. Hacking seeks to gain unauthorised access to steal critical data, often from institutions, governments and businesses.

The chief among hackers' weapons is the ransomware which is, a type of malware aimed at holding data or information systems hostage (usually via encryption) until the victim pays the ransom. Some ransomware attacks also exfiltrate data.

Phishing attacks is also a dangerous weapon for committing cyber terrorism. Phishing attack attempts to collect information through a target's email, using that information to access systems or steal the victim's identity

- **Disruption of Major Websites**

The intent is to stop traffic to websites that serve many users and whose disruption might create widespread public inconvenience.

- **Unauthorised Access**

Attackers often aim to gain access to certain systems or to modify communications that control military systems or other critical technology.

- **Disruption of Critical Infrastructure Systems**

Threat actors try to disable or disrupt cities, cause a public health crisis, endanger public safety or cause massive panic and fatalities, for example, by targeting a water treatment plant, causing a regional power outage, or disrupting an oil or gas pipeline.

- **Cyberespionage**

Rogue governments or nation-states carry out or sponsor cyberespionage attacks to spy on rival nations and gather sensitive, secret, or confidential intelligence, such as troop locations or military strategies.

4.4 Strategies to Defend Against Cyber Terrorism

In the past, cyberterrorism mostly targeted government entities. But now, businesses and other organisations are also becoming targets, so they must implement extensive cybersecurity measures and vigilance to counter cyberterrorism. For one, they must ensure that all Internet of Things devices are secured and inaccessible via public networks. To protect against ransomware and similar attacks, they must backup systems regularly and implement continuous monitoring techniques. They must also use firewalls, antivirus software, and antimalware to protect their systems from these attack vectors. Companies must also implement controls and IT security policies to protect business data. This includes limiting access to sensitive data and enforcing strict password and authentication procedures, like two-factor or multifactor authentication.

Self-Assessment Exercise(s) 1

1. What are the benefits of defending against cyber terrorism?

4.4.1 International Efforts to Combat Cybercrime and Cyber Terrorism

The National Cyber Security Alliance is a partnership between the public and private sectors that aims to raise awareness about cybersecurity and create a safer, more connected world. It plays a role in the global fight against cybercrime and cyber terrorism.

The U.S. Department of Homeland Security (DHS) also works with other government agencies and private partners to share information on potential terrorist threats and ways to protect national security. They also collaborate on counterterrorism strategies that can be used by the U.S. and other countries to combat the growing issue of cyber terrorism.

The Council of Europe's Convention on Cybercrime, also known as the Budapest Convention on Cybercrime, is the first international treaty designed to address cybercrime and cyberwarfare. It encourages countries to work together, share information, and align their laws. As of

2024, 69 countries have ratified the Convention, with 22 more invited to join. The United Nations is in the process of developing a significant cybercrime treaty that will cover various topics, such as international cooperation, law enforcement access to digital evidence, and procedural safeguards. The final text and negotiations for this treaty are expected to be completed by 2024.

4.4.2 Signs to Notice on a Hacked System

Email, social media or some other type of online service, there are many things which can alert you to the fact that someone else is accessing your account. Things to look out for include:
Being locked out of the account is an obvious indication that something has gone wrong. Logins or attempted logins from strange locations or at unusual times

Self-Assessment Exercise(s) 2

1. Why is cyber terrorism a global concern?

4.5 Defence against Cyber Terrorism

Cyber defense is a coordinated act of resistance that guards information, systems, and networks against cyber-attacks by implementing protective procedures such as firewalls, network detection and response (NDR), endpoint detection and response (EDR) to identify, analyse, and report incidents that occur within a network.

A cyber security strategy is an action plan detailing how a business will protect itself from cyber threats. An effective cyber security strategy provides a blueprint on what to prioritize to have a safe and secure cyber environment. Organisations or individuals guard against attacks by the following defence strategies.

- **Update Devices**

The operating systems and apps on the devices you use should all be updated. These updates will install the latest security fixes. If you have it installed, you can run a scan with up-to-date antivirus software. This is not usually necessary for phones and tablets.

- **Contact Service Provider**

If you can't access your account, go to the account provider homepage, and find a link to their help or support pages. These will detail the account recovery process. If you can't find what you need on the service's website, try a search engine like Google or Bing. For example, 'Facebook account hacked.' Then follow the links to the service's own advice.

- **Prevent Email Account Hacking**

Once you've regained control, check your email filters and forwarding rules. It is a common trick for the person hacking an account to set up an email forwarding rule that sends a copy of all your received emails to them. Information on how to do this should be found in your provider's help pages

- **Change passwords**

Once you have confirmed there are no unwanted email forwarding rules in place, change the passwords on all accounts which have the same password as the hacked account. Then change the passwords for all the other accounts that send password reminders/resets to the hacked account

- **Set up 2-Factor Authentication**

This provides an extra layer of protection against your account being hacked in the future - see guide on using 2-factor authentication (external link)

- **Notify Contacts**

Cyber Terrorism is a major worldwide issue because it can cause extensive harm, disrupt essential infrastructure, and create instability in countries. The interconnected nature of our digital world makes it a prime target for individuals looking to create chaos and instill fear.

- **When an Account cannot be Recovered**

You may choose to create a new one. Once you've done this, it's important to notify your contacts that you are using a new account. Make sure to update any bank, utility services or shopping websites with your new details.

Discussion

Considering the increasing reliance on digital infrastructure, how do you define cyber terrorism, and discuss the key challenges in differentiating between cyberterrorism and other forms of cybercrime, particularly in terms of legal definitions, intent, and global countermeasures?

4.6 Summary

As you have learnt in this unit, the discussion about cyberterrorism shows that these attacks have various motives, such as political extremism, financial gain, and state-sponsored sabotage. Cyberterrorism has a wide-reaching impact, affecting national security, critical infrastructure, and public trust in digital systems.

To combat this threat, governments, organisations, and individuals need to take a comprehensive approach by investing in strong cybersecurity measures, promoting international cooperation, and sharing intelligence. It is also important to address the root causes of radicalization and promote digital literacy to prevent the spread of cyberterrorist ideologies.

You have learnt from this unit cyber terrorism and its negative consequences on peace, economy and security of the world.

4.7 References/Further Readings/Web Resources

Adeyemi, O. O. (2023). *Cyber Terrorism in Nigeria: A Threat Assessment*. University Press of Nigeria.

Aransiola, J. O., & Asindemade, S. O. (2023). Understanding Cybercrim e Perpetrators and the Strategies They Employ in Nigeria. Cyberp sychology, Behavior, and Social Networking.

Blakemore, B. (2016). Cyberspace, cybercrime and cyber terrorism. In Policing cyber hate, cyber threats and cyber terrorism (pp. 5-20). Routledge.

Cohen, D. (2014). Cyber terrorism: Case studies. In Cyber Crime and Cyber Terrorism Investigator's Handbook (pp. 165-174). Syngress.

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2018). *Cybercrime and Digital Forensics: An Introduction* (3rd ed.). Routledge.

Jangada Correia, V. (2022). An explorative study into the importance of defining and classifying cyber terrorism in the United Kingdom. SN Computer Science, 3(1), 84.

Saint-Claire, S. (2011). Overview and Analysis on Cyber Terrorism. School of Doctoral Studies European Union Journal, (3).

Zerzri, M. (2017). The Threat of Cyber Terrorism and Recommendations for Countermeasures. Cyber Terror., 6.

