Cybercrime- Motivations, Modes, and Emerging Trends with Nigeria as a Case Study

The thesis was submitted in partial fulfilment of the requirements for the award of the degree of Doctor of Philosophy of the University of Portsmouth

Supervisor: Dr Victoria Wang
Second Supervisor: Chris Lewis

Institute of Criminal Justice Studies
Faculty of Humanities and Social Sciences
University of Portsmouth
May 2021
Abstract

This study aims to investigate, empirically, the motivation, mode of operation and emerging trends of cybercrime, using Nigeria as a case study. The academic discussion of cybercrime is relatively new, and there is limited amount of literature that focuses on in-depth holistic research into cybercrime in the context of an individual country. This study addresses these issues by exploring the subject area through the perceptions of stakeholders. It was conducted using key criminological concepts to examine the unique social conditions of Nigeria and their contribution to cybercrime.

A review of the current general literature on cybercrime was first conducted. The qualitative method was adopted in this research because it integrates effectively with the phenomenology philosophy preferred in the research. With the selected method, this study adopted three methods: documentary analysis, focus groups and interviews. The documentary analysis explored the evolution, contributing factors, sub-culture and government intervention in cybercrime. Overall, twenty-eight participants from Nigeria were involved in this research, with three participating in the focus group and twenty-five in the interviews. In the focus group, key current cybercrime characteristics were retrieved. The findings from the focus group and interviews were discussed with the literature to present a holistic view.

Overall, this research identified five core contributions to knowledge in the area of motivation and mode of operation. They include; i) new motivations which are emerging outside financial gain including altruism, creativity, revenge and political principles; ii) modus operandi of cybercrime is becoming much less predictable; iii) the organisation of cybercrime is decentralised without any control or rigid structure; iv) rural-urban migration contributes to the complexity and number of crimes in developing countries; and v) a sociotechnical and multidisciplinary approach to cybercrime is key for effective regulation. These findings demonstrate the present situation of cybercrime in numerous countries.

The findings highlighted core emerging trends in the conduct of cybercrime worldwide. These trends include; i) cybercrime in some developing countries can dominate the world; ii) the development and strengthening of a transnational economy through uncontrolled collaborations among cybercriminals; iii) rise in professionalisation of cybercrime and cybercrime-as-a-service; and iv) becoming accepted and legitimised as a way of life in some countries. The growth of these trends will differ among countries. The difference will be subject to the strength of cybersecurity and regulation in individual countries.
There are core implications for criminology theories from these findings. The implications include: i) no theory can adequately explain cybercrime; ii) criminologists are trying to fit the theories to the crime; and iii) the future of cybercrime further provides significant concern for the theories. Thus, it is important to develop new theories or amend previous theories to reflect the technological realities of cybercrime.

In conclusion, this research proposes a more social approach to combating cybercrime rather than the current criminal and technical approach. This is crucial because motivations reflect the result of challenging social conditions on young citizens. Further, there is the need for an integrated approach that focuses on cybercrime prevention rather than investigation. This research has contributed to the body of knowledge in this subject area by presenting in-depth knowledge of the evolution, current state, and the expected trend of cybercrime from the Nigerian case study.
Acknowledgement

I appreciate the input, contribution, and impact of those that have supported me during this PhD programme and the overall completion of the thesis. My profound gratitude goes to my supervision team including Dr Victoria Wang, Chris Lewis, and Barry Loveday for their professional and valuable advice and critical contributions to achieving the desired quality and standard expected for a Doctoral thesis. Their hard work and suggestions continually spurred the need for improvement and diligence in the entire process.

My family deserved special recognition because of their immense support during this process. I wish to thank my beloved wife, Adeola Apantaku for her steadfast support and increasing encouragement through the entire research. Her support through two childbirths in the period of study remained highly crucial to the completion of this research. I would like to mention the support of my three kids Irawooluwa, Ooreoluwa, and Idununoluwa for inspiring daddy during this process. I would like to thank my parents for their immense support and moral encouragement to achieve this dream. I appreciate my parents-in-law and my siblings for their continual assistance in difficult times.

It is essential to mention the contribution of gatekeepers and contact persons in participant recruitment. I am grateful to all the research participants for their time and willingness to contribute to this research. Furthermore, the moral and emotional support from specific individuals in Portsmouth cannot be underestimated, including Mr Bill Moore, Bolaji, Williams, Musa, Uthman, and Fola. Some families that have helped during this programme include Mr and Mrs Adeniran, Mr and Mrs Famuditi, Mr and Mrs David and Mr and Mrs Oladejo.

Overall, my utmost gratitude is to Almighty God for giving me good health and the ability to conclude this study.
Statement of Declaration

I declare that this thesis is an original academic report conducted by me and has not been presented for any previous degree. I declare that all work contained in this thesis was composed by myself or elsewhere otherwise stated. The research was purely my work with an explicit acknowledgement of every contribution and collaboration in the report. Every supporting resource and literature were duly referenced.

Word Count: 56, 804
### Key Terms

<table>
<thead>
<tr>
<th>Key Terms</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blacklisting</td>
<td>The process where the internet address is added to the list of malicious and unacceptable sources of request or electronic communication on the web.</td>
</tr>
<tr>
<td>Cartel</td>
<td>A group of perpetrators that controls an industry, market or sector.</td>
</tr>
<tr>
<td>Corruption Perception Index (CPI)</td>
<td>The index, which ranks 180 countries and territories by their perceived levels of public sector corruption according to experts and businesspeople</td>
</tr>
<tr>
<td>Craigslist</td>
<td>An American advertisement website where sections are classified into different sections, including community services, housing for sale and others.</td>
</tr>
<tr>
<td>Cyberbullying</td>
<td>The use of electronic communication or the internet for bullying another individual through threatening and intimidation messages.</td>
</tr>
<tr>
<td>Cybercafé</td>
<td>A location or cafe where internet access is provided to the public.</td>
</tr>
<tr>
<td>Cybercriminal</td>
<td>Any individual that perpetrates criminal activities on the internet.</td>
</tr>
<tr>
<td>Cyberfraud</td>
<td>Cyber fraud is any criminal activity involving computers and networks of deliberate deception for unfair or unlawful gain that occurs online (Singleton and Singleton, 2010)</td>
</tr>
<tr>
<td>DDOS</td>
<td>Acronym for Distributed Denial of Service. A type of cyberattack where multiple computer systems are used to target a particular internet server/service so legitimate users would not be able to access.</td>
</tr>
<tr>
<td>Dumps</td>
<td>Examination dumps are topics and questions that were released online by individuals that have taken the examination.</td>
</tr>
<tr>
<td>EFCC</td>
<td>The Economic and Financial Crimes Commission (EFCC) is a Nigerian law enforcement agency that investigates financial crimes, including money laundering and advance fee fraud.</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>FBI</td>
<td>An acronym for the Federal Bureau of Investigation, the domestic security and intelligent service for the United States.</td>
</tr>
<tr>
<td>FUT Minna</td>
<td>It is the Federal University of Technology in Minna, Niger State of Nigeria. It was the first Nigerian University to conduct a degree course on cybersecurity.</td>
</tr>
<tr>
<td>Galaxy Backbone</td>
<td>Galaxy Backbone is the information technology and shared services provider of the Federal Government of Nigeria.</td>
</tr>
<tr>
<td>Gang</td>
<td>An organised group of criminals.</td>
</tr>
<tr>
<td>GRQS</td>
<td>It is an acronym of the Get Rich Quick Syndrome. It involves individuals wishing and aggressively looking for money either legally or illegally.</td>
</tr>
<tr>
<td>IC3</td>
<td>IC3 represents the Internet Crime Complaint Centre at the Federal Bureau of Investigation at the United States of America. It accepts online Internet crime complaints from either the actual victim or from a third party to the complainant.</td>
</tr>
<tr>
<td>Industry</td>
<td>The entire practice of cybercrime in Nigeria.</td>
</tr>
<tr>
<td>Maga</td>
<td>It is a colloquial name given to cyber fraud victims</td>
</tr>
<tr>
<td>MMM</td>
<td>Mavrodi Mondial Moneybox which is an online Ponzi scheme that was conducted in Nigeria.</td>
</tr>
<tr>
<td>MoJ</td>
<td>It is the Federal Ministry of Justice representing the legal arm of the Nigerian Government. They bring cases that are initiated by the government before the Judiciary.</td>
</tr>
<tr>
<td>M-Pesa</td>
<td>It means “m-money” in Swahili and is the global brand for Vodafone's Mobile Money service. It is a mobile money service that originates from Kenya.</td>
</tr>
<tr>
<td>MTN</td>
<td>MTN is one of the leading telecommunication service providers in Nigeria and other African countries.</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>NASS</strong></td>
<td>An acronym for the National Assembly of Nigeria. It consists of the House of Representatives and House of Senate.</td>
</tr>
<tr>
<td><strong>NCC</strong></td>
<td>The Nigerian Communications Commission is the independent regulatory authority for the telecommunications industry in Nigeria.</td>
</tr>
<tr>
<td><strong>NITDA</strong></td>
<td>National Information Technology Development Agency (NITDA) implements the Nigerian Information Technology Policy and coordinates general IT development in the country.</td>
</tr>
<tr>
<td><strong>NPF</strong></td>
<td>It is the acronym for the Nigerian Police Force</td>
</tr>
<tr>
<td><strong>NSCDC</strong></td>
<td>The Nigeria Security and Civil Defence Corps (NSCDC) is a para-military institution of the Federal Republic of Nigeria commissioned to provide measures against threat and any form of attack or disaster against the nation and its citizenry.</td>
</tr>
<tr>
<td><strong>Phishing</strong></td>
<td>The fraudulent practice of sending emails purporting to be from reputable companies to induce individuals to reveal personal information, such as passwords and credit card numbers.</td>
</tr>
<tr>
<td><strong>SARS</strong></td>
<td>Acronym for Special Anti-Robbery Squad of the Nigerian Police Force.</td>
</tr>
<tr>
<td><strong>Sextortion</strong></td>
<td>It is the process of extortion (financial or other favours) from someone by threatening to disclose information or content of their sexual activity.</td>
</tr>
<tr>
<td><strong>Stuxnet</strong></td>
<td>A family of cleverly written malware worms that primarily target SCADA (Supervisory Control and Data Acquisition) control systems for large infrastructures such as industrial power plants.</td>
</tr>
<tr>
<td><strong>Transparency International</strong></td>
<td>Is a non-profit organisation that measures corruption in different countries around the world.</td>
</tr>
<tr>
<td><strong>TSA</strong></td>
<td>Treasury Single Account (TSA) is a Policy in which every income and expenditure of the Nigerian government is managed using one account. This is used by many countries around the world.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>West Africa</td>
<td>The part of Africa that lies to the north of the Gulf of Guinea.</td>
</tr>
<tr>
<td>Yahoo Boys</td>
<td>They are the fraudsters that commit fraud online.</td>
</tr>
<tr>
<td>Yahoo Yahoo</td>
<td>A colloquial term describing Nigerians that commit cybercrime. Some often use the term in place of Advanced Fee Fraud</td>
</tr>
<tr>
<td>Yahooism</td>
<td>The act of committing financial fraud online. It is a subculture within the Nigerian society.</td>
</tr>
</tbody>
</table>
# Table of Contents

Abstract ........................................................................................................................................... i
Acknowledgement ........................................................................................................................... iii
Statement of Declaration ................................................................................................................... iv
Key Terms ........................................................................................................................................ v
Chapter 1: Introduction .................................................................................................................. 1
  1.1 Research Aim and Objectives .................................................................................................. 2
  1.2 Research Questions ............................................................................................................... 2
  1.3 Why Nigeria as a case study? ............................................................................................... 3
    1.3.1 Potential Cybercrime Dominance .................................................................................. 3
    1.3.2 Failure of basic industry ............................................................................................... 4
    1.3.3 Economic Condition ....................................................................................................... 4
    1.3.4 Failure of government response .................................................................................... 5
    1.3.5 High level of inequality ................................................................................................. 5
    1.3.6 Failure of criminological theories .................................................................................. 6
  1.4 Thesis Organisation .............................................................................................................. 6
Chapter 2: Literature Review ......................................................................................................... 8
  2.1 Understanding Cybercrime .................................................................................................. 8
  2.2 Definition of Cybercrime .................................................................................................... 9
  2.3 The Classification of Cybercrime ....................................................................................... 12
    2.3.1 Classification by Target ............................................................................................... 12
    2.3.2 Classification by Machine and Targets ........................................................................ 13
    2.3.3 Classification by Generation ....................................................................................... 14
    2.3.4 Classification using Dual Paradigm ............................................................................. 15
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.4</td>
<td>The nature and characteristics of Cybercrime</td>
<td>17</td>
</tr>
<tr>
<td>2.4.1</td>
<td>Technical Skills Oriented</td>
<td>17</td>
</tr>
<tr>
<td>2.4.2</td>
<td>Transnational in Nature</td>
<td>18</td>
</tr>
<tr>
<td>2.4.3</td>
<td>Automation</td>
<td>19</td>
</tr>
<tr>
<td>2.4.4</td>
<td>Cybercrime as a Service</td>
<td>21</td>
</tr>
<tr>
<td>2.5</td>
<td>Criminological Theories applied to Cybercrime</td>
<td>23</td>
</tr>
<tr>
<td>2.5.1</td>
<td>Routine Activity Theory (RAT)</td>
<td>24</td>
</tr>
<tr>
<td>2.5.2</td>
<td>Strain Theory (ST)</td>
<td>27</td>
</tr>
<tr>
<td>2.5.3</td>
<td>Social Learning Theory (SLT)</td>
<td>29</td>
</tr>
<tr>
<td>2.5.4</td>
<td>Rational Choice Theory (RCT)</td>
<td>31</td>
</tr>
<tr>
<td>2.5.5</td>
<td>Techniques of Neutralisation</td>
<td>33</td>
</tr>
<tr>
<td>2.6</td>
<td>Motivations for Cybercrime</td>
<td>35</td>
</tr>
<tr>
<td>2.6.1</td>
<td>Altruism</td>
<td>36</td>
</tr>
<tr>
<td>2.6.2</td>
<td>Financial Gain</td>
<td>37</td>
</tr>
<tr>
<td>2.6.3</td>
<td>Psychosocial motivation</td>
<td>38</td>
</tr>
<tr>
<td>2.6.4</td>
<td>Political Motivation</td>
<td>39</td>
</tr>
<tr>
<td>2.6.5</td>
<td>Revenge</td>
<td>40</td>
</tr>
<tr>
<td>2.7</td>
<td>Modes of Operation of Cybercrime</td>
<td>41</td>
</tr>
<tr>
<td>2.7.1</td>
<td>Technological Development and Dimensions</td>
<td>42</td>
</tr>
<tr>
<td>2.7.2</td>
<td>Social Dimensions</td>
<td>43</td>
</tr>
<tr>
<td>Chapter 3</td>
<td>Understanding Cybercrime in Nigeria</td>
<td>46</td>
</tr>
<tr>
<td>3.1</td>
<td>Overview of Nigeria</td>
<td>46</td>
</tr>
</tbody>
</table>
### 3.1 Economic Situation

- 3.1.1 Economic Situation ................................................................. 46
- 3.1.2 Agriculture .............................................................................. 47
- 3.1.3 Rural-Urban Migration .............................................................. 48
- 3.1.4 Social Stratification ................................................................. 49
- 3.1.5 Technology in Nigeria .............................................................. 49

### 3.2 Characteristics of Cybercrime in Nigerian

- 3.2.1 Sub-culture evolution ................................................................. 51
- 3.2.2 Diverse Cybercrime Practitioners ............................................. 51
- 3.2.3 Crime Exportation ................................................................. 52
- 3.2.4 The Prominence of Banking Services ........................................ 53
- 3.2.5 Advance Fee Fraud (AFF) ....................................................... 53

### 3.3 Emerging Trends

- 3.3.1 Increasing Local Targets ......................................................... 54
- 3.3.2 Changing Motivations ............................................................. 56
- 3.3.3 High Technology Cybercrime .................................................. 56

### 3.4 Organised Crime (OC) and Cybercrime in Nigeria

### 3.5 Regulation of Cybercrime in Nigeria

- 3.5.1 Law Enforcement of Cybercrime .............................................. 59
- 3.5.2 Cyber-surveillance in Nigeria .................................................. 62
- 3.5.3 The Nigerian Cyber Security Strategy ................................. 63

### 3.6 Challenges of Combating Cybercrime in Nigeria

- 3.6.1 Issues of Expertise ................................................................ 66
3.6.2 Measurement Challenges......................................................................................66
3.6.3 Corruption in the Nigerian Criminal Justice System.............................................68
  3.6.3.1 Corruption in the Judiciary...............................................................................68
  3.6.3.2 Corruption in the Nigerian Police Force .........................................................69

Chapter 4: Research Methodology...............................................................................71
4.1 Research Philosophy...............................................................................................72
4.2 Research Design.....................................................................................................73
4.3 Qualitative Method ...............................................................................................74
4.4 Access ....................................................................................................................74
4.5 Sampling ................................................................................................................77
4.6 Data Collection .......................................................................................................79
  4.6.1 Data Collection Process .....................................................................................80
  4.6.2 Research Constraints........................................................................................83
    4.6.2.1 Participant Reluctance ................................................................................83
    4.6.2.2 Security .......................................................................................................84
    4.6.2.3 Infrastructure .............................................................................................84
    4.6.2.4 Diseases and Sickness ...............................................................................85
    4.6.2.5 Interviewing Convicted Criminals ...............................................................85
4.7 Data Analysis ..........................................................................................................86
4.8 Ethical Considerations ............................................................................................87

Chapter 5: Data Analysis .............................................................................................90
5.1 Demographic Analysis .........................................................................................90
5.2 Financial Motivation .............................................................................................93
  5.2.1 Financial Gain..................................................................................................94
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2.2</td>
<td>Unemployment</td>
<td>95</td>
</tr>
<tr>
<td>5.2.3</td>
<td>Poverty</td>
<td>97</td>
</tr>
<tr>
<td>5.2.4</td>
<td>Standard of Living</td>
<td>99</td>
</tr>
<tr>
<td>5.3</td>
<td>Behavioural motivation</td>
<td>103</td>
</tr>
<tr>
<td>5.3.1</td>
<td>Revenge</td>
<td>104</td>
</tr>
<tr>
<td>5.3.2</td>
<td>Frustration</td>
<td>107</td>
</tr>
<tr>
<td>5.3.3</td>
<td>Anger</td>
<td>109</td>
</tr>
<tr>
<td>5.3.4</td>
<td>Creativity and skills</td>
<td>110</td>
</tr>
<tr>
<td>5.4</td>
<td>Modes of Crime</td>
<td>113</td>
</tr>
<tr>
<td>5.4.1</td>
<td>Phishing</td>
<td>114</td>
</tr>
<tr>
<td>5.4.2</td>
<td>Identity Theft (Hurt the wealthy)</td>
<td>116</td>
</tr>
<tr>
<td>5.4.3</td>
<td>Romance Fraud (Social media and dating site)</td>
<td>118</td>
</tr>
<tr>
<td>5.4.4</td>
<td>Hacking</td>
<td>120</td>
</tr>
<tr>
<td>5.4.5</td>
<td>Cybercrime as a service</td>
<td>123</td>
</tr>
<tr>
<td>5.4.6</td>
<td>Attacking Government Infrastructure</td>
<td>126</td>
</tr>
<tr>
<td>5.4.7</td>
<td>Kidnapping</td>
<td>127</td>
</tr>
<tr>
<td>5.5</td>
<td>Organised Crime</td>
<td>129</td>
</tr>
<tr>
<td>5.6</td>
<td>Recruitment and Capacity Building</td>
<td>131</td>
</tr>
<tr>
<td>5.6.1</td>
<td>Cybercafe and Participant Recruitment</td>
<td>132</td>
</tr>
<tr>
<td>5.6.2</td>
<td>Capacity Building</td>
<td>134</td>
</tr>
<tr>
<td>5.7</td>
<td>Government Intervention</td>
<td>135</td>
</tr>
<tr>
<td>5.7.1</td>
<td>Surveillance</td>
<td>136</td>
</tr>
</tbody>
</table>
Chapter 1: Introduction

This thesis investigates the motivation, mode of operation, and emerging cybercrime trends by considering disciplines such as law, psychology, technology, and social policy. It uses Nigeria as a case study (see: Section 1.3) because there is a limited amount of research that focuses on cybercrime in the context of an individual country. Nigeria is an appropriate environment because it:

i) provides a viable context for a better understanding of how cybercrime is evolving and
ii) allows the researcher to expose the links between crime and social problems by drawing on knowledge from several disciplines. This criminological investigation has three core areas of enquiry: motivation (why), mode of operations (how) and emerging trends (what), as explained in Figure 1:

![Diagram of Research Scope](image)

Figure 1: Summary of Research Scope, using Nigeria as a case study

The discipline of criminology continues to evolve by expanding criminal behaviour knowledge (Brantingham & Brantingham, 2015). Hence, Criminologists\(^1\) have always been interested in understanding the reason (Why) behind criminal activities. Criminological understanding of cybercrime requires in-depth insights into theoretical and operational motivations that give rise to this type of crime. Motivation demonstrates the inter-connectedness of different processes

---

\(^1\) Criminologists are individuals that study both sociological and biological causes, consequences of crime and criminal behaviour.
and rules that influence the decisions and process of committing these crimes. Also, it is a continuous and evolving concept. It can change at any time, thereby changing the landscape of crimes. Its understanding provides a viable insight into the current state of cybercrime. Thus, researching motivation is fundamental in the knowledge of cybercrime.

Understanding motivation is not sufficient, but the influence on the actual crime is vital. The mode of operation reflects motivation in the areas such as typology of the crime, crime organisation and technology deployment. The mode of operation influences the way and nature of criminal behaviour (Burt & Simons, 2013). It is critical to understand the way (How) crimes are committed, by showcasing the nexus between motivation and the actual committed crime.

The evolution of the theoretical disciplines (e.g. law, sociology) associated with criminology often impact its conceptualisation. For example, the foundational classical perspective of crime described by Beccaria and Bentham in the eighteenth century has changed due to the growth in research, knowledge, and reality (Wincup, 2017). Technology evolution in the 21st century is more rapid and is changing the process of crime. For example, the “letter scam” has moved from the traditional physical crime into cyberspace (Rich, 2018). Technology is transforming both motivation and mode of operation, thereby necessitating the constant study of criminal behaviour (Lazarus, 2018). These changes make it vital to investigate the emerging trends (What) of cybercrime towards determining the potential growth area.

1.1 Research Aim and Objectives

This research aims to investigate changing motivations, modes of operations, and emerging trends of cybercrime, using Nigeria as a case study. The country is experiencing continual social, economic, and technological evolution (see: Section 1.3). The empirical findings will enrich the understanding of cybercrime in core areas as defined in the following objectives:

- To investigate the motivations driving cybercrime
- To discover the modes of cybercrime operations
- To derive potential cybercrime trends

1.2 Research Questions

Defining suitable research questions hinges on familiarity with the subject (Farrugia et al., 2010). In-depth knowledge of the research topic can result in numerous questions. Answers to these questions often deepen the knowledge in the subject area. In this light, specific questions
have emerged within the scope of this research towards filling the knowledge gap that hitherto exists in the subject area.

- Why are people currently engaging in cybercrime?
- What are the social, economic, and technical characteristics of cybercrime, including government responses?
- How will cybercrime develop in the future?

1.3 Why Nigeria as a case study?

Cybercrime in Nigeria is similar to that which is obtainable in other developing countries such as Ukraine, Brazil, India, Cameroon, Russia, and South Africa. Both motivation and the mood of crime are core areas of similarities. However, the country is an exemplar because of unique fundamental socio-economic, regulatory, and cultural factors. Six core factors make the country a viable exemplary case study for this research.

1.3.1 Potential Cybercrime Dominance

Cybercrime has developed in western countries despite the effective Criminal Justice System (CJS), but its future is likely to be dominated by countries where digital penetration is greatest. This will be countries like Nigeria, Brazil, India, China, etc. Nigeria is 7th in Internet penetration with over 100 million Internet users (see: Section 3.1.5). There is technology in the hand of millions of Nigeria that can be deployed for either positive or harmful use. However, evidence showed that the country thrives in the criminal use of the Internet. Cybercrime has evolved into the national social consciousness with increasing volume and sophistication.

For decades, the country has been one of the leading cybercrime countries. BBA (2015) ranked Nigeria among the top 10 cybercrime sources in the world. The country remains the third source of cybercrime globally (Internet Crime Complaint Center, IC3, 2013; Danbatta, 2017). However, the country is gradually growing into a more potent part of the global cybercrime ecosystem. Nigeria can become the capital of cybercrime as Mexico is to narcotics. The rising penetration of technology, burgeoning population, and weak Criminal Justice System (CJS) provide a viable platform for uncontrolled cybercrime growth. Cybercriminals from the country can take away potency from developed countries such as the United Kingdom and the USA and replicate it with limited hindrance locally. They can become a significant force that cannot be controlled by local law enforcement. Hence, the need to understand its evolution, motivation, and mode of operation becomes vital to provide relative insight into other West
African countries (such as Ghana, Cameroon, Ivory Coast and Benin Republic) and other developing countries worldwide.