4.8 Possible Answers to Self-Assessment Exercise(s)

Answers to SAEs

1. *Cyberterrorism is the use of _____ to disrupt, damage, or destroy critical infrastructure, computer systems, or electronic data.*

Answer: Computer networks and internet technologies

2. One of the primary motivations of cyberterrorists is to _____ fear and intimidation in the public.

Answer: Inspire

3. Cyberterrorists often use techniques such as _____ and malware to carry out their attacks.

Answer: Phishing

4. The goal of cyberterrorism is often to _____ the stability and security of a nation or organisation.

Answer: Compromise

5. What are the benefits of defending against cyber terrorism?

Answer:

Protecting against cyberterrorism is crucial for safeguarding critical infrastructure, economic stability, and national security. By successfully stopping and reducing cyberattacks, countries can keep their citizens safe from physical harm, financial loss, and a decline in trust in government institutions. Furthermore, strong cybersecurity promotes international collaboration, encourages innovation, and upholds democratic values amid digital dangers.

MODULE 3 COMPUTER CYBERCIME INVEESTIGATIONS

Module Introduction

In Module 2, you have learned how to conduct basic static and dynamic analysis of malware using static code analysis, in Unit 2, and dynamic program tracing techniques in Unit 3. In this module, I will take you through the advance concepts of malware analysis such as program pointer variable analysis and program data flow analysis.

This module is classified into the following two (2) units:

Unit 1 Computer Network and Forensic Investigations
Unit 2 Digital Evidence Collection and Evaluation

In each unit, I will explore a particular topic in detail and highlight self-assessment exercises at the end of the unit. Finally, I highlight resources for further reading at the end of each unit.

Unit 1 Computer Network and Forensic Investigations

Unit Structures

1.1 Introduction

In this unit, I will take through computer and network forensics as a specialised field that employs scientific methods to recover, preserve, and analyse digital evidence from computer systems and networks. Computer and network forensics play a pivotal role in investigating cybercrimes, intellectual property theft, fraud, and other digital-related offenses. Experts can uncover crucial information, reconstruct events, and provide admissible evidence in legal proceedings.

1.2 Learning Outcome

By the end of this unit, you will be able to:

- discuss how to perform forensic analysis using a simple forensic tool.

1.3 Computer Network and Forensic Investigations

1.3.1 Network Forensics

Traditional forensic science is skilled at examining physical evidence in criminal cases, but digital forensics is more challenging. It involves using specialised tools and techniques to uncover evidence and insights. Network forensics, which focuses on investigating activity across interconnected networks, was developed to meet these specific needs

- **What is Network Forensic?**

The term "forensics" refers to using science and technology to investigate and establish facts in criminal or civil court cases. Forensics involves applying scientific knowledge to analyse evidence and present it in court. Network forensics is a subset of digital forensics that focuses on examining networks and the traffic passing through them to identify potential malicious activities. This includes investigating networks involved in spreading malware, stealing credentials, or carrying out cyber-attacks.

As the Internet has grown, so have cybercrimes, making network forensics increasingly important due to the rise of network-based services like the World Wide Web and emails. By utilising network forensics, all data such as messages, file transfers, emails, and web browsing history can be recovered and reconstructed to reveal the original transactions. While the payload of the top-layer packet may end up on the disk, the envelopes used to deliver it are only captured in network traffic. Therefore, the network protocol data containing each conversation is often highly valuable.

- **Computer Forensic and Network Forensics**

Digital or computer forensics involves investigating and analysing data that is stored on digital devices. This process includes carefully

examining digital devices to assist in investigations related to cyberbullying and data breaches.

Network forensics, a subset of digital forensics, focuses on investigating data that is in motion and deals with volatile and dynamic information. It is essential for understanding the interactions and activities that take place between devices on a network.

1.3.2 Forensic Investigations

Forensics refers to the scientific techniques used to solve crimes. Forensic investigation involves gathering and analysing physical evidence related to the crime to determine the suspect. Investigators examine fluids, fingerprints, residue, electronic devices, and other technology to understand how the crime occurred. This is a broad definition, as there are various types of forensics.

1.3.3 Types of Forensic Investigation

There are 11 types of forensic investigation. I will list and explain them below:

- **Forensic Accounting/Auditing**

Forensic Accounting / Auditing Forensic accounting investigations help victims of fraud or financial crimes. Also known as financial investigations, this type of analysis uses intelligence-gathering techniques, accounting, business, and communication skills to provide evidence to attorneys involved in criminal and civil investigations.

Investigators sift through a large amount of relevant data to identify irregularities or illegal financial practices. Crimes investigated can range from tax evasion to theft of company assets, as well as insurance claims and large payouts. Forensic accounting services may include:

i. Searching for hidden assets
ii. Calculating lost wages
iii. Tracing misappropriated funds
iv. Conducting fraud investigations

- **Computer or Cyber Forensics**

Forensic Computer or Cyber Forensics Computer investigations, similar to electronic discovery (e-discovery), recover data from computers and hard drives to solve crimes or find evidence of misconduct. Investigators

can uncover activities such as the sale of black-market goods, fraud, and trafficking.

Common situations that require computer investigations include divorce cases, wrongful termination, employee Internet abuse, unauthorized disclosure of corporate information, and other illegal internet activities. Forensic computer investigations can retrieve information from cell phones and hard drives, including emails, browsing history, downloaded files, and even deleted data. One of the earliest cases where computer forensics led to a conviction involved messages exchanged in an online chat room.

- **Crime Scene Forensics**

Crime Scene Forensics Crime scene investigations involve documenting and collecting physical evidence found at a crime scene to solve crimes or determine if a crime has occurred. This type of investigation also includes analysing the collected evidence to ensure its credibility and relevance.

Various crime scene investigators specialise in different areas, such as ballistics experts who study ammunition trajectories and match bullets to potential firearms, and odontologists who focus on teeth and bite-marks to identify missing persons or victims of mass disasters.

- **Forensic Archaeology**

Forensic Archaeology Forensic archaeology focuses on human remains that are severely decomposed. The main focus is on clues that can be gathered from bones, including using carbon dating to determine their age. These clues can sometimes help establish the cause of death. In cases of mass graves or large casualties, forensic archaeologists can identify victims using facial reconstruction software.

- **Forensic Dentistry**

Forensic Dentistry Forensic dentists play a crucial role in cases where a victim cannot be identified through other means or when a suspect bites a victim. Teeth have unique patterns, and the marks left behind can identify a suspect or victim. The shape of the jaw can also provide information about age, gender, and DNA can be extracted from teeth similar to bone marrow and hair. Even if the victim was not bitten, physical evidence found at a crime scene, such as bite marks on a pencil or a half-eaten apple, can reveal someone's identity.

- **Forensic Entomology**

Forensic Entomology Forensic entomology involves studying insects found at a crime scene. Whether alive or dead, these bugs can provide information about the location of a crime, whether the victim was drugged, and the time of death. Some insects are specific to certain areas, so finding them on a body can indicate if the body was moved. The presence of larvae in a body can also indicate how long a victim has been deceased. In cases that are not murders, insects can still be useful in identifying untreated wounds in abuse cases or determining the origin of illegally imported goods like cannabis.

- **Forensic Graphology**

Forensic Graphology Forensic graphologists analyse handwriting on various documents like ransom notes, poison pen letters, and suicide notes. While age and gender cannot be determined solely from handwriting, it can provide insights into the writer's state of mind when the note was written. Handwriting can reveal information about mood, motivation, integrity, intelligence, and emotional stability. The style of writing, size, slant, and weight can all provide clues about the writer. Phrases and slang used can also indicate location and motive. Forensic graphologists are also used to verify the authenticity of documents like insurance claims or police statements.