1.3.2 Failure of basic industry

Nigeria is also an example of a country where basic industries have declined, with the economy dependent on oil as the basic export (see: Section 3.1). Many other countries in this situation are performing better than Nigeria. Unlike other developing countries, the Nigerian case is terrible, with no globally competitive industry. The agriculture sector performs poorly with an annual food import bill of $10b (about £8.8billion) (International Trade Administration, 2020). Agriculture in Nigeria does not measure up to what is obtainable in other developing countries such as Brazil, which is the fourth-largest producer of food in the world (WeForest, 2019). Other West African countries like Ivory Coast, Benin and Cameroon are now sources of food imports.

Also, there is limited opportunity for technology experts to excel and contribute to the economy. Unlike India, whose Information Technology (IT) outsourcing industry is $150billion (Sachitanand, 2017), the country does not have a viable IT industry that could positively employ skilled personnel (see: Section 3.1.5). The manufacturing industry remains abysmal when compared to other countries. Manufacturing in Nigeria contributed 12 per cent of Gross Domestic Product (GDP) in 2019 but still below 20 per cent recorded in the mid-1980s (Pilling, 2020). The manufacturing sector performs poorly than South Africa, whose contribution to GDP is 26 per cent (Plecher, 2020a). The failure of industries directly makes Nigeria an exemplar even among developing countries.

1.3.3 Economic Condition

Nigeria’s young and educated population is repeated all over the world. Its government has proved inadequate in the task of finding them employment. Thus, they are employing themselves using the cheapest form of technology such as smartphones and moving into cybercrime. With 34 per cent youth unemployment, cybercrime is regarded as the only ladder for gainful employment (see: Section 3.1.1). Nigeria graduates 300, 000 thousand young people from higher education annually but can only employ a few (Edeh, 2017). The crime is robust, making the country a viable case study to understand cybercrime.

The economic condition of the country is dire when compared with other West African countries. With unemployment rates in Ghana (4 per cent), Cameroon (3 per cent), and Niger (below 1 per cent) better than Nigeria (Plecher, 2020b; Trading Economics, 2020), the
economic motivation of tens of million makes the country an exemplar situation. The country remains an island of poor economic condition amid economically upward countries. Thus, providing a socio-economic outlier for investigating cybercrime.

1.3.4 Failure of government response

The inability of Nigerian governments to appropriately respond to cybercrime is also common globally: laws are running behind criminals: there is little international cooperation: law enforcement agencies are not skilled in digital interventions. Also, the Nigerian situation is further enhanced by other factors that make law enforcement inefficient. Some of them include corruption, excessive support for cybercrime, and poor regulatory infrastructure (see: Section 3.5 and 3.6)

The government has not invested sufficiently or focused on cybercrime significantly. While other countries continue to strive for increased intervention to mitigate these crimes, Nigeria struggles for an adequate response. For example, the USA has the Federal Bureau of Investigation (FBI), the UK set up Government Communications Headquarters (GCHQ), but Nigeria has not set up a dedicated institution for cybercrime (Section 3.5). China arrested 60,000 in one month as part of their effort to mitigate cybercrime (Ashkar & Caixiong, 2019). The Nigerian response has been weak and ineffective (see: Section 3.5 and 3.6).

On the other hand, the government might not be totally at fault for the weak response. The country has a lot of problems with traditional crimes, making cybercrime to be a secondary problem. Some security problems include terrorism, kidnapping, banditry, smuggling, oil bunkering, and other contact crimes. Internal security of the country is beyond the ability of the Police necessitating the deployment of the military. The Nigerian army is conducting security operations in 32 of the 36 states of the country (Oyedele, 2017). The focus of the country is to ensure internal security, thereby permitting cybercriminals to operate with relative freedom. Thus, cybercrime in Nigeria can progress into becoming dangerous and uncontrolled.

1.3.5 High level of inequality

Nigeria has tremendous inequality, and many other countries are also moving that way. There is high level of inequality worldwide as the wealth of a few overshadows those of the entire masses. The wealthiest 1 per cent of the world has more than twice the wealth of 6.9 billion people (Oxfam, 2020). This inequality is present in every country and society, putting extreme pressure on the less privilege.
The exemplarity in the Nigerian situation is the narrowing of the middle class, ineffective strategy to bridge the gap, increasing influence of the wealthy, and widespread abuse of the poor. The pervasiveness of poverty remains a contrast despite the country being the biggest economy and having the richest man in Africa. The World Bank has projected that 100 million Nigerians will be impoverished by 2022 (Munshi, 2020). The inequality is tremendous and has been stimulating criminogenic behaviour.

Money is the only measure of responsibility, influence, and recognition in the country irrespective of source. Thus, the adoption of cybercrime is to satisfy the Get Rich Quick Syndrome (GRQS) that is pervasive in the country. Both the government and the affluent have not been able to lift numerous poor from poverty. The country provides a viable case study for which poverty, inequality and government apathy can be explored within the cybercrime context.

1.3.6 Failure of criminological theories

Criminological theories within the cybercrime context have lagged behind the crime. The field of criminology has not responded theoretically to the evolution of crimes on the Internet. Researchers have applied tradition theories such as Routine Activity Theory (RAT), Strain Theory (ST), Rational Choice Theory (RCT) and others to investigating cybercrime (see: Section 2.4). Despite some level of suitability, the evolution of the crimes continues to emphasise the inadequacies of already established theories.

No singular theory has captured different elements and understanding of these crimes. Areas such as motivation and mode of operation remain subjective with weak theoretical frameworks. The failure to have a concise definition and classification of these crimes further highlights the failure of the theories. This research provides further insight using a viable case study in establishing a theoretical understanding of cybercrime. The new knowledge will contribute to developing theories that will further stimulate the criminological body of knowledge concerning these crimes.

1.4 Thesis Organisation

The thesis is in six other chapters. Chapter Two is the literature review that contains a theoretical discussion about cybercrime definitions, classifications and characteristics,

---

2 GRQS is the support of the society for insatiable urge to make money in irrespective of through crime or legitimate means.
economic impacts and different types of motivation, and the discussion of five relevant criminological theories as they apply to cybercrime. Chapter Three discusses the application of the existing theoretical framework to Cybercrime in Nigeria within the reality of the criminology theories that are earlier explained in the previous chapter.

Chapter Four presents the methodology of this research. The sections include research philosophy, research design, research process, data collection and analysis, and ethical considerations. Phenomenology is the preferred philosophy with the use of interpretative experience of participants. The qualitative method is preferred in agreement with the preferred philosophy. The processes for data collection include interviews, focus groups and documentary analysis.

Chapter Five is in two parts. The first part presents the analysis of the collected primary data. It starts with demographic analyses of the research participants. Five core themes are derived, including financial motivation, behavioural motivation, mode of crime, organised crime, and government intervention. The second part places the primary research findings within the current body of knowledge.

Chapter Six presents the theoretical implications of the findings. It discusses the overall contribution of the findings to the various criminological theories. Chapter Seven presents the concluding discussion of this research. It discusses the research recommendations and contribution of the findings to the body of knowledge.
Chapter 2: Literature Review

This chapter considers the available literature on Cybercrime. The first discussion focuses on distinguishing the two paradigms that characterise these crimes. It is followed by discussing the problem of definition and classification of Cybercrime. The chapter discusses criminological theories, including how they might apply in Nigeria and ends with discussing cybercrime motivations and modes of operation.

2.1 Understanding Cybercrime

There are two conflicting paradigms in understanding Cybercrime, forming two philosophical schools of thought concerning its nature and scope. Overall, they influence different aspects of crimes on the Internet, such as its definition (Section 2.1) and classification (Section 2.2).

The first paradigm claims that Cybercrime is a traditional crime conducted using new methods (Grabosky, 2001). Cybercrime is not new, and only the use of the Internet is its unique feature: it results from human emotions that inspire real-life corruption, as seen previously in traditional crimes. This paradigm is supported by Yar (2005), who argued that the Internet is the core feature of any cybercrime. The argument suggests a broad scope with the use of the Internet in any crime qualifies it as Cybercrime.

What could be gleaned from Grabosky’s (2001) position is the irrelevance of a new conceptual framework for Cybercrime. Attaching a prefix to any crime where it involves the Internet or electronic processing is sufficient: e.g. the use of prefixes such as “e-”, “information”, “digital”, “computer”, “internet” or “cyber” as identified by Van der Hulst and Neve (2008).

On the other hand, the second paradigm says that Cybercrime has introduced a new realm of crime that is quite different from traditional crime. Scholars such as Leukfeld et al. (2013) and Lusthaus and Varese (2017) argue that significant aspects of Cybercrime are new even though consisting of digital perpetration of ‘traditional crimes’. The increasing numbers of cases such as hacking, computer network disruption, zero-day attacks, malware and Ransomware undermines Grabosky’s (2001) argument. The increasing contextual mutation of such crimes point to a level of sophistication that cannot be associated with traditional crimes before the arrival of the Internet. The Internet has introduced new threats and models of crime (Lusthaus & Varese, 2017; Wall, 2007a). It is a platform for crimes that cannot be placed within the traditional constructs of criminology.
The Internet changed crime from the claim that it is “old wine in new bottles.” The advent of technologies such as 4G, big data, virtual reality and robotics has provided a new frontier for criminal behaviour. In this light, an understanding of Cybercrime should be derived from the new paradigm. Luekfeldt and Yar (2016) concluded that cybercrimes are transforming the conventional elements of criminology by introducing new characteristics. Indeed, Internet crime has become highly technical, borderless, intense, and technically complex (see Section 2.4). The crimes are diverse in typology, victim distribution, victimisation speed, and different from what is experienced in contact crimes.

Also, there is less regard for the incidence of crime in the Grabosky (2001) paradigm. Where the crime took place remains essential in developing a definition. When a crime is committed in a human, physical, and social space, it should be regarded as contact crime irrespective of the involvement of Internet. Cybercrime however, should be presented as the incidence of crime that occurs on the Internet. Incorporating criminal behaviour where the Internet is used for legitimate purposes is inappropriate. It continues to increase the difficulty in finding a definition for Cybercrime based on the expanding scope.

2.2 Definition of Cybercrime

The definition of Cybercrime remains challenging because scholars have tried to accommodate elements of both overarching paradigms. A further factor that challenged previous attempts at defining these crimes is the heterogeneity of the crimes (Europol, 2014). It is reflected in the malleability and ever-changing nature of criminal behaviour on the Internet. Indeed, the evolution of Cybercrime has resulted in the need for a continuous reassessment of its meaning. A further contributing factor is the rising complexity of cybercriminal activity. Ibekwe (2015) discovered that offenders are highly skilled, which enabled them to widen the scope of the criminal enterprise. The subjective approach for defining these crimes challenged the earlier consensus around its original definition. Over time, definitions have reflected different contexts such as personal, professional, or regulatory perspectives.

All these factors contributed to frequent changes in the definition of Cybercrime. Thus, a time-series approach to cybercrime definition is adopted in this section. One of the early definitions is from Thomas and Loader (2000, p. 3); “computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic
networks”. This definition identified that Cybercrime is conducted on the Internet. It also includes any activity that is considered to be illegal.

The definition is broad by recognising certain unspecified elements. Any activity that is conducted can be regarded as a crime from subjective point of view. This feature gives great latitude to different agencies in specifying what they considered illicit. It allows criminal activity to vary and could be dependent on the terrain or location. Thus, the meaning and scope of Cybercrime become highly unpredictable.

Also, Thomas and Loader (2000) fail to recognise crimes by other devices that are not computer-related (such as PoS\(^3\), RFID Scanners\(^4\), and mobile phones). Advances in technology such as robotics, quantum computing and big data were not significant considerations in this definition. For example, Internet of Things (IoT) increases the number of internet-connected devices and enhances the risk of them being used for crime. The advances of technology have increased the number of devices that can either be used or attacked by cybercriminals.

Some years after Thomas and Loader’s definition (2000), a new definition emerged to provide a more precise scope and boundary for Cybercrime. Yar (2005, p. 409) presented Cybercrime to “signify a range of illicit activities whose common denominator is the central role played by networks of information and communication technology (ICT)\(^5\) in their commission”. This definition leaned towards Graboski’s (2001) paradigm as it stressed the role of ICT. It did elaborate on the characteristics of Cybercrime to involve human agents using a machine.

Yet, one critical issue is the failure to remove the subjective definition of these types of crime. Thus, illicit activities were not clearly defined. It allows every individual, business, or government to specify what they subjectively prefer to be criminal behaviour. There is freedom to input any crime or behaviour under illicit activities, thereby promoting inconsistency in the scope of Cybercrime.

On the other hand, it is believed that simplifying the definition would further reduce or eliminate any confusion concerning its scope. In this light, Wall (2007a, p. 11) defined Cybercrime as “crimes which are mediated by networked technology”. However, this definition is unsuitable because it fails to recognise that not all networked technology is part of the

---

\(^3\) Point of Sales

\(^4\) Technology used to track goods using bar codes in stores and other logistic companies.

\(^5\) ICT are technologies that involve internet and other communication technologies such as telephones.
Internet. Crimes can be committed using a local area network (LAN)\textsuperscript{6} or a Bluetooth device which does not make it primarily a cybercrime concerning this definition.

Four years after the Walls (2007a) definition, it emerged that motivation and the result of the crime could provide a means for establishing a generally accepted definition. Based on this belief, Abdulhamid, Haruna, and Abubakar (2011, p. 47) defined Cybercrime as “\textit{all crimes performed or resorted to by abuse of computer network or Internet to influence the functioning of the computer system and also for financial gains}.” The definition highlight financial gains and abuse of computer networks as the core elements of Cybercrime.

However, there are critical points that weaken the suitability and acceptability of this definition. The identification of computer system functioning and financial gain as core features is not totally appropriate. An overreliance on financial gain proved to be a significant drawback. Not every crime is focused on financial gain. But this definition neglected other non-financial crimes such as cyberbullying and cyberstalking. The identification of financial gain within the definition made it inadequate within the broader scope of cybercrime scholarship.

There are other outcomes of Cybercrime that provided a basis from which criticism emerged concerning this definition. Although cybercrimes such as Ransomware and distributed denial of service (DDoS)\textsuperscript{7} directly affect the functioning of the computer system, others such as cyberespionage and identity theft affect non-computer targets. The malfunctioning of a computer system is a significant focus of the crime. A further feature relates to state sponsored attacks where purposes are diverse and do not necessarily focus on a specific outcome.

Another definition emerged from other scholars. Leukfeldt, Veenstra and Stol (2013a) defined Cybercrime as any illegal activity conducted over the Internet. Their position provides flexibility and broad coverage for different online crimes by not giving specific examples. It implies that Cybercrime can be any alleged, or agreed, crime.

However, it did not capture crimes where online actions (though not illegal) contributed to offline crime. Furthermore, human beings may orchestrate this crime. In this light, the concept of Cybercrime relates to every form of criminal activity emanating from using the Internet or computer networks.

\textsuperscript{6} LAN implies Local area Network. It is a network that links together computers and peripheral equipment within a limited area, such as a building or a group of buildings.

\textsuperscript{7} DDoS is Distributed Denial of Service. It is a type of attack where many systems attack a network with malicious traffic to make it unavailable for legitimate users.
One fundamental impact of this inconsistency is that notable organisations such as the African Union Convention, the Council of Europe Cybercrime Convention and the Cybercrimes Act of Nigeria 2015 refused to define these crimes. Their approach emphasises the meaning of Cybercrime through the type of crime rather than through definition.

However, there remains a need to create a definition for the future understanding of this type of crime. The definitions can be made much sharper and concise. The researcher believes that Cybercrime should be defined as “all crimes perpetrated or facilitated using internet connection”. This definition focuses on capturing the subjective aspect of crime definition and the interface of cybercrimes with environmental crimes.

2.3 The Classification of Cybercrime

Categorising Cybercrime into different types or groups is a challenge because of the differing perspectives and criteria identified by various stakeholders. Over time, criminological research has significantly expanded our knowledge of these crimes. The absence of a consensus around a definition has resulted in continuous conceptual division among scholars (Holt & Bossler, 2014). The lack of standardised contextual scope and definition (see: Section 2.1) of Cybercrime means classifications are undertaken using different lenses and approaches.

2.3.1 Classification by Target

Cybercrime is classified based on the target of the crime. Three types of targets were identified: property, morals, and person (Wall, 2001; Yar & Steinmetz, 2019). The first category is cyber-trespass. These are crimes that cross boundaries, do damage by way of viruses, defacement, and hacking. The damage relies on gaining unauthorised access to computer systems, network, devices, and services using the Internet.

The second category is cyber-deception. These are crimes that involve the theft of property and money, such as violations of intellectual property and credit card fraud. The third category is cyber-violence covering any crime that causes psychological or physical harm. This type of crime exhibits the violation of laws concerning the protection of people, such as stalking and hate speech. Cyber-pornography can be situated within cyber-violence context. It involves a breach of decency and obscenity laws.

The target for the first two categories is property, while that for the third category is people. However, the expanding nature of targets creates the need for an additional category. Yar and Steinmetz (2019) added crimes against the state as another category. They are activities that
violate laws which protect the integrity of the nation and the infrastructure (e.g., espionage, terrorism, and official secrets disclosure). This approach to classification is flexible and expands as the crimes evolve.

Despite the extensive and straightforward nature of the categories, there are notable flaws that make it difficult to accept them. It primarily focuses on crimes that target individuals rather than businesses and governments. The absence of categories that primarily address crime against the business sector proves to be a significant weakness despite the increasing targeting from cybercriminals. They have been victims of espionage, DDoS to their technology infrastructure, website defacement and Ransomware. Thus, there is need for classification that caters for businesses.

Yar and Steinmetz (2019) argue this classification also left only limited room to cater for new crimes. The increasing evolution of Cybercrime implies a continuous introduction of new categories: e.g. Cybercrime against the environment, intellectual property, national infrastructure, or public health. Thus, this approach to classification remains significantly incomplete.

2.3.2 Classification by Machine and Targets

In addition to the target approach, this classification introduces the role of machines as a factor. It identifies the target as a core metric and consideration for the different types of Cybercrime. It can be derived from this perspective that Cybercrime is in four categories concerning machines and the targets of the crime.

The first category is crimes with the computer as a target (Wall, 2015). These are crimes that focus on illegal access to the system for malicious purposes. Fafinski et al. (2010) and Jahankhani et al. (2014) labelled this category as ‘crimes against the machines’. They include intellectual property theft, illegally gained electronic files for blackmail and marketing information theft. Some of the crimes include Ransomware, malware attacks and website defacement. They are crimes that disrupt services and technology infrastructure, such as servers and networks.

The second category is crimes involving the use of computer as an instrument of crime. Jahankhani et al. (2014) cite examples to include credit card fraud, telecommunications fraud, businesses of different sizes, machines include different devices such as computer systems, switches, mobile phones, servers, and others. Other target can be broader such as computer networks, servers, databases, and other devices.
fraudulent accounts, ATM frauds, and computer transactions (billing, sales, and stock transfer). They are crimes committed using a machine, computer networks and infrastructure for criminal activities (Wall, 2015). The role of technology is to facilitate crime by the cybercriminal.

In the third category, the computer is incidental to other crimes. These crimes involve using ICT and computer networks to complement or complete other crimes (Wall, 2015). They involve the use of technology side-by-side with traditional criminal activity. The crimes in this category included bookmarking, illegal banking transactions, and money laundering.

The fourth category is crimes that focus on the lives of every individual and organisation. Jahankhani et al. (2014) cite examples of this category to include software piracy, technological equipment theft, counterfeit equipment and black-market programs or equipment. These crimes directly reflect profound effects on the victims, which can be individuals or organisations.

However, the classification possesses gaps that allow future classifications. Firstly, the classification does not adapt to crimes that target entities that are not necessarily online. An example of this type of crime is fake news that focuses on misinformation. Also, the government was not identified in the fourth category as a target. These gaps are significant and affected the efficacy of this approach.

2.3.3 Classification by Generation

Cybercrime is also divided into three generations (Wall, 2017). These generations are regarded as distinct and consisted of different concepts of criminal opportunity. It provides a foundation to discuss the type of these crimes. The crimes are classified into three generations.

The first generation consists of crimes involving information destruction or financial gain and those supporting traditional crime (Wall, 2007a). The crimes include support for previous conventional crimes through the manipulation and exploitation of computers. They are crimes that migrated from offline into the realm of the Internet to affect the functioning of the computer.

The second generation consists of crimes that involve the use of networks (Wall, 2017). This category highlights traditional crimes that use the Internet, such as using social media to locate a kidnap victim or internet use for personal slave auctions. The Silk Road website for auctioning narcotics is another example. It is the generation where traditional crimes are used to facilitate the conduct of conventional crime. The Internet performs a complementary role for traditional crimes.
The third generation involves criminal activities that occur solely on the Internet. The disappearance of the Internet would make this crime impossible (Wall, 2007a). Every crime (such as hacking, denial of services, the spread of viruses or spamming) whose incidence only occurs on the Internet belongs to this generation.

On the other hand, this classification fails to acknowledge core elements of the crimes. The absence of motivation (see: Section 2.6) meant that every action deemed illegal is adopted in the crimes. The last two generations did not reference motivation, leaving a gap in establishing criminal liability of the crimes. In the era of intelligent and complex computing, this classification will struggle to establish typologies of crimes for unknown motivations.

Also, modern cybercrimes demonstrate an overlapping of the generations. With financial gain and Internet-dependent crime becoming integrated into crimes such as Ransomware, the classification becomes less distinct and inseparable. Overall, the viability of the separation becomes less viable.

Also, this classification is not entirely correct by not considering the incidence in the classification. The need to include crimes that are conducted offline is a significant drawback to this approach. As discussed earlier, only crimes that occur online should be regarded as Cybercrime. Actions that are not illegal, but used with offline crime, should not be classified as Cybercrime.

### 2.3.4 Classification using Dual Paradigm

Cybercrime is divided into cyber-dependent and cyber-enabled crime. Cyber-dependent crime is those offences that can only be committed using computer networks, computers, and other types of ICT (McGuire & Dowling, 2013). Examples include hacking, the spread of viruses, DDoS attacks and Ransomware. They are exclusive crimes whose conduct requires the Internet. When technology is unavailable, this type of crime cannot occur.

Cyber-enabled crimes are traditional crimes that are escalated in their scale, speed and reach using the Internet. They represent the transformation of tradition and physical crime to the electronic processing and internet platform. Identified examples include fraud, theft, paedophilia, identity theft, and bullying. They occur both offline and online. Wall (2015) noted that crimes such as Pyramid schemes and Ponzi frauds use Internet for their perpetration but are not conducted on the web. Without the Internet, this type of crime would still occur but within a localised context. The Internet increases the coverage and scope of the perpetration.
One critical aspect of this classification is the failure to identify crimes that combine both categories. In situations where viruses are used for fraud or identity theft, the two categories have been integrated, thereby blurring the difference. This approach appeared basic and disregarded the integration and combination of numerous acts involved in a crime. For example, the Sony movies case in 2014 involved hacking and theft of intellectual property (Sullivan, 2016). This categorisation is not appropriate because of the combination of actions in perpetrating any of these crimes.

However, another dual approach was formulated by Jahankhani et al. (2014). Cybercrimes are classified as either active or passive computer crimes. Active crime represents computers for criminal activity (e.g., hacking), while passive computer crime occurred when illegal activity is supported or advanced using a computer.

The reliance on Cybercrime as computer crime remains a significant drawback in the classification. It reflects Thomas and Loader’s (2000) definition that exhibits significant scoping challenges for these crimes. When devices that are targeted are not computer systems, this classification becomes irrelevant.

Table 1: Cybercrime Classification Summary

<table>
<thead>
<tr>
<th>Authors</th>
<th>Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yar (2005)</td>
<td>New crime</td>
</tr>
<tr>
<td>Wall (2001) and Yar (2005)</td>
<td>Cyber-trespass</td>
</tr>
<tr>
<td></td>
<td>Cyber-deceptions and thefts</td>
</tr>
<tr>
<td></td>
<td>Cyber-pornography</td>
</tr>
<tr>
<td></td>
<td>Cyber-violence</td>
</tr>
<tr>
<td>Wall (2007a)</td>
<td>The first generation (involving traditional crime)</td>
</tr>
<tr>
<td></td>
<td>The second-generation (use of networks)</td>
</tr>
<tr>
<td></td>
<td>The third generation (sole use of the Internet)</td>
</tr>
<tr>
<td>Jahankhani et al. (2014)</td>
<td>Active or Passive computer crime</td>
</tr>
<tr>
<td>Wall (2015)</td>
<td>Technology-encoded</td>
</tr>
<tr>
<td>McGuire and Dowling (2013)</td>
<td>Technology-dependent</td>
</tr>
<tr>
<td>Wall (2017)</td>
<td>Computer as a target</td>
</tr>
<tr>
<td>Fafinski et al. (2010)</td>
<td>Computer as the instrument of crime</td>
</tr>
<tr>
<td>Jahankhani et al. (2014)</td>
<td>The computer is incidental to other crimes</td>
</tr>
<tr>
<td></td>
<td>Computer prevalent crimes</td>
</tr>
</tbody>
</table>
Another critical point is the simplistic approach to the definition. This approach to classification widens the scope using categories that support seemingly endless scope. This classification is simplistic but fails to create a broad scope for each type of Cybercrime.