- **Forensic Pathology**

Forensic Pathology Forensic pathologists are responsible for determining the cause of death, especially in cases where foul play is suspected. They conduct autopsies to examine both the external and internal aspects of the victim. External signs like bruises, bullet wounds, or signs of asphyxia can provide clues, while internal examinations of organs and stomach contents can help determine if the death was a suicide, murder, or natural causes.

- **Forensic Psychology**

Forensic Psychology Forensic psychology focuses on understanding the motivations behind a perpetrator's actions. Before considering how to catch a suspect, forensic psychologists analyse why the crime was committed. They look at sources of extreme stress in the perpetrator's life that may have led to violent actions. They also examine the crime scene to determine if the act was impulsive or premeditated. Forensic psychologists can also assess the mental state of suspects and victims, even in cases of suspected suicide.

- **Forensic Science**

Forensic Science: Forensic science encompasses all scientific processes involved in solving crimes. This includes Deoxyribonucleic Acid (DNA) analysis, toxicology, serology, ballistics, and the collection, storage, and analysis of physical evidence like fibers and bodily fluids. Forensic scientists play a crucial role in providing reliable and accurate evidence for criminal cases, and the field is constantly evolving with advancements in technology.

- **Forensic Toxicology**

Forensic Toxicology: Forensic toxicology focuses on studying toxic substances, environmental chemicals, and poisons. This includes drug testing for job applications and analysing both illegal and legal drugs using bodily samples like urine, blood, or hair. Forensic toxicologists study how these substances are absorbed, distributed, and eliminated by the body, as well as their effects, which can be crucial in cases of murder.

Self-Assessment Exercise(s) 1

1.	Why do you need digital forensic investigation?

1.3.4 Digital Forensic Tools

Digital forensics software is a set of tools specifically designed to investigate digital devices. These tools enable the retrieval, examination, and analysis of information stored in electronic devices like computers, cell phones, and tablets. The main objective is to gather evidence for legal purposes or to aid in investigations. In today's digital world, forensics software is essential. These tools facilitate in-depth investigations that can uncover hidden information for various purposes. Some digital forensics tools are:

1. Autopsy: Autopsy is an open-source digital forensics software that gives investigators a full base to work from.
2. FTK (Forensic Toolkit): FTK is a top-tier forensic analysis tool with extensive data-gathering and analysis features.
3. VIP 2.0 (Video Investigation Portable): VIP 2.0 is an all-in-one video forensics software for CCTV DVR/NVR drives developed by SalvationDATA. It can efficiently recover deleted, lost, or fragmented videos and perform rapid and effective forensics.
4. Sleuth Kit: The primary functions of the free and open-source Sleuth Kit are file system analysis and data carving.

5. Cellebrite UFED: Cellebrite UFED specialises in mobile forensics software for data acquisition and analysis.
6. X-Ways Forensics: When it comes to forensic investigations and data retrieval, nobody does it better than X-Ways Forensics.
7. Volatility: An open-source memory digital forensics software, Volatility specialises in analysing RAM dumps.
8. Magnet AXIOM: Magnet AXIOM is a well-known digital forensics software with exceptional evidence-gathering, analysis, and reporting capabilities.
9. OS Forensics: OS Forensics analyses many facets of computers to help with digital investigations.
10. Paladin Forensic Suite: A Linux-based digital forensics software platform, Paladin includes various tools for analysis and data recovery.

1.3.5 How to Choose Digital Forensic Tools

In choosing the right forensic tool for digital investigation, there are some factors to consider. Some of these factors are explained in sections 3.5.1 to 3.5.5.

- **Considerations for Law Enforcement**

Commercial Organizations, and Incident Response Different industries have specific needs. Law enforcement must strictly enforce compliance and evidence preservation. In the business world, data security and efficiency are top priorities, and incident response teams need to act quickly to identify and fix problems. Choosing the right digital forensics software that aligns with company goals and regulatory norms requires a deep understanding of these unique requirements.

- **Scope**

Individual Tools vs. Suite of Tools decide whether to purchase individual tools or a suite for the task at hand. While individual programs have their uses, using multiple tools together is often more efficient. A forensics software suite is a comprehensive solution that can address multiple problems simultaneously, speeding up the investigation process.

- **Privacy and Security Concerns**

Confidentiality and security are crucial in digital forensics. The chosen digital forensics software should prevent unauthorized access to data during the review process. Look for defensive features like encryption, authentication, and write-protection to enhance the tool's security.

Before purchasing, ensure the product has been thoroughly tested for safety flaws and complies with all relevant regulations and standards.

- **Open-Source vs. Proprietary Tools**

Expertise vs. User-Friendly Features While open-source software may require more technical expertise to maintain and update, its flexibility and customization options are often worth the learning curve. Proprietary systems typically have user-friendly interfaces and support to help new users get started quickly. Consider factors such as team skill level, the need for unique capabilities, and preference for free or paid maintenance when making this decision.

- **Pricing Information**

Open-source tools, Basic Suites, and Large Organizations Tool selection are heavily influenced by available funds. Open-source software is often free but may require a high level of expertise to use effectively. Basic suites with minimal features can be costly for small businesses. Larger companies may be able to afford more sophisticated suites with additional features and support. Consider cost, functionality, and return on investment when choosing a tool.

 **Discussion**

What are the key stages involved in conducting a computer-based cybercrime investigation, and discuss how legal and technical challenges, such as evidence preservation and chain of custody, impact the effectiveness of these investigations?

 **1.4 Summary**

In this unit, I explored pointers, pointer expression and how they reference a memory location. I also explored how to perform pointer analysis on a program.

In this unit, you have learned the different forensics. You have also learned forensic investigation methods, including an understanding of pointer variables and how to perform pointer analysis to identify the object in a (malware) program that a pointer variable refers to.

1.5 References/Further Readings/Web Resources

Adeyemi, I. R., Razak, S. A., & Azhan, N. A. N. (2012). Identifying critical features for network forensics investigation perspectives. arXiv preprint arXiv:1210.1645.

Adeyemi, O. O. (2023). *Cybercrime Investigations: A Nigerian Perspective*. University Press of Nigeria.

Casey, E. (2019). *Handbook of Digital Forensics and Investigation* (2nd ed.). Academic Press.

Khan, S., Gani, A., Wahab, A. W. A., Shiraz, M., & Ahmad, I. (2016). Network forensics: Review, taxonomy, and open challenges. Journal of Network and Computer Applications, 66, 214-235.

Lazzez, A. (2013). A survey about network forensics tools. Int. J. Comput. Inf. Technol, 2(1).

Qureshi, S., Tunio, S., Akhtar, F., Wajahat, A., Nazir, A., & Ullah, F. (2021). Network Forensics: A Comprehensive Review of Tools and Techniques. International *Journal of Advanced Computer Science and Applications, 12(5).*

Sibe, R. T., & Kaunert, C. (2024*). Cybercrime, Digital Forensic Readin ess, and Financial Crime Investigation in Nigeria*. Springer.

Sikos, L. F. (2020). Packet analysis for network forensics: A comprehensive survey. *Forensic Science International: Digital Investigation, 32, 200892*.

1.6 Possible Answers to Self-Assessment Exercise(s)

Answers to SAEs

1. What is the primary goal of computer forensics?

Answer:
To collect, preserve, and analyse digital evidence to aid in investigations and legal proceedings.

2. Which of the following is a key principle of network forensics?

Answer:
To ensure the integrity and authenticity of evidence through proper documentation and chain of custody.

3. What is the term for the process of recreating a digital crime scene to understand the sequence of events?

Answer:
Reconstruction.

4. What type of forensic analysis involves examining network traffic and logs to identify potential security incidents?

Answer:
Network traffic analysis.

5. Why do you need digital forensic investigation?

Answer:
Digital forensic investigation is necessary for a multitude of reasons in today's digital age. With cybercrimes on the rise, businesses and individuals alike need to have the tools to investigate and prevent potential security breaches. Digital forensics can uncover crucial evidence in legal proceedings, help identify data breaches, and even assist in recovering lost or corrupted information.

By analysing and interpreting digital evidence, investigators can track down cybercriminals, protect sensitive data, and ensure the integrity of digital systems. Whether it's investigating a hacking incident or recovering deleted files, digital forensic investigation plays a vital role in maintaining trust and security in our increasingly technology-dependent world. So, it's important to have experts who can navigate through complex digital landscapes with precision and expertise.

Unit 2 Digital Evidence Collection and Evaluation

Unit Structures

2.1 Introduction

In this unit, I will take you through digital evidence collection. This will show you what constitutes digital evidence, various types of digital evidence, methods of collection and how they are collected. Finally, I will take you through digital evidence evaluation.

2.2 Learning Outcome

By the end of this unit, you will be able to:

- examine how to collect digital evidence and know how to evaluate them.

2.3 Digital Evidence Collection and Evaluation

2.3.1 Digital Evidence

Digital devices are prevalent in today's world, making communication easy both locally and globally. While most people think of computers, cell phones, and the Internet as the main sources of digital evidence, any technology that processes information can be used for criminal activities. For instance, hand-held games can transmit encoded messages between criminals, and even modern household appliances like

refrigerators with built-in TVs could be used to store, view, and share illegal content.

Responders must be able to identify and seize potential digital evidence. Digital evidence refers to valuable information and data for an investigation that is stored on, received, or transmitted by an electronic device. This evidence is obtained when electronic devices are confiscated and secured for analysis. Digital evidence is hidden, like fingerprints or DNA evidence, easily crosses jurisdictional borders, it can also be altered, damaged, or destroyed with minimal effort.

There are various sources of digital evidence, but for this publication, the focus is on three main forensic categories of devices where evidence can be found: Internet-based, stand-alone computers or devices, and mobile devices. Each of these areas has distinct processes, tools, and concerns for gathering evidence, and different types of crimes are more likely to involve one type of device over another.

- **Electronic evidence**

Electronic evidence in cyber forensics refers to any digital data that is valuable for investigating cybercrimes or legal matters. This can include files, logs, emails, metadata, and internet history. This evidence is typically found on computers, mobile devices, networks, and cloud storage, and it plays a crucial role in uncovering illegal activities such as hacking or fraud. The process of collecting electronic evidence involves using forensic tools to capture data without making any changes to it. Preservation is also important to maintain the integrity and authenticity of the evidence for legal proceedings. Analysing electronic evidence helps extract relevant information, such as identifying communication patterns or unauthorized access. It is essential to follow legal compliance, including adhering to chain of custody protocols, to ensure the evidence is admissible in court. Ultimately, electronic evidence is used to understand cyber incidents and effectively extract information about hacking activities.

Self-Assessment Exercise(s) 1

1. Why do we need digital evidence?

2.3.2 Digital Evidence Collection

In the early 1980s, personal computers became more popular and accessible to the general population. This increase in computer usage also led to a rise in criminal activities involving computers, such as fraud and software cracking. As a result, the field of computer forensics emerged to investigate these crimes. Today, digital evidence collection

is used to investigate a wide range of crimes, including fraud, espionage, and cyberstalking. Forensic experts use their knowledge and techniques to analyse digital artifacts found on seized devices like computers, Solid-State Drives (SSDs), hard disks, Compact Disc Read-Only Memory (CD-ROMs), Universal Serial Bus (USB) flash drives, as well as electronic documents such as emails, images, chat logs, and phone logs.

- **Challenges of Digital Evidence Collection**

Collecting digital evidence in cybersecurity presents many challenges due to the constantly changing technology landscape and the emergence of new issues, such as the inconsistency of cyber environments. One major challenge is data volatility, where crucial evidence can be easily altered or lost if not captured promptly from running systems. Accessing encrypted or protected data also poses difficulties, requiring more than just passwords but decryption methods and legal authorization.

Maintaining data integrity and authenticity is crucial, as any changes during collection can make the evidence inadmissible in court. Legal and jurisdictional issues often arise when evidence spans multiple regions or countries, leading to the need for compliance with various legal frameworks and international cooperation. The rapid pace of technological advancement means forensic tools and methodologies must continuously evolve to address new forms of digital evidence and cyber threats, necessitating ongoing training and adaptation by cybersecurity professionals.

2.3.3 Process of Digital Evidence Collection

The main processes involved in digital evidence collection are given below:

Data collection: In this process, data is identified and collected for investigation.
Examination: In the second step the collected data is examined carefully.

Analysis: In this process, different tools and techniques are used, and the collected evidence is analysed to reach some conclusion.

Reporting: In this final step all the documentation and reports are compiled so that they can be submitted in court.
Digital Evidence Collection Process

- **Types of Collectible Data**

Computer investigators and experts analysing seized devices must identify potential pieces of evidence and determine the type of evidence they are seeking to effectively conduct their search Crimes involving computers can vary widely, from trading illegal items like endangered animals to intellectual property theft and personal data breaches. Deleted files on the computer may be lost, encrypted, or damaged. Investigators should be knowledgeable about different tools, methods, and software to ensure data integrity during the recovery process. There are two types of data that can be collected in a computer forensics investigation:

Persistent data: It is the data that is stored on a non-volatile memory type storage device such as a local hard drive the external storage devices like SSDs, HDDs, pen drives, CDs, The. The data on these devices is preserved even when the computer is turned off.

Volatile data: It is the data that is stored on a volatile memory type storage such as memory, registers, cache, RAM, or it exists in transit, that will be lost once the computer is turned off or it loses power. Since volatile data is evanescent, an investigator must know how to reliably capture it

- **Types of Evidence**

Collecting the shreds of evidence is important in any investigation to support the claims in court. Below are some major types of evidence.

i. Real Evidence: This type of evidence includes physical items like flash drives, hard drives, and documents. An eyewitness account can also be considered real evidence.
ii. Hearsay Evidence: This type of evidence consists of out-of-court statements made to prove the truth of a matter in court.
iii. Original Evidence: This type of evidence involves statements made by individuals who are not testifying witnesses. It is used to prove that a statement was made, not necessarily to prove its truth.
iv. Testimony: Testimony occurs when a witness swears an oath in court and provides their statement. The evidence presented should be authentic, accurate, reliable, and admissible, as it can be challenged in court.

2.3.4 Evaluation

The integrity of digital evidence is crucial for it to be considered reliable and admissible in court. To ensure its probative value, digital evidence

must be reliable, complete, and authentic. Therefore, maintaining integrity during and after forensic investigations is a top priority for forensic investigators. The goal is to identify the most suitable and effective security measures to safeguard the integrity of digital evidence. This assessment should adhere to globally recognized standards like ITSEC (Information Technology Security Evaluation Criteria) and CC (Common Criteria for Information Technology Security Evaluation).

2.3.5 Digital Evidence Evaluation Criteria

The ITSEC evaluation criteria are used to assess security methods that protect the integrity of digital evidence. The ITSEC model includes nine sub-criteria that are used to evaluate integrity protection mechanisms across three categories.

- **Security Properties**

This section focuses on the security properties of a security method, including data confidentiality, data integrity, and non-repudiation.

- **Time Binding**

This criterion evaluates the ability of a security method to associate time with processed data. This is crucial for digital evidence to determine the validity and sequence of events during forensic investigations.

- **Accuracy**

Accuracy assesses the precision of a security method through experiments testing errors, time, and verification. The experiments involved processing 25MB of data with 20 files, repeated 15 times for each security method.