Based on the different perspectives, it is evident that multiple cybercriminal activities could be categorised differently. Hence, the evolution of these types of crime necessitated an increasing means of classification. Table 1 provides a detailed summary of the variation in the categorisation of Cybercrime.

2.4 The nature and characteristics of Cybercrime

As the Internet expands human interaction boundaries, criminal usage continues to mutate and become more sophisticated. Cybercrime in its evolution, demonstrates distinct features that were not existing in previous traditional crimes. Advances in technology change the nature of the crimes (Microsoft, 2017; Mitchell, 2016; The Royal Society, 2017; Venčkauskas et al., 2015). This section discusses the characteristics of Cybercrime.

2.4.1 Technical Skills Oriented

Cybercrime can require highly skilled individuals and organisations. Attacks such as WannaCry ransomware, Zeus, Spy Eye, Stuxnet, Red October, Flame and others demonstrate the advanced skill level required for cybercrime activities (Armin et al., 2015b; Krombholz et al., 2015; Naidu & Sireesha, 2017; Wall & Williams, 2013). Because these crimes are technology-based, the skills required are higher than for other conventional crimes (Kshetri, 2010a). Clough (2015) noted that technical skills are required for illegal intrusions into computer networks to implement denial of service (DDoS) attacks or carry out website defacement. Participation in crimes often involves the mastery of one technology-oriented skill.

Technology skills have a significant influence on criminal behaviours on the Internet. Hargreaves and Prince (2013) identified two ways: Firstly, it enhances the communication and behaviour of criminals with potential victims worldwide; Secondly, it reduces the entry barrier for criminogenic activity (Hargreaves & Prince, 2013). These two areas (especially the second area) emphasise that high technological skills increase the potency of criminal behaviour.

However, the variations in cybercrime activity also prove the limited relevance of technical skills. Offline crimes that are conducted through information on the Internet are not
technological. For example, a kidnapper using an application such as Facebook, Twitter, or WhatsApp to retrieve the picture of the victim does not use any exceptional skills. The overemphasis on the technical characteristics is not, therefore totally sustainable.

As discussed earlier (Section 2.2), many cyber-enabled crimes require no technical knowledge. In numerous instances, cybercrimes often involve offline perpetration so that technological knowledge or expertise does not surface. The Anajemba case involved Internet use for communication as part of a broader 419 scheme (Frank & Odunayo, 2013). In the Silk Road case, the conviction was achieved by the claim that a website provided a platform for the assassin to meet the customer (Garcia, 2017). It cannot be entirely accepted that technological skill remained a fundamental feature of Cybercrime.

Despite the argument over technical proficiency, what cannot be ignored is that Cybercrime requires a basic knowledge of the Internet to use it. Kshetri (2010a) indicates that Cybercrime is structurally unique because of technology and skill-intensiveness. Manky (2013) also notes that offender profiles in Cybercrime demonstrated that highly skilled individuals are involved in achieving their goals. Perpetrators must master Internet technology to be actively engaged in Cybercrime.

2.4.2 Transnational in Nature

The borderless nature of the Internet also extends to cybercrime. Unlike traditional crime, where jurisdictions could be mapped, both perpetrator and victim could span across nations or even continents (Chambers-Jones, 2013). For example, the WannaCry ransomware attack victims were found in many countries, while members of the Hacking group “Anonymous” resided in multiple countries (McAlaney, Thackray & Taylor 2016; Vigliarolo, 2017). Cybercriminals have taken advantage of borderless internet characteristics to make crimes transnational. It remains a complex crime that can simultaneously involve multiple countries.

There is no physical barrier or demarcation on the Internet. It allows cybercriminals to target victims from any part of the world without geographical hindrances (Ibrahim, 2016b). This characteristic is fundamental in increasing the risk of a remote attack. Cybercriminals are not limited by space, thereby making their enterprise transnational.

A further dimension of this characteristic is the introduction of a transnational network of attacks. Considering the concept of distributed computing, perpetrators across countries can collaborate and attack any target (Leukfeldt, 2017). Every attack on the Internet is now local because of the virtual elimination of space and time.
However, this characteristic is never limited to cybercrime. Crimes such as child trafficking, drugs, tax evasion and money laundering are conducted across borders (Le Nguyen, 2020; Stambøl, 2019; van der Lan, 2017): and criminals such as Al Pacino and Pablo Escobar\(^\text{11}\) perpetrated international crimes without the Internet. The only difference between these crimes and cybercrime is the use of the Internet.

Also, countries can regulate and monitor Internet traffic within their country. The borderless characteristics might be overstated as various countries have technologies to prevent unwanted traffic within their country. For example, Saudi Arabia blocks websites that are considered contrary to their values from being accessed in their country. Even when criminals use technologies to hide their identity or location, sophisticated investigation can still be used to identify the source of cybercrime. Hence, the transnational nature of crimes can still be restricted or criminal activities.

### 2.4.3 Automation

Another characteristic of cybercrime is increasing automation. Offender-victim engagement is automated using malicious programs, software, and spams\(^\text{12}\) (Enoch et al., 2020). Offending is no more a function of human interaction, with the use of tools, programmed to function in a certain way and at a specific time. Criminal behaviour on the Internet is automated using computers, and programs act without human intervention (Kraemer-Mbula et al., 2013). It is a malicious use of the automation element of the Internet that has been acknowledged by governments worldwide. The Australian House of Representatives (2010) acknowledges the Internet as an active medium for automated systems deployment, thus enabling the automation of online criminal activities. Recognising that the Internet is not regulated, it is easier to deploy these tools towards an intended target. Technological knowledge and facilities enable a high level of automation and action at a distance (Enoch et al., 2020; Neufeld, 2010). Thus, remote attacks can be programmed and initiated using automation.

Automated exploitation of vulnerabilities on the Internet continue to increase the intensity and impact of cybercrime. It relies on improved accessibility to robust systems and fast connection for automating sophisticated attacks. The deployed tools enable more applications to attack and exploit more vulnerabilities than is possible with a manual method (Imperva, 2012). Because they are computer programs, the perpetration rate and scope are beyond what humans can

---

\(^{11}\) Prominent drug dealer from Colombia.

\(^{12}\) Irrelevant or unsolicited messages sent over the Internet, typically to a large number of users.
manually achieve. It increases the ruthlessness and power of cybercrime because of the enhanced abilities that this introduced (Nurse, 2018). Automation, for example, ensures a rapid incidence of malicious attacks.

One implication of automation is both an expanding typology and mutation of crimes over the Internet. Automation enhances real-time fusion of programs to form cyberattacks with diverse effect. Kharouni (2012) noted that automatic transfer systems (ATSs)\(^{13}\) are combined with Zeus\(^{14}\) and SpyEye\(^{15}\) (both malware) to develop WebInject files\(^{16}\) that automate online banking fraud. Sood, Bansal and Enbody (2013) stated the possibility of combining automated malware framework with general distribution techniques for cyberattacks such as a drive-by-download attack. Combination attacks are evident and demonstrate the growing sophistication of these crimes.

Irrespective of the form or approach, crimes on the Internet continue to demonstrate significant automation characteristics. According to Hoanca and Mock (2020), cybercriminals are adopting rudimentary automation tools for conducting crimes on the Internet. Some of the tools include botnet, exploit kits and cryptojacking\(^{17}\) software. Every advancement recorded in technology has stimulated corresponding sophistication in criminal behaviour (Nurse, 2018). There is a possibility in the near future that Cybercrime will adopt high-level technologies such as Artificial Intelligence, quantum computing, distributed computing, and augmented reality.

The use of automation has been growing for some time. As of 2013, the use of exploit kits for cybercrime automation was the fourth evolving threat landscape of the Internet (ENISA, 2013). These tools also increase the efficient use of resources and expanded avenues for evading security defences (Imperva, 2012). In some cases, perpetrators use compromised servers as a platform for attacks. The tools function smoothly on these servers for optimised targeting of specific systems on the internet. Agana and Inyama (2015) noted that automated attack tools often overwhelm the defence and monitoring systems of various networks. It can change the

---

\(^{13}\) Automatic transfer systems are programmes or devices that dynamically propagate traffic on the Internet.

\(^{14}\) Zeus is a trojan malware. It is a form of malicious software that targets Microsoft Windows and is often used to steal financial data.

\(^{15}\) SpyEye a malware program that attacks users running Opera, Microsoft Windows operating systems, Firefox, Google Chrome, and Internet Explorer. Microsoft Windows operating systems.

\(^{16}\) Webinfects are modules or packages used in financial malware that typically inject HTML or JavaScript code into content before it's rendered on a web browser.

\(^{17}\) Cryptojacking is the unauthorised deployment of computer, devices, mobile phone, tablets and connected home devices for mining cryptocurrency by cybercriminals.
IP address\textsuperscript{18} or HTTP User-Agent header\textsuperscript{19} to bypass security systems or split the attack among different hosts to eliminate blacklisting.

Despite the potency and evidence of this crime, one fundamental and critical point is that automation is overly expensive. The cost of implementing automation is significantly higher because of the required infrastructure. For example, the processing power for the automation forced groups like ‘anonymous’ to solicit distributed attacks from different members worldwide. Significant investment continues to be a requirement to run large scale automated cyberattacks.

This characteristic does not provide equal opportunity and, as a result, it may influence the location of a cybercriminal who wishes to use automation. The cost involved is always a turnoff for cybercriminals in developing countries. Cybercriminals in countries that struggle with electrical power, a high cost of living, or economic challenges will find it exceedingly difficult to implement automation.

Another critical point is the level of skills required to run an automated and potent cybercrime. These skills are not readily available in every country, making its deployment to be selective and not general worldwide. The purchase of automation tools is also relatively costly, thereby making it difficult in developing countries. Overall, required skill level is a drawback for this characteristic.

\section*{2.4.4 Cybercrime as a Service}

The different demands of cybercrime encourage individuals to become more professional. Within the cybercrime context, Wall and Williams (2013) identified professionalism as the presence of specialists that conduct sophisticated and complex operations attached to human users and computer systems. Every online crime needs a different kind of expertise and skillset. Panda Security (2014) found that the FBI has identified ten dedicated professions within any cybercrime group. There are different types of professionals that provide specific services. For example, malware writers were contacted by criminals to develop malware and sell this on to criminals that were deployed across the Internet (Sood et al., 2013). The roles are essential within the life cycle of the crime, making each participant a specialist where they function (Rege, 2009; Whitty, 2015). Individuals are skilful in technical areas (such as programming, networking, and data analysis) and non-technical areas (such as language translation, money

\textsuperscript{18} Unique address for every device on the internet.
\textsuperscript{19} Information sent with a web page on the internet.
laundering, and document faking). These highly competent individuals and groups of people act professionally within the cybercrime industry.

There are globally identified markets for buying and selling goods (and services) derived from cybercriminal activities. In some cases, the markets (e.g. Darknet, Deep Web and Web forums) are online forums strictly directed at criminals (Leukfeldt, Domenie, & Stol, 2010; Odinot et al., 2016). Transactions in the market demonstrate the coordination and professional level at which cybercrime is conducted. Leukfeld (2017) has discovered that cybercrime markets provide distinctive services such as stolen data, cybercriminal tools, services such as escrow (money laundering across countries) services, and illegal trade. These markets offer different skills of dedicated experts.

Feedback on the services is also provided to ensure that the marketplace understands the quality of the goods and services on offer (Dupont et al., 2016; Holt and Smirnova, 2014). The feedback is usually in terms of service satisfaction rating. Hence, service professionals often realise the need to offer quality to sustain a good reputation in the various cybercrime markets.

On the other hand, professionalism is not unique to cybercrime, as service-oriented criminal activities have existed for a long time. Over time, roles such as drug mule, money launderer and assassin were previously offered as specialised services long before the Internet. Thus, cybercrime may have adopted age-long modes of operation that are used in traditional crimes. It further reflected the reality that although cybercrime is a new phenomenon, it still retains the characteristics of older established crimes in tandem with Grabosky’s (2001) perception. The only difference is the impact of this characteristic on criminal behaviour in its entirety. Professionalism liberalises cybercrime in an unprecedented way.

Liberalisation through service provision has reduced or eliminated the need for personal skills for criminal masterminds. Tabansky (2012) stated that the recent trend in cybercrime is outsourcing research and development, which reduces the skill set needed to become a cybercriminal. Any individual or group could purchase tools or services for any cyber-attack without having any personal input in the development. The technical knowledge barrier to participation is irrelevant to the use of a low-cost service-based model (Huang, Siegel, & Madnick, 2017; Manky, 2013). Because of the availability of skilled service providers, the competence needed for developing cyber tools is no longer needed.

Cybercrime-as-a-service (CaaS) has emerged from the increasing prominence of professionalism of cybercriminals. The ‘service-oriented approach’ is a significant contributor
to group-based criminal behaviour. Europol (2014) discovered cybercrime-as-a-service to be responsible for ‘traditional’ criminal groups becoming involved in cybercrime. The criminals use Dark Web markets, resulting in the acquisition of criminal services such as spam networks and botnets in launching DoS attacks against specific targets. This approach further enhances the development of customised malware for willing buyers (Nurse & Bada, 2019). This access to the tools and services has transformed our entire understanding of cybercrime and its conduct. The acquisition of tools and services has reduced the need for cybercriminals not to have technological knowledge.

Despite the declining requirement of skills (as argued in Section 2.4.1), some technical knowledge remained fundamental for cybercrime activity. The suppliers of tools and specialised services continue to be highly skilled individuals. Internet crime requires qualified individuals and high-quality deployed tools (Wall & Williams, 2013; Huang et al., 2017). The service-oriented characteristic has continued to mean that cybercrime activity still relies on highly competent professionals.

### 2.5 Criminological Theories applied to Cybercrime

The application of criminological theories adds a different perspective to the study of Cybercrime. The efficacy of previous criminological theories in understanding or identifying cybercrime patterns is fundamental (Leukfeldt & Yar, 2016). It directly influences the knowledge of these crimes. Adapting criminological theories to the technological nature of cybercrime remains an effective approach because of the limited suitable theoretical principles.

The characteristics and parameters of cybercrime continue to change, but the nature of these crimes directly reflect the theoretical explanation. These theories help understand the crimes in terms of motivation and mode of operation (Hong et al., 2013; Stratton et al., 2016). The different characteristics of cybercrime have influenced the way the crimes are understood and analysed.

The theoretical exploration further illuminates the sociocultural dimension of cybercrime. Okeshola and Adeta (2013) noted that theories are an integral aspect of sociological research because they state general principles that predict and explain events, observation, and facts. The sociological analysis concept relies primarily on the existence and discussion of different theories. Adesina (2017) noted that the social characteristics of developing countries could encourage cybercrime. The choice of Nigeria as a case study provides the basis for applying a
criminological theoretical framework. Nigeria demonstrates features that make it an exemplar case for cybercrime (see: Section 1.3).

Discussing cybercrime in Nigeria within its social characteristics helps to narrow the scope of this study. Criminological theory and its utility in studying cybercrime are not applicable in the absence of a technological context. The technical position of the country (see: Section 1.5.5) has contributed to the evolution of cybercrime in society. For example, Kraemer-Mbula et al. (2013) pointed to technological penetration and competence, two significant elements that foster cybercrime in developing countries. This argument highlights the socio-technical nature of cybercrime.

As society develops, the landscape of crime changes, which challenges the applicability of criminological theories. Like every other society, Nigeria will evolve in a way that criminology theories cannot predict. This growth can be explained from the theoretical perspective. In this section, a discussion of five theories (see Figure 3) exploring different angles of understanding cybercrime will be discussed.

![Theoretical Approach](image)

**Figure 2: Criminology Theories Adopted for this Research.**

### 2.5.1 Routine Activity Theory (RAT)

RAT emphasises victim and target exposure to potential attackers. In cybercrime, proximity is a tool for offenders and not a modus operandi. The Internet eliminated the importance of location as the distance between offenders, and cyber actions are almost “zero” (see Section
2.4.2). Targets require no temporal interaction with the offender to become victims. Kigerl (2012) elaborate that the RAT makes understanding cybercrime at a macro level easier because the three elements (a motivated criminal, a suitable victim, and the absence of a capable guardian) are relevant to the virtual world of the Internet.

Online behaviours by a target (or victim) can enhance the suitability of the victim. This behaviour includes risk-taking, time spent on online forums, time spent purchasing goods, time using social media, time purchasing online along in engagement with online banking (Choi, 2018; Pratt et al., 2010; van Wilsem, 2013). The Internet also increases the possibility of online harassment victimisation through increased exposure to offenders and infected files (Bossler & Holt, 2009). The vulnerability of Internet users contributes to their risk of becoming targets of cybercriminals.

However, RAT has not adapted to the unique characteristics of cybercrime. Broadhurst et al. (2014) highlight the level of offender resources as a fundamental aspect that can ascertain the execution of crime on the web. Resources such as hacking tools, social engineering skills, money laundering competencies and identity theft skills are required for cybercrime (see Section 2.4.1 and 2.4.4). The tools and resources that can be deployed are a significant element in the conduct of cybercrime (Broadhurst & Choo, 2011; Kigerl, 2012). For example, when an offender possesses access to fast internet and a sophisticated hacking tool, the convergence can result in a potentially high level of criminal activity. When a cybercriminal has just the motive but lacks the required skills, their ability to commit crime is limited. The absence of this factor weakens the overall suitability of RAT theory within the cybercrime context.

On the other hand, the basis for any victimisation reflects the ability of potential victims to exercise choice. The assertion that victims have a choice of not becoming a victim (Felson & Clarke, 1998) remains, in fact, a controversial topic in cybercrime. The theory presumed that more time spent online would increase the likelihood of victimisation (Kalia & Aleem, 2017). Evidence of data theft and banking hacks suggest that victimisation does not rely on routine activity online. Bossler and Holt (2009) noted that malware infection or distribution is not subject to online presence. Risk does not relate to the time spent on the internet. Some targets are not active on social media but have, nevertheless, seen their account hacked. In this light, the choice remains with the cybercriminal and not the victim.

Another critical angle to RAT adaptation to Cybercrime is the role of other factors in criminal activity. Some other parameters and factors influence offending, which RAT did not identify
For example, political, sociocultural, and economic factors could affect criminal behaviour (Leukfeldt & Yar, 2016). These elements are essential because they determine the involvement of individuals and recidivism. Thus, the application of RAT to cybercrime is not entirely appropriate.

Nigeria is a burgeoning location for cybercriminals. Therefore, the perpetrator element of RAT is evident. But the absence of guidance and presence of victims need to be discussed.

Firstly, the infrastructure and laws that uphold the safety of internet users are both weak and inadequate in Nigeria. As detailed in Section 3.4.1, there has been a struggle to establish effective law enforcement and security for citizens using the internet. This absence of effective regulation either by government, regulators or service provider has itself encouraged criminal behaviour. Without proper national guidance and security strategy, internet users are vulnerable to different types of security risk.

However, many other developing countries struggle to provide guidance and protection on the Internet. Muller (2015) established that weak cybersecurity implementation in developing countries is fundamental to sustaining criminal behaviour online. Dennis et al. (2014) cited Jamaica as having no formal national cyber-security policy.

Victims exist both in and out of the country. Nigerian businesses, government and individuals are targeted by cybercriminals and in 2018, Nigerian banks lost ₦15 billion (about £30 million) (Adesoji, 2019). Pawlak (2014) note that citizens also are targets of cybercrime. The government has itself been at the receiving end of significant criminal behaviour (see Section 3.3.1 for more details).

The Nigerian situation shows several weaknesses of RAT. Its failure to identify the role of technological penetration is reflected within cybercrime in Nigeria. Technological penetration exposes users to high-level attacks. The quality and nature of the infrastructure, software and hardware enhance the targetability of victims. With Nigeria having a high number of internet users demonstrates the role of technology in increasing crimes.

Another critical point in Nigeria is the lack of choice for potential victims. Kugler (2009) highlighted that weak technological infrastructure contributes to possible attacks on the information flow in developing countries. The government must have its processes on various internet platform as a necessity. Thus, the choice of becoming a victim is not suitable to the experience of the country. For example, conducting businesses online does not mean that the
government will be a victim of cyber warfare. Only the criminals will determine their choice of victims.

### 2.5.2 Strain Theory (ST)

The conduct of cybercrime can be affected by different types of strain. Cybercrime perpetration is a response to the poor economic situation of the perpetrators (Anyanwu & Obiyo, 2012). Economic hardship has always been associated with crime: e.g. the United Nations (2005) attributed arms trafficking and other crimes to strain from the alarmingly high economic problem of the West African region. For example, strain is linked with unemployment and poverty, forcing offenders into a life of crime (Ajimotokin et al., 2015; Cohen & Felson, 1979; Lageson & Uggen, 2013; Verbruggen et al., 2015; Virta, 2013; Warner, 2011). The strain experienced by deprived residents in developing countries may explain the popularity of fraud and other financially induced crimes.

The type of experienced strain can influence the nature of criminal behaviour. Unemployment has become a significant reason why cybercrime is increasing. In Brazil, unemployment and low social mobility were identified as being responsible for the prominence of cybercrime. (McAfee Centre for Strategic and International Studies, 2014a). In Eastern Europe, the economic downturn resulted in jobless, but skilful, individuals leading to high levels of cybercrime (Lusthaus & Varese, 2017). The prevalence of poverty and poor social infrastructure has influenced economic-focused cybercrime activity (Okunade & Shehu, 2015).

Also, other strains can promote cybercriminal behaviour: e.g. poor academic performance can result in peer isolation, and detachment is a strain that can encourage malicious behaviour online (Udris, 2017). This theory has provided evidence for explaining delinquent behaviour on the internet.

However, strain from a failure to fulfil the economic and educational aspirations is not entirely appropriate as an explanation for cybercriminal activity. Poverty is not necessarily the only reason for financial gain driven crime. In some cases, individuals with a job and not experiencing any hardship engage in cybercrime. It could be a choice (see: Section 2.5.4) or the result of social relationships (see: Section 2.5.3): e.g. unemployment was found not to be the only reason for criminal behaviour (Janko & Popli, 2015; Kleemans & de Poot, 2008; Van

---

20 A prominent antivirus company.

Furthermore, cybercrime undertaken by people of higher social, financial, and educational status is a significant gap area that this theory could not fill. In some identified cases, individuals with legitimate business interests and an unhindered path to fulfilling their goals are involved in cybercrime. For example, Colibasanu (2008) reported that Porsche complained against Volkswagen for spying on its Chief Executive Officer (Wendelin Wiedeking). Evidence of insider trading within companies does not reflect economic strain.

Also, Strain Theory puts every cybercrime into one group in which economic gain is the only motivation (see: Section 2.6.2 for further explanation). It did not cater to its heterogeneous nature. Different crimes exhibit different characteristics and contexts that could not be explained solely by strain theory: e.g. cyber warfare\textsuperscript{21} between governments is not compatible with any strain. Professional criminogenic behaviours (such as website defacement, cyberstalking and DDoS) are not concerned with the failure to achieve personal aspirations. Many cybercriminals are neither deprived nor inhibited in ambitions to achieve their goals.

Nigeria shows characteristics of ST as the economic condition, and the low level of career opportunities in Nigeria do stimulate cybercrime: e.g. the core motivation for AFF is financial gain. The core motivation for AFF is economic gain. The migration of the AFF to the web has given Nigerian cyberspace a reputation for breeding cyber fraudsters. Adesina (2017) noted that cybercrime in Nigeria is for economic gain, and victims were primarily located in foreign countries. The term “419” is generally perceived to be the template of cybercrime in Nigeria despite unverified evidence of these crimes coming from the country (Byrne, 2013). Nigerian scams primarily target individuals and organisations in developed countries.

Despite the evidence that Nigerian economy is experiencing high unemployment and poverty levels (see: Section 1.3.1), several cybercriminals are not poor. The involvement of both professionals and gainfully employed citizens attest that strain theory cannot be applicable in Nigeria. For example, bank managers have themselves been discovered to be members of cybercrime networks. The involvement of both professionals and gainfully employed citizens attest that strain theory cannot be applicable in Nigeria.