- **Strength of Mechanisms**

This criterion measures the ability of a mechanism to withstand potential attacks.

- **Computational Efficiency**

This criterion evaluates the computational efficiency of a security method when processing data using various file sizes.

- **Binding of Functionality**

This criterion examines how well a security method can work with another to provide stronger security solutions.

- **Ease of Use, Complexity or Simplicity**

This criterion assesses the ease of use, complexity, and simplicity of security methods.

- **Identification and Authentication**

This criterion focuses on functions that establish and verify claimed identities.

- **Attacks and Vulnerability Assessment**

This criterion defines a database of potential vulnerabilities and attacks that a security method can detect, resist, and encounter.

 **Discussion**

What are the key challenges and best practices involved in the collection and evaluation of digital evidence during a cybercrime investigation, and explain how improper handling of digital evidence can affect the admissibility and integrity of the evidence in court?

 **2.4 Summary**

In this unit, I discussed digital evidence collection as it involves the identification, acquisition and preservation of digital data from various sources to support investigations and legal proceedings. I also explored the processes of handling and documenting to ensure the integrity and authenticity of the evidence. Finally, I discussed the methods of collection and evaluation. I will take you through cyber law and countermeasures in the next unit.

In this unit, you have learned what is meant by digital evidence and how to collect It. You have also learnt the challenges of digital evidence and the evaluation of digital evidence.

2.5 References/Further Readings/Web Resources

Adeyemi, O. O. (2023). *Digital Evidence Collection and Analysis in Nigeria*. University Press of Nigeria.

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2017). *Cybercrime and Digital Forensics: An Introduction* (3rd ed.). Routledge.

Setya, A., & Suganda, A. (2022). Design of Digital Evidence Collection Framework in Social Media Using SNI 27037: 2014. JUITA: Jurnal Informatika, 10(1), 127-137.

Sibe, R. T., & Kaunert, C. (2024). Cybercrime, Digital Forensic Readine ss, and Financial Crime Investigation in Nigeria. Springer.

Sin, J. M., & Son, H. R. (2019). Dealing with the problem of collection and analysis of electronic evidence. International Journal of Electronic Security and Digital Forensics, 11(3), 363-377.

Singh, C., Tara, H., & Mishra, A. (2022). Digital Evidence Collection. In Manual of Crime Scene Investigation (pp. 145-156). CRC Press.

Vaghela, R., Gowda, V. D., Taj, M., Arudra, A., & Chopra, M. (2024). Digital Evidence Collection and Preservation in Computer Network Forensics. In Handbook of Research on Innovative Approaches to Information Technology in Library and Information Science (pp. 42-62). IGI Global.

2.6 Possible Answers to Self-Assessment Exercise(s)

Answers to SAEs

1. What is the first step in the digital evidence collection process?

Answer:
Identification: Identifying the source and location of potential digital evidence.

2. What is the purpose of hashing in digital evidence collection?

Answer:

To ensure the integrity and authenticity of evidence by creating a unique digital fingerprint, allowing for verification of the evidence's integrity during analysis and court proceedings.

3. What is the difference between "best evidence" and "secondary evidence" in digital evidence evaluation?

Answer:
"Best evidence" refers to the original digital evidence, while "secondary evidence" refers to a copy or reproduction of the original evidence. In legal proceedings, best evidence is preferred, but secondary evidence may be accepted if properly authenticated.

4. Why do we need digital evidence?

Answer:
Digital evidence is typically utilised during the incident response process to identify if a breach has occurred, determine the root cause and threat actors, eliminate the threat, and supply evidence for legal teams and law enforcement authorities.

MODULE 4 CYBER LAW AND COUNTERMEASURES

Module Introduction

In this module, I will take you through cyber law and countermeasures, the legal frameworks, regulations, and technological measures designed to prevent, detect, and respond to cyber threats. I will also take you through data protection, privacy laws, cybersecurity policies and standards.

This module is classified into the following four (4) units:

Unit 1 Introduction to Cyber Law
Unit 2 Cyber Law Applications
Unit 3 Cyber Law Framework in Nigeria
Unit 4 Challenges and Opportunities for Cyber Law and Countermeasure Enforcement in Nigeria

In each unit, I will explore a particular topic in detail and highlight self-assessment exercises at the end of the unit. Finally, I highlight resources for further reading at the end of each unit.

Unit 1 Introduction to Cyber Law

Unit Structure

1.1 Introduction

In this unit, I will take through what cyber law implies, I will explain the importance and benefits of cyber laws. I will also take you through the types of cyber laws from both national and international perspective.

1.2 Learning Outcomes

By the end of this unit, you will be able to:

- discuss the meaning of cyber laws
- mention and discuss the types of cyber laws
- explain the importance and the benefits of cyber laws

1.3 Introduction to Cyber Law

1.3.1 What is Cyber Laws?

Cyber Law, also known as Internet law or digital law, refers to the legal rules and regulations that govern digital activities. It encompasses various issues such as online communication, e-commerce, digital privacy, and the prevention and prosecution of cybercrimes. With the Internet being an essential part of our daily lives, cyber law plays a crucial role in ensuring the orderly and secure functioning of digital spaces.

1.3.2 Importance of Cyber Law

The importance of cyber law lies in its ability to address and regulate the complex challenges that arise from the widespread use of technology. Cyberlaw establishes a framework for protecting individuals and organisations from cyber threats, safeguarding the privacy and security of digital transactions, and setting standards for ethical and legal behavior in cyberspace. As the digital landscape continues to evolve, the significance of cyber law becomes increasingly evident, serving as a foundation for the responsible and lawful use of digital resources.

Self-Assessment Exercise(s) 1

1.	How can Rogue Conditional Jump technique be resolved?

1.4 Benefits of Cyber Law

Code obfuscation transforms program code to a form that makes it significantly less human-readable while retaining its functionality. Code obfuscation adds a substantial level of complexity and resilient, that is, it is difficult to reverse. Common code obfuscation transformations are control flow transformation and data transformation.

1.4.1 Protection against Cybercrimes

Cyber laws serve as a deterrent by providing legal options and penalties for different cybercrimes. This proactive strategy helps reduce unlawful online behaviors and creates a more secure digital space for both individuals and businesses.

1.4.2 Data Privacy

Protecting individuals' digital information is a top priority addressed by cyber laws. These regulations ensure that organisations handle personal data responsibly, establishing trust in digital transactions and interactions.

1.4.3 E-commerce Regulation

The legal framework provided by cyber laws is crucial for regulating e-commerce. It defines rules for online transactions, contracts, and consumer protection, fostering a fair and secure online marketplace.

1.4.4 Intellectual Property Protection

Cyber laws play a crucial role in protecting intellectual property rights in the digital domain. These laws prevent unauthorized use and distribution of digital content, encouraging innovation and creativity by safeguarding intellectual labor.

1.4.5 Cybersecurity Standards

Cyber laws significantly contribute to establishing cybersecurity standards. By requiring organisations to implement measures for protecting their networks and systems, these laws address the evolving landscape of cyber threats.