\textsuperscript{21} Cyberwarfare is the deployment of technology to attack a nation in a similar way to warfare.
2.5.3 Social Learning Theory (SLT)

The increasing application of SLT to cyber deviant behaviour reflects a recognition of its perceived relevance. SLT theory is increasingly prominent among cybercrime researchers (Heirman & Walrave, 2012; Ross & Weaver, 2012; Van Ouytsel et al., 2017a, 2017b). For example, Ross and Weaver (2012) discovered that observational learning was responsible for harmful behaviour in online games. Peer learning is the primary way that cybercriminals learn ways to target and attack internet users. Cybercrime adaptation of SLT demonstrates that peers who actively approve such criminal behaviour encourage the crimes, especially for the engagement of adolescents (Van Ouytsel et al., 2017a). SLT is therefore a theory that can explain a range of criminal behaviours including both cyberbullying and sexting.

However, learning through social interaction is subjective and may not apply to everybody. Yar and Steinmetz (2019) noted that numerous factors (such as attention, retention, reproduction, and motivation) must align before social learning can be effective. As this process is not uniform, its individual and personalised nature means that any degree of success is difficult to measure.

Additionally, ascribing cybercrime to SLT placed too much reliance on the impact of peers. Instances of cybercrime where peers are not involved demonstrate its limited relevance: e.g. Kane Gamble, a 15-year-old, hacked the computers of America’s most powerful spy chiefs (BBC, 2018). He did not learn from, or involve any of, his peers in doing so. Social learning could be secondary, as peer involvement is not always relevant.

Moreover, the impact of individual learning of technology must mean that the emphasis placed on peer impact will be diluted. The advent of free technological courses online provided individual pathways towards technical proficiency. Social learning becomes less critical and perhaps irrelevant, as individuals can develop their competencies without relying on others. As a result, SLT theory become questionable in terms of its overall relevance to cybercrime.

A further aspect of SLT is the prevalence of ‘virtual peers’ online. Given the current number of internet users, it is evident that peer relationships exist in a ‘virtual space’. Benson et al. (2015) stated that social media creates an avenue for virtual peers to collaborate and exchange information. Meldrum and Clark (2013) noted that virtual peer relationships are unsupervised and give unfettered means of communication that ultimately influence behaviour.
This relationship can either be strictly online but also develop into online-offline relationships. Warr (2002) presented young virtual peer groups where they can develop their sexuality, speech, and norms of dress tastes. Virtual peers can be in the life of a person for a long time and significantly influence the development of their attitudes and beliefs (Miller & Morris, 2014).

Virtual peers have a similar impact on traditional relationships. Holt (2009) established that virtual peers could influence individuals developing hacking behaviour. Holt and Copes (2010) discovered links between digital piracy and offline criminal behaviour from online relationships and interactions. They include prostitution and sexual abuse (Holt et al., 2010). Miller and Morris (2014) concluded that a virtual peer could be prominent in social learning while also impacting criminal behaviour development.

The development of cybercriminal groups, gangs or networks reflects social learning theory. Leukfeldt et al. (2017) investigated eighteen cybercrime networks and discovered that social contacts were responsible for the growth of thirteen of them. SLT is an essential means of criminal recruitment as gangs often focus on social relationship to attract potential targets.

The SLT theory assumes that every learned new information does not necessarily result in criminogenic behaviours irrespective of the platform on which the peers meet or interact. For example, the hacktivist group members often learn about attacking infrastructures worldwide (Macmanus et al., 2013). Cybercriminals often learn new skills to improve their enterprise. Every observational skill is primarily concerned with cybercriminals becoming more potent and enhancing their skills. Here the perpetrators of cybercrime learned skills are not interested in any knowledge that adds no value to their criminal behaviour.

However, some cybercrime requires little or no skills. Social learning could not explain these crimes as peer relationships did not form part of the criminogenic behaviour. In the case of Cybercrime-as-a-service (see: Section 2.1.3.4), the skills are not critical, making social learning irrelevant. For example, managers of government cyberteams are usually politicians with no skills fostered by social learning. Criminal masterminds do not need any observational learning when it is possible to combine various professionals for a planned crime.

Also, SLT becomes less relevant to cybercrimes that are not technical. Cybercrime from within an organisation requires no technical knowledge but only the misuse of access and information. Thus, internal crime in organisations is difficult to relate to SLT because the perpetrators need no peers or any technical knowledge (Omodunbi et al., 2016). They already have access, and
their involvement does not require any extensive technical knowledge. SLT theory has only limited relevance within the context of cybercrime.

It is crucial to discuss SLT in the context of the role of the cybercafé, which dominated access to the internet in its early days in Nigeria. In the mid-1990s, the number of cybercafes grew in different cities in Nigeria and strengthened the silos of cybercrime groups (Sodiq, 2012). They contributed to both technology adoption and malicious use in Nigeria. Nuhu Ribadu (the former chair of the EFCC from 2003-2007) noted that cybercafes dominance of the early Internet access in the country enabled the transformation of offline based AFF to cyber mail fraud (Ribadu, 2007).

However, the advent of GSM (see: Section 1.5.5) technology in the country since 2001 has reduced the impact of cybercafes in the perpetration of cybercrime. The demise of numerous cybercafés was caused by a sharp drop in their patronage (Osho & Adepoju, 2016). Individual connections are now steadily growing with low-cost internet and computer systems (Obuh & Babatope, 2011; Tiermo & Nelly, 2016). Thus, cybercafes have lost their role and reputation for communal and social gathering.

The social learning associated with cybercafes has also been adversely affected by the increasing technological penetration. Individual connection to the internet implies that social learning in cybercafes is on the wane, which undermines the relevance of the theory. Technology remains the core element, but access to the internet has changed criminal conduct dimensions, as cybercriminals are not relying on peer approval or social relationships. These features demonstrate the progressive weakening of the SLT within cybercrime in Nigeria.

2.5.4 Rational Choice Theory (RCT)

RCT theory demonstrates how value maximisation may influence cybercrime. Crimes online remain attractive when the benefits outweigh any perceived loss. According to Pittaro (2007), a high-value realisation by offenders makes cybercrime highly attractive. Electronic crime rewards can be enormous compared to the cost as it provides many potential victims. Leukfeldt (2017) acknowledged that the likelihood of detection and punishment of internet crime is minimal and probably much less likely than traditional crime.

From the perspective of cybercriminals, the benefits of this crime are much higher than the cost. From a rational choice point of view, cybercrime pays more than traditional crime and involves lower risk (Boes & Leukfeldt, 2017; Holt, Smirnova, & Chua, 2016; Hutchings &
Clayton, 2016). For example, warning banners as a deterrent to cybercriminals is not a costly deterrence (Maimon et al., 2014). Deterring cybercriminals also remains highly inconsistent. However, RCT theory does not adapt to the possibility of cybercrime using proxy activity or that of a group. Higgins (2011) stated that not every crime on the web is rational as other factors and situations might be responsible. A coordinated attack resulting from peer pressure can be responsible for coordinated internet attacks. The individualistic approach of this theory does not recognise organised crime that occurs in coordinated attacks such as DDoS. Within organised crime (see: Section 3.4), RCT cannot be a significant determinant of cybercrime. The growing possibilities on the internet have served to attract traditional organised crime groups because of its seemingly low risk and potentially high financial and material benefit (Viano, 2017). Thus, rationalised thinking is replaced by loyalty to peers and the group.

A further critical issue is that RCT does not account for the significance of anonymity by internet users in understanding Cybercrime. The anonymity of the web influences the perspective of the participants by highlighting the low level of risk attendant to committing crimes online. For example, cyberstalkers regard their anonymity in evaluating their risks and prospective rewards before committing the crime (Cornish, 2010). Thus, anonymity promotes the belief of invisibility that reduces the associated cost in the eyes of cybercriminals.

Also, other factors are beyond the scope of RCT while discussing how cybercriminals arrive at their decisions. These factors include speed of connection, cost of internet access, skill level and internet characteristics. The internet generates different issues beyond what was foreseen in the development of RCT.

A further area in which RCT fails is apparent in terms of state-sponsored cybercrime. State-sponsored cybercrime is prominent, with offenders usually being shielded by their respective nations (Blinderman & Din, 2017; Lotrionte, 2014). This type of crime does not offer a cost-benefit analysis and are in no way individualistic in nature. An attack in this category needs to focus on a rationalisation of the malicious intent of the states involved.

This theory falls short in identifying the role that knowledge and competency play in the conduct of cybercrime. When the tools available for the crime make a perpetrator almost invisible, the rationality of these acts might be irrelevant. Tabansky (2012) noted the development of tools for sale online as now being almost rampant. High tech cybercriminals are not easily caught because their activities are sophisticated, which minimise the likelihood of detection or arrest.
Rewards for their activities are evident for cybercriminals in Nigeria. Byrne (2013) reported that financial gain is significant and has made crime on the internet increasingly attractive. In recent times, society has become more receptive to cybercrime with an increasing appreciation of proceeds from these offences. It is worth billions of naira in terms of financial gain. The quest to live a spendthrift lifestyle and buy high-value cars has undoubtedly encouraged many youths into cybercrime (Adesina, 2017).

The perceived benefit of these crimes has disoriented the moral compass of many Nigerian citizens. The earlier honoured African moral rectitude and culture of chastity have been abandoned as materialism, selfishness, and greed have become more dominant (Okunade & Shitu, 2015). Young people see cybercrime as the core avenue for social mobility to attain prominence within society.

A further aspect is that the cost of the crime, as explained by RCT is, in this context, of limited value. The Nigerian state has failed to control cybercrime. The rate of criminal perpetration is exceptionally high and outstrips the rates of arrest and prosecutions. Corruption (see Section 3.6.3) and failure of law enforcement (see: Section 3.5.1) also contribute. The elite in society influences the criminal justice system (Adogame, 2007; Ibrahim, 2016b; Odumesi, 2015). Weak law enforcement reduces the perception of cost, making benefits more evident.

However, the weak cost of these crimes is not limited to Nigeria. Button et al. (2015) investigate the views of victims on the sentencing of fraudsters and discovered that the sentencing does not provide corresponding impact as the seriousness is challenging to measure. The inability to provide commensurate punitive measures reduce the perception of cost while strengthening the perception of cybercriminals.

### 2.5.5 Techniques of Neutralisation

It is also recognised that delinquents may use techniques that neutralise the social controls that might limit or check the perpetration of cybercrime. Jantz and Morley (2017) note that offenders can be committed to conventional norms but that they neutralised these principles by concluding they are unimportant, irrelevant, or inapplicable. The techniques of neutralisation enabled offenders to evade blame from others (Froggio et al., 2009). It ensures offenders

---

22 The victims were in the United Kingdom and their response is based on the judgements and punishment given to convicted cybercriminals.
maintain their positive self-image. These techniques are used to justify the act but are not necessarily acceptable before the law or societal norms.

This theory proves to be limited in application as it fails to identify factors that directly influence the way that humans think. Social background and environment are essential in determining deviant behaviours. It disregards factors that are important in the thought process and decision making of criminals. The factors include age, ethnic group, social class, and gender. Hence, the theory of neutralisation is limited because of the emphasis on the outcome. It does not acknowledge those factors that are subjective to individual cybercriminals.

Cybercrime is a context where this theory has been explored. Aiken et al. (2016) note that neutralisation theory provides a direct insight into explaining why adolescents might be involved in hacking behaviour. For example, Bryan (2014) and Siponen et al. (2012) discover that an appeal to higher loyalties and a rejection of critical opinions is the most compelling justification in software piracy offending. Cybercriminals also often exhibit neutralisation by denying inflicting any physical injury to their victims. Offenders will argue that victims are “worthy”, mainly when the motivation is revenge (see: Section 2.6.5) or political (see: Section 2.6.4). Cybercriminals may also blame victims who are gullible or attracted to financial reward that may reflect evident greed. The attribution of greed to victims (see: Section 2.6.2) enables cybercriminals to neutralise their crime. In the case of hackers, the neutralisation process is strengthened by the belief that victims are unknown and not fatally affected (Morris, 2011). The justification for hacking is usually subjective and does not reflect the norms in their immediate society.

Despite the examples and discoveries generated by much research, cybercrime continues to provide a significant challenge for this theory. The neutralisation can be applied before or after the crime (Morris, 2011). Determining when the perpetrators use neutralisation remains a significant challenge. Its application after the crime presents the justification as a means of rationalisation rather than the original basis for undertaking the crime.

Also, the techniques of neutralisation are not adaptable to Cybercrime because they failed to consider its unique elements. Some of these elements include internet access, borderless communication, regulation, and communication speed, which remain very important to online criminal behaviour. Failure to accommodate these features suggest limitations in its adoption for understanding internet crime.
Overall societal acceptance of this criminal activity is also contributing to the growth of cybercrime. In Nigeria, cybercrime has become a ‘societal norm’. In the form of sociocultural values transmitted to the younger generation, socialisation is now being used by parents to encourage their children to engage in crime (Meke, 2012).