1.5 Types of Cyber Law

There are several types of Cyber Law

i. Privacy Laws
Privacy laws focus on protecting individuals' personal information from unauthorized access and use. They establish guidelines for responsible handling of personal data by organisations, ensuring individuals' privacy rights are upheld.

ii. Cybercrime Laws
Cybercrime laws define and penalize various cybercrimes, ensuring legal consequences for offenders. These laws deter individuals from engaging in illegal online activities and provide a legal framework for prosecuting cybercriminals.

iii. Intellectual Property Laws
Intellectual property laws in the digital domain protect patents, copyrights, and trademarks from unauthorized use. They provide a legal foundation for creators and innovators to protect their digital assets.

iv. E-commerce Laws
E-commerce laws regulate online business transactions, defining rules for contracts, transactions, and consumer protection. These laws contribute to establishing a secure and fair online marketplace.

v. Cyber Defamation Laws
Cyber defamation laws address libel and slander in the digital space. They provide legal remedies for individuals or entities whose reputations may be tarnished by false or damaging information circulated online.

vi. Cybersecurity Laws
Cybersecurity laws establish standards for securing digital systems and data. These laws mandate organisations to implement measures to protect against cyber threats, contributing to the overall resilience of digital infrastructure.

vii Social Media Laws
Social media laws address legal issues related to social media platforms, including user rights and content regulations. These laws aim to balance freedom of expression and prevent online abuse or misinformation.

viii **Cyber Contracts and E-signature Laws**
Governing the validity and enforceability of contracts formed online, cyber contracts and e-signature laws provide legal certainty for electronic transactions. They facilitate the growth of online commerce by ensuring the legal recognition of digital agreements.

ix **International Cyber Laws**
With the increasing prevalence of cross-border cybercrimes, international cyber laws address the need for cooperation between nations. These laws facilitate collaboration in investigating and prosecuting cybercriminals operating across borders.

x **Data Breach Notification Laws**
Mandating organisations to inform individuals and authorities in the event of a data breach enhances transparency and accountability. These laws ensure prompt action in response to security incidents, minimizing the potential impact on individuals and businesses.

Discussion

How do existing cyber laws address the rapidly evolving nature of cybercrime, and discuss the effectiveness of current legal frameworks and countermeasures in combating cybercrime on a global scale, particularly in terms of international cooperation and enforcement challenges?

1.6 Summary

In this unit, you have learned how to identify and understand the legal framework governing online activities, including intellectual property rights, data protection, and cybercrime. You have also learned the ethical implications of technology and its impact on society.

In this unit, I explored the types of cyber law. I also explained how to differentiate between various legal frameworks governing online activities, such as intellectual property rights, data protection laws, leading to a deeper understanding of users' rights and responsibilities in the digital age.

1.7 References/Further Readings/Web Resources

Adeyemi, O. O. (2023). *Cyber Law and Countermeasures in Nigeria*. University Press of Nigeria.

Chander, H., & KAUR, G. (2022). Cyber laws and IT protection. PHI Learning Pvt. Ltd.

Chawki, M., Darwish, A., Tyagi, S., & Abdelwahed, A. (2015). *Cybercrime, Digital Forensics and Jurisdiction* (1st ed.). Springer.

Dewani, N. D., Khan, Z. A., Agarwal, A., Sharma, M., & Khan, S. A. (Eds.). (2022). Handbook of research on cyber law, data protection, and privacy. IGI Global.

Roguski, P. (2020). Application of international law to cyber operations: a comparative analysis of states' views.

Sibe, R. T., & Kaunert, C. (2024). *Cybercrime, Digital Forensic Readin ess, and Financial Crime Investigation in Nigeria*. Springer.

Tokan, K., Amin, M. E., Syaufi, A., & Mispansyah, M. (2024). Protecting Digital Society: Policies for Criminalising Illegal Smartphone Applications Through Cyber Law Frameworks. West Science Law and Human Rights, 2(03), 175-183.

Ubaydullayeva, A. (2023). Artificial intelligence and intellectual property: navigating the complexities of cyber law. *International Journal of Law and Policy, 1(4).*

1.8 Possible Answers to Self-Assessment Exercise(s)

Answers to SAEs

1. Cyber Law primarily focuses on addressing legal issues related to _____ and the internet.

Answer:
technology

2. Cyber Law is important because it regulates online transactions and protects individuals' _____ rights.

Answer:
digital

3. Some examples of areas covered by Cyber Law include _____, data privacy, and cybercrime.

Answer:
intellectual property

4. How can Rogue Conditional Jump technique be resolved?

Answer:
Disassemblers contain specific command that deal with ambiguous situations such as commands that inform the disassembler, such as IDA and OllyDbg, whether a certain byte is code or data. To properly disassemble the rogue code, you can inform the disassembler that the code is a data not code. This will enable the disassembler to produce correct code. Therefore, the rogue byte is ignored by the disassembler.

Unit 2 Cyber Law Applications

Unit Structures

2.1 Introduction

In this unit, I will take you through the concept of cyberlaw application both in general areas and specific areas. I will also take you through how the cyber law regulates activities in emerging Technology.

2.2 Learning Outcomes

By the end of this unit, you will be able to:

- learn cyber law application on cybercrime related issues
- identify violation of law and the benefits of cyber laws

2.3 Cyber Law Applications

2.3.1 General Area of Cyber Law Application

Cyberlaw covers a wide range of legal issues related to the Internet, technology, and digital communication. Some general areas of cyber law application include privacy protection, cybersecurity, intellectual property rights, online harassment, and e-commerce regulations. For example, cyber laws govern how personal information is collected and stored online, ensuring that companies follow regulations to protect user data.

Additionally, cybersecurity laws establish requirements for organisations to implement measures to prevent hacking and data

breaches. Intellectual property rights in cyberspace involve protecting original creations like music, artwork, and software from unauthorized use or distribution. Online harassment laws address cyberbullying or defamation on social media platforms. E-commerce regulations set guidelines for online transactions and consumer protection. Overall, cyber law plays a crucial role in regulating the vast digital landscape we navigate daily.

2.3.2 Specific areas of cyber law application

Malware uses a variety of techniques to scan for indications that a debugger is attached. This includes using the Windows API, manually checking memory structure for debugging artefacts and searching the system for residue left by a debugger. Debugger detection is the most common way that malware performs anti-debugging.

- **Social media**

Social media platforms need regulation for content, privacy, and liability. Legal frameworks are needed for the development, use, and liability of Artificial Intelligence.

- **Blockchain technology**

Blockchain technology faces legal challenges with cryptocurrency and smart contracts.

- **Internet of Things (IoT)**

Internet of Things (IoT) devices require privacy, security, and liability measures. Overall, cyber laws establish a legal structure for the digital era, aiming to balance innovation with the protection of individuals, businesses, and society.

2.3.3 Application of cyber law on emerging technologies

Cyber law is the legal framework that regulates online activities. With the rise of new technologies such as artificial intelligence, blockchain, and the Internet of Things, it is increasingly important to have regulations in place to protect individuals and businesses from potential risks. Privacy concerns, data breaches, and intellectual property rights are some of the issues that cyber law addresses in relation to these new technologies.

Additionally, there is the ongoing challenge of keeping up with rapid advancements in technology and updating laws accordingly. Therefore, cyber law on emerging technologies plays a vital role in ensuring a safe and secure digital environment for all parties involved.

Discussion

In what ways are cyber law applications evolving to address new challenges posed by emerging technologies and cyber threats, and discuss the implications of these changes for individuals, organisations, and law enforcement in maintaining cybersecurity and protecting digital rights?

3.4 Summary

In this unit, you have learned that cyber law plays a crucial role in regulating online activities, protecting digital rights, and addressing legal challenges arising from the Internet, such as intellectual property infringement, cybercrime, and privacy violations.
You have also learned that by providing a legal framework for online interactions, cyber law can help to maintain order, security and fairness in the digital world.

In this unit, I explored the cyber law framework in Nigeria and discussed how it provides a robust foundation for regulating cyber activities, protecting citizens' rights, and promoting digital economic growth. I also discussed that the effectiveness of cyber law applications depends on continuous review and update to address emerging cyber threats.

7.0 References/Further Readings/Web Resources

Adeyemi, O. O. (2023). *Cyber Law and Countermeasures in Nigeria*. University Press of Nigeria.

Alese, B. K., Thompson, A. F., Owa, K. V., Iyare, O., & Adebayo, O. T. (2014). Analysing issues of cyber threats in Nigeria. In Proceedings of the World Congress on Engineering (Vol. 1, pp. 2-4).

Chawki, M., Darwish, A., Tyagi, S., & Abdelwahed, A. (2015). *Cybercrime, Digital Forensics and Jurisdiction* (1st ed.). Springer.

Eboibi, F. E. (2020). Concerns of cyber criminality in South Africa, Ghana, Ethiopia and Nigeria: rethinking cybercrime policy

implementation and institutional accountability. Commonwealth Law Bulletin, 46(1), 78-109.

Ibekwe, C. R. (2015). The Legal Aspects of Cybercrime in Nigeria: An Analysis with the UK Provisions.

Karake-Shalhoub, Z., & Al Qasimi, L. (2010). *Cyber law and cyber security in developing and emerging economies.* Edward Elgar Publishing.

Sibe, R. T., & Kaunert, C. (2024*). Cybercrime, Digital Forensic Readin ess, and Financial Crime Investigation in Nigeria*. Springer.

2.4 Possible Answers to Self-Assessment Exercise(s)

1. What is the primary application of Cyber Law in electronic commerce?

a. To regulate online business transactions and protect consumer rights
b. To promote online freedom of speech and expression
c. To enforce intellectual property rights in digital works
d. To govern online privacy and data protection

Answer:
'a' To regulate online business transactions and protect consumer rights

2. Which of the following is an application of Cyber Law in cybersecurity?

a. To develop artificial intelligence and machine learning algorithms
b. To conduct cybercrime investigations and digital forensics
c. To establish incident response and disaster recovery plans
d. To create secure online payment systems and protocols

Answer:
'c' To establish incident response and disaster recovery plans.

Unit 3: Cyber Law Framework in Nigeria

Unit Structure

3.1 Introduction

In this unit, I will take you through the concept of cyber law framework in Nigeria. I will explore the legal provisions that regulate online activities, protect digital rights, and address cybercrime within the country for your better understanding.

3.2 Learning Outcomes

By the end of this unit, you will be able to:

- identify different cyber law frameworks in Nigeria and their specific area of employment.

3.3 Cyber Law Frameworks in Nigeria

3.3.1 General Cyber Law Framework

Nigeria's cyber law is mainly based on the Cybercrimes (Prohibition, Prevention, etc.) Act of 2015. This law offers a complete legal structure for dealing with cybercrimes and related matters in the country.

3.4 Provisions of the Cybercrimes Act

The Cybercrimes Act provides a comprehensive legal framework to combat cybercrime, outlining specific offenses, penalties, and procedures for investigation and prosecution.

3.4.1 Definition of Cybercrimes

The Act outlines various cybercrimes, including cyberstalking, cyberbullying, identity theft, computer fraud, and cyber terrorism.

3.4.2 Penalties

It prescribes penalties for different cybercrimes, ranging from fines to imprisonment**.**

3.4.3 Law Enforcement Powers

The Act grants law enforcement agencies powers to investigate cybercrimes and gather electronic evidence.

3.4.4 Protection of Critical Infrastructure

It emphasizes the protection of critical national information infrastructure.

3.4.5 Cybersecurity Measures

The Act encourages organisations to implement cybersecurity measures.

3.4.6 Other Relevant Laws

While the Cybercrimes Act is the cornerstone, other laws also contribute to the cyber law framework in Nigeria. Evident Act provides rules for

the admissibility of electronic evidence in court, copyright act to protect intellectual property rights in the digital age, and data protection regulation to protect personal data.

 **Discussion**

How effective is the current cyber law framework in Nigeria in addressing the challenges of cybercrime, and discuss the role of regulatory bodies and enforcement agencies in ensuring compliance with these laws while promoting cybersecurity and protecting citizens' rights?

 **3.5 Summary**

In this unit, you have learned how that cyber law framework in Nigeria provides a robust foundation for regulating cyber activities. You have also learned Nigeria can enhance its trust in digital transactions and align with global best practices.

In this unit, I have delved into a detailed explanation of the cyber law framework, providing you with the information needed to understand the world of cyber regulations. This knowledge will help you protect individual rights and create a safe digital environment.

 **3.6 References/Further Readings/Web Resources**

Adeyemi, O. O. (2023). *Cyber Law and Countermeasures in Nigeria*. University Press of Nigeria.

Chawki, M., Darwish, A., Tyagi, S., & Abdelwahed, A. (2015). *Cybercrime, Digital Forensics, and Jurisdiction* (1st ed.). Springer.

Nte, N. D., Enoke, B. K., & Teru, V. A. (2022). A comparative analysis of cyber security laws and policies in Nigeria and South Africa. Law Research Review Quarterly, 8(2), 233-258.

Olayemi, O. J. (2014). A socio-technological analysis of cybercrime and cyber security in Nigeria. *International Journal of Sociology and Anthropology, 6(3), 116.*

Saulawa, M. A. A., & Abubakar, M. K. (2014). Cybercrime in nigeria: An overview of cybercrime act 2013. JL Pol'y & Globalization, 32, 23.

Sibe, R. T., & Kaunert, C. (2024). Cybercrime, Digital Forensic Readine ss, and Financial Crime Investigation in Nigeria. Springer.

Yusuf, C. N. I. B. (2014). Cyber threats and national security in nigeria: Challenges and options. NDC E-JOURNAL, 13(2), 131-146.

3.7 Possible Answers to Self-Assessment Exercise(s)

Answers to SAEs

Why is cyber law relevant in today's digital age?

Answer:
Cyber law is relevant because it provides a legal framework to address the unique challenges and risks associated with online activities, such as cybercrime and data breaches.

How does cyber law impact businesses and organisations?

Answer:
Cyber law impacts businesses and organisations by requiring them to implement robust cybersecurity measures, protect customer data, and comply with regulations.

What role does cyber law play in protecting individual rights?

Answer:
Cyber law plays a crucial role in protecting individual rights by establishing guidelines for online privacy, data protection, and freedom of expression.

Unit 4: Challenges and Opportunities for Cyber Law and Countermeasure Enforcement in Nigeria

Unit Structures

4.1 Introduction

In this unit, I will take you through the concept of cyber law enforcement, countermeasures and its complex landscape. I will also take you through the challenges and opportunities in cyber law enforcement.

4.2 Learning Outcome

By the end of this unit, you will be able to:

- learn how effective enforcement of cyber law can balance between protecting national security, promoting innovation, and safeguarding individual rights and freedoms in the face of increasingly sophisticated cyber threats

4.3 Challenges and Opportunities for Cyber Law and Countermeasure Enforcement in Nigeria

4.3.1 Cyber law challenges in Nigeria

Nigeria has made progress in creating laws to deal with cybercrimes, but there are still some obstacles to be overcome.

- **Rapid Evolution of Technology**

i. Outdated Legislation: The rapid pace of technological advancement often outstrips the ability of lawmakers to create and update legislation.
ii. Emerging Cybercrimes: New forms of cybercrime emerge constantly, making it difficult for the law to keep up.

- **Enforcement Challenges**

i. Limited Expertise: There is a shortage of skilled professionals in cybercrime investigation and prosecution.
ii. Lack of Resources: Law enforcement agencies often lack the necessary resources, such as equipment and funding, to effectively combat cybercrime.
iii. Cross-Border Issues: Cybercrimes often transcend national borders, making international cooperation essential but challenging to achieve.

- **Digital Literacy and Awareness**

i. Low Digital Literacy: A significant portion of the population lacks digital literacy, making them vulnerable to cyberattacks and scams.
ii. Lack of Awareness: Many people are unaware of their rights and responsibilities in the digital space, hindering prevention efforts.

- **Economic Impact**

i. Financial Losses: Cybercrimes result in significant financial losses for individuals, businesses, and the government.
ii. Reputational Damage: Cyberattacks can damage the reputation of businesses and countries.

- **Balancing Security and Privacy**

i. Privacy Concerns: Striking a balance between ensuring cybersecurity and protecting individuals' privacy rights is a complex challenge.
ii. Data Protection: Developing a robust data protection framework is crucial but requires careful consideration of various interests.

- **Corruption and Impunity**

i. Corruption: Corruption within the law enforcement and judicial system can hinder the effective prosecution of cybercrimes.
ii. Impunity: Cybercriminals often operate with impunity due to weak enforcement and lenient penalties.

4.3.2 Cyber law opportunities in Nigeria

Nigeria, like many other countries, is experiencing a surge in digital transformation, making cyber law a rapidly expanding field. The increasing reliance on technology has led to a corresponding increase in cybercrimes, data breaches, and online disputes. This creates a significant demand for legal professionals with expertise in cyberlaw.

- **Cybersecurity Lawyer**

i. Advising organisations on data protection and privacy compliance.
ii. Developing and implementing cybersecurity policies and procedures.
iii. Responding to cyberattacks and data breaches.
iv. Representing clients in cybercrime investigations and litigation.

- **Cybercrime Investigator**

i. Investigating cybercrimes such as fraud, identity theft, and online harassment.
ii. Collecting digital evidence and preparing legal cases.
iii. Collaborating with law enforcement agencies.

- **Cybersecurity Consultant**

i. Assessing organisations' cybersecurity risks and vulnerabilities.
ii. Developing and implementing cybersecurity strategies.
iii. Providing training and awareness programs

- **Cyber Law Researcher**

i. Conducting research on emerging cyber law issues.
ii. Analysing existing laws and proposing legislative reforms.
iii. Contributing to academic publications and conferences.

- **Cybersecurity Compliance Officer**

i. Ensuring compliance with data protection regulations (e.g., Nigeria Data Protection Regulation).
ii. Conducting regular audits and risk assessments.
iii. Implementing data protection policies and procedures

4.4 Creation of Advisory Council on Cybercrime Law

The Cybercrime Advisory Council (CAC) was created by the Cybercrimes Act 2015 to develop policy guidelines for preventing and fighting cybercrimes, as well as promoting cyber security in Nigeria. The Cybercrime Advisory Council is made up of representatives from the Ministries, Departments, and Agencies listed in the First Schedule of the Cybercrimes Act 2015.

- **Advisory Council Mandate**

The cybercrimes act 2015 under section 43, has given the council the mandates to:

i. formulate and provide general policy guidelines for the implementation of the provisions of the Cybercrimes Act 2015.

ii. promote Graduate Traineeships in Cybersecurity and Computer and Network Security Research and Development

iii. establish a program to award grants to institutions of higher education to establish Cybersecurity Research Centers to support the development of new Cybersecurity defences, techniques and processes in the real-world environment.

iv. advise on measures to prevent and combat computer related offences, cybercrimes, threats to national cyberspace and other cyber security related issues.

v. create an enabling environment for members to share knowledge, experience, intelligence, and information regularly and shall provide recommendations on issues relating to the prevention and combating of cybercrimes and the promotion of cyber security in Nigeria.

- **Advisory Council Representation**

The Cybercrime Advisory Council consists of representatives from relevant Ministries, Departments, and Agencies (MDAs) for proper coordination of Cybercrime laws. The under-listed MDAs are well represented:

1. Internet Service Providers Association of Nigeria
2. Nigeria Prisons Service
3. Non-Governmental Organisation with Focus on Cyber Security
4. Galaxy backbone
5. Nigeria Security and Civil Defence Corps
6. Defence Headquarters
7. Federal Ministry of Justice
8. Nigeria Insurance Association.
9. Nigeria Customs Service
10. National Space Management Agency
11. Association of Telecommunications Companies of Nigeria
12. Nigerian Communications Commission
13. Central Bank of Nigeria
14. National Agency for the Prohibition of Traffic in Persons
15. Economic and Financial Crimes Commission
16. Nigeria Immigration Service
17. Federal Ministry of Finance
18. Department of State Services
19. Nigeria Police Force
20. Defence intelligence Agency
21. Office of the National Security Adviser
22. Nigerian Information Technology Development Agency
23. National Identity Management Commission
24. Federal Ministry of Trade and Investment
25. National Intelligence Agency
26. Ministry of Foreign Affairs
27. Nigerian Stock Exchange
28. Nigeria Bankers Committee
29. Independent Corrupt Practices Commission

 **Discussion**

What are the key challenges facing the enforcement of cyber laws and countermeasures in Nigeria, and discuss the potential opportunities for strengthening these frameworks to enhance cybersecurity and protect citizens from cyber threats? Consider factors such as technological

advancements, regulatory gaps, and the role of public awareness in your response.

4.5 Summary

In this unit, you have learned how that the challenges and opportunities for Cyber Law highlight the need for a dynamic and adaptive legal framework that can address the evolving nature of cyber threats and technologies. You have also learned that by embracing these challenges and opportunities, cyber law can strengthen the solutions to cybercrimes in Nigeria.

In this unit, I explained the challenges and opportunities of cyber law in Nigeria. I also discussed the economic impact of cyber law. I also enumerated all the regulatory agencies and stake holders in cyber law matters in Nigeria.

4.6 References/Further Readings/Web Resources

Adalikwu, C. (2012). Challenges and opportunities in the implementation of electronic commerce: The case of Nigeria. African Journal of Business Management, 6(46), 11495.

Adeyemi, O. O. (2023). *Cyber Law and Countermeasures in Nigeria*. University Press of Nigeria.

Ajayi, E. F. G. (2016). Challenges to enforcement of cyber-crimes laws and policy. Journal of Internet and Information Systems, 6(1), 1-12.

Chawki, M., Darwish, A., Tyagi, S., & Abdelwahed, A. (2015). *Cybercrime, Digital Forensics, and Jurisdiction*. Springer.

Frank, I., & Odunayo, E. (2013). Approach to cyber security issues in Nigeria: challenges and solution. International Journal of Cognitive Research in science, engineering and education, 1(1), 100-110.

Ibrahim, Y. A., Ishaya, A. O., Yusuf, M., Nancy, I., Bijik, H. A., & Aiyedogbon, S. F. (2024, April). Cybersecurity and Cybercrimes in Nigeria: An Overview of Challenges and Prospects. In 2024 International Conference on Science, Engineering and Business

for Driving Sustainable Development Goals (SEB4SDG) (pp. 1-7). IEEE.

Oni, S., Berepubo, K. A., Oni, A. A., & Joshua, S. (2019, April). E-government and the challenge of cybercrime in Nigeria. In 2019 sixth International Conference on eDemocracy & eGovernment (ICEDEG) (pp. 137-142). IEEE.

4.7 Possible Answers to Self-Assessment Exercise(s)

1. What is the primary role of a cybersecurity lawyer?

Answer:
To provide legal counsel and representation to clients on cybersecurity-related matters, such as data breaches and cyber attacks.

2. What skills are required to be a successful cybercrime investigator?

Answer:
Strong technical skills, analytical mindset, and knowledge of cybercrime laws and regulations.

3. What skills are required to be a successful cyber law researcher?

Answer:
Strong research skills, analytical mindset, and knowledge of legal and technical concepts.