Two areas that demonstrate this are the fashion and the entertainment (music) industry. Ekeji (2013) noted that the fashion industry had contributed designs labelled Yahoo shirts that depict a taste or style of young people with money and contribute to the expensive and lavish lifestyle of cybercriminals. The music scene is also a major contributing factor to the neutralisation of guilt among cybercriminals. Music has the power to transform society (Christopher, 2012), but Nigerian society has become receptive to its excesses. Cybercrime is encouraged through the lyrics of songs released in Nigeria (Tade, n.d.). It has become a common occurrence for artists to praise cybercriminals in their albums. With the prevalence of media-induced support for illicit cybercrime, young people continue to see it as a positive and acceptable way of life.

A critical point within the social acceptance argument and theory of neutralisation is the focus on financial crime. But motivation for cybercrime goes well beyond making money. The failure to acknowledge other rewards creates a gap for criminals not just motivated by monetary gain. In the situation where altruism is the motivation, the impact of fashion or the music industry cannot neutralise the feeling of guilt. Hence, there are significant limits to understanding cybercrime in Nigeria by applying the theory of neutralisation.

2.6 Motivations for Cybercrime

Motivation is the reason for the behaviour of an individual. Guay et al. (2010, p. 712) define motivation as “the attribute that moves us to do or not to do something”. This definition comes from the basis that every human behaviour is driven by underlying behaviour. It is a combination of closely related interests, values, perceptions, and beliefs.

Motivation has three implications for cybercrime. Firstly, it influences the nature of the crime. Motives affect crimes such as romance scam, phishing, inheritance scam, fake news, cyber-espionage, and pharming. Making money is a core motive and leading cause of cybercrime (Bernik, 2014; Olowu, 2009). It contributes to crimes like sextortion, where people are bullied and threatened for monetary benefit. Kopecky (2017) states that child blackmail online is

---

23 Phishing is the fraudulent practice of sending emails purporting to be from reputable companies to induce individuals to reveal personal information, such as passwords and credit card numbers.
driven by the ulterior motive of the criminal. Motivation determines the expected outcome and the type of crime committed on the internet.

Secondly, motivation influences the targets of crime. Cybercriminals have used their motive to select their targets. The situation of victims remains fundamental to the crime. Findings from research on 106 countries by Hui et al. (2017) show that DDoS attacks in the banking, ICT and telecommunication sector are driven by financial motivation. For example, the motivation to retrieve valuable trade secrets or intellectual properties can influence cyber espionage by competing companies.

Thirdly, motivation influences the process of crime. As Kaur (2013) explained, motivation drives the action of humans and determines the way they apply themselves. All criminal behaviour hinges on the reasons and justifications for the criminal act. A cybercriminal selects the process of crimes based on such grounds (McGuire & Dowling, 2013). For example, a cybercriminal driven by political considerations will use high technology tools to attack government networks such as websites, services, and offices. The influence of motivation on Cybercrime is fundamental in its perpetration.

Based on these factors, it is essential to consider the various motives for engaging in cybercrime. Putting every category of cybercriminals into a single homogenous level of motivation is never appropriate (Holt, Freilich & Chermak, 2017). Andersen (2012) noted that cybercrimes have numerous players that have vastly different kinds of motivation. In this research, five applicable incentives have been selected based on their contextual relevance.

2.6.1 Altruism

Altruism as motivation is a subject of debate among scholars, as many cybercriminals have argued this in their defence. Their drive is to perform social good and not for selfish or illicit reasons. Some arrested criminals claimed their exploitation of massive data repository from large organisations is to highlight the flaws and to recommend improvement (Broadhurst et al., 2014). Hence, their gain is to use the skills to better humanity and not with criminal intent.

The personal belief of self-realisation can also influence this motivation. Some exceptionally skilled cybercriminals continue to believe their activities benefit others and make the world a better place. The case of Aaron Swartz pointed to the view that making information freely available could be criminally interpreted despite evidence of altruism (Abelson et al., 2013).
The motivation for hacking the JSTOR was to make the publicly funded research journal articles free. Armin et al. (2015) stated that the provision of data or information online could be motivated by altruism. It could provide the rationale for hacktivism as suggested by the perpetrators. Some cybercriminals have used the proceeds of crimes for social good and developing their community. Hacking tools that do not endanger the public but expose online security risks have a motivational offshoot that is altruistic.

Society could see altruism as a factor driving cyberattacks as good practice. However, this activity usually results in criminal behaviour. Improving the welfare and interest of others through illegal behaviour on the internet remains a criminal act. Any infringement of the law on the internet remained maliciously motivated (Balajanov, 2018). Altruism is never a viable motivation for cybercrime. For example, Olumoye (2013) argued that “hacktivists” are not altruistic because they promoted chaos and terror. The impact of these acts is significant and adverse on many victims that have not previously committed crime.

Despite social good being the perceived goal, altruism cannot justify the criminal thought and impact on victims: e.g. when government systems are hacked and confidential information released, the innocent victims are not in government but have been wrongly affected.

2.6.2 Financial Gain

Financial gain is one of the most popular and generally agreed motivations of cybercrime. This motivation remains as old as the internet. Fraud and financial reward are the reasons for crimes such as identity theft and phishing. Fraud over the internet is of significant concern because of the monetary gains (Lavorgna & Sergi, 2016). McGuire and Dowling (2013) note that crimes are often aimed mostly at financial income or personal profit. For example, malware deployment for accessing bank accounts are used to withdraw money illegally.

"Fraud is the Daughter of Greed"

The quotation attributed to John Grant has characterised the primary public perception of cybercriminals. Scholars argue that greed provides financial motivation for these crimes (Agwu et al., 2018; Balogun et al., 2010; Broadhurst et al., 2014). Recidivism by cybercriminals and increasing perpetration by those who have gained from crime are they argue a result of greed.

---

24 JSTOR is a digital library containing digitized books and other primary sources as well as current issues of journals.
Even when perpetrators have attained economic sufficiency, they continue the crime to satisfy their insatiable desire.

The emphasis on greed can be subjective or based on a moral perception rather than an objective analysis. Some cybercriminals require continuous financial gain from their enterprise because of their environment or location (Mustard, 2010; Nicholson & Higgins, 2017). In developing countries where every citizen is provided with their basic needs such as shelter, power, security, education and healthcare, the flow of financial income through crime may be the reason for recidivism. In some instances, the cybercriminal caters to the needs of members of the local community. Hence, the sense of responsibility and the environment can be a significant driving force that is wrongly perceived as greed.

2.6.3 Psychosocial motivation

Psychosocial motivation is also evident within the cybercrime context. Cybercriminals can be motivated by the need to exercise both emotional and mental punishment on victims. Ibrahim (2016b) stated that crimes such as cyber rape, cyber harassment, and cyberstalking are motivated by the desire to inflict psychological distress. Based on the binary classification of motivation, non-financial motivations are psychosocial because they do not rely on monetary gain. Berson (2003) noted that benefits retrieved from the sexual exploitation of internet users could be psychosocial. Hence, the perpetrator is motivated by threatening the mental and emotional health of the victim.

The benefits derived from this are psychological, which make it difficult to detect or measure. Crimes that are driven by non-financial motivation consist of intense emotional sensations and elements (Ibrahim, 2016a). The psychological satisfaction of making the victim suffer directly fuels the motivation of perpetrators (Li, 2017). It is a highly emotional crime, and the perpetration often arises from a revenge motive (see Section 2.5.5). It is due to mental illness or child abuse experienced by the cybercriminal.

The effect on victims is highly significant because it directly victimises their personality, emotions, psychology, health, and relationships. Wolak et al. (2008) stated that significant emotional sensations resulted in the use of violence and fatalities. For example, Gabrielle Green committed suicide because of criminal behaviour experienced online from those who derive psychosocial pleasure from their acts (Lynch, 2018). This motivation could escalate and go beyond the intended intensity of the perpetrators.
However, this motivation is not new to cybercrime either. It existed offline long before the advent of the internet as cybercriminals exploit human weaknesses. The online psychology-based crime exhibited patterns that are similar to what obtainable offline. It is a potent reason that made the internet a dangerous place for psychologically and emotionally unstable users.

2.6.4 Political Motivation

Political motivation has always been driven by the need to target a government in protest. It is a complex motivation to detect because the perpetrators and the intent can be elusive. For example, neither the source nor the intent of the Estonian government hacking in 2007 (Button, 2013; Jackson, 2013) was discovered. This motivation is complex and can be explored only by adopting a contextual perspective. A review of scholarly articles and discussion present two aspects of this motivation.

The first aspect is the activity of an individual who uses their online base to serve as an activist against political arrangements in the country. Targeted attacks arising from this are often aimed at conducting political sabotage and subversion (Burns, 2017). Individuals or a group of individuals may be politically motivated, resulting in them either disclosing vital information, campaigning against the government or even attacking government infrastructure. Arabo (2015) cited the online hacker group “Anonymous” as having a political agenda in their attack pattern. The primary focus of this motivation is to score political points.

The second type is state-sponsored motivated cybercrime against other countries. Some cybercriminals are encouraged into cyberattacks by the loyalty to their nation, thereby sponsored to launch cyber warfare (Kshetri, 2013). This motivation involves a perception of political supremacy among other countries. For example, Bernik (2014) noted that computer systems in the United States and Asia were used to launch a cyberattack on the Estonian government infrastructure in April 2006. Israel and Iran continue to engage in cyber warfare (Melman, 2020). In some cases, there are criminal accusations made against intelligence service officials for illegal activities against the economy and government infrastructures of other nations. Theohary and Rollins (2015) labelled these actors as cyber terrorists motivated by the support they received from the state.

Scholars have acknowledged the political motivation for cybercrime (Dalla & Geeta, 2013; Hill, 2018; Jackson, 2013; Schmidt, 2013). It remains an underdeveloped research area in criminology. The actions of individuals could be morally justified and usually argued as induced by their status in posterity. However, this behaviour usually infringed the law, which
exposed them to severe criminal sanction. Actors engaged in this, such as Bradley Manning, Edward Snowden and Julian Assange, have demonstrated why politically induced motivation remains highly problematic.

The engagement in cyberwarfare for political reasons is often reported but not substantiated by any official acknowledgement. It is usually subject to speculation and affirmed by experts. However, crimes induced by this motivation are generally officially denied. It creates a significant problem in understanding the degree of influence that political motivation of governments has on criminal behaviour on the internet.

### 2.6.5 Revenge

Revenge is another motivation that is assuming greater importance in the criminological understanding of cybercrime. This motivation manifests in different ways. The first is seeking revenge via child blackmail. Kopecky et al. (2014) discover that online blackmail victims confessed to having been part of the same crime, thereby sustaining the crime cycle. In most cases, victims often turned into offenders. Revenge often stems from the desire of the child to seek revenge based on previous experience or a desire to experience a similar feeling to that experienced as a victim (Kopecky, 2017).

Another form of revenge motivation may be linked to economic frustration. Broadhurst et al. (2014) cited an arrested cybercriminal who stated that the loss of jobs created the motive to attack businesses. It is claimed that the most dangerous hackers are unemployed Russian cyber specialists (Karatgozianni, 2010). It could represent the fulfilment of one or more of the needs identified earlier by Maslow (1954). A lack of esteem could result in negativity among employees or society. These attacks serve as a means of earning respect in the hacking society while enhancing their confidence simultaneously.

Additionally, revenge passion is another form of this motivation. It remained prominent in sexual crimes where an ex-lover maliciously targets individuals through criminal activities such as cyberstalking and revenge pornography. Leukfeldt et al. (2017) identify passion as a primary reason for committing these cybercrimes. Different people have weaponised the internet in committing a passion-driven vendetta against other individuals.

One of the most prominent areas in which revenge has become notorious is revenge pornography. Aston (2012) for example, reported a case of an ex-boyfriend posting nude
pictures of his former lover as revenge for jilting him. Many similar cases exist globally as former partners and individuals continue to victimise people.

There are other facets that revenge motivation can take in cybercrime. Arora (2016) found revenge from dissatisfied former employees using privileged information to commit crimes against the company. Armin et al. (2015b) reported that countries could exercise revenge attacks against another using cybercrime. Revenge cannot be ignored in the discussion of motivation as it reflects the different core areas of human lives.

2.7 Modes of Operation of Cybercrime

Cybercrime implementation combines both social and technical qualities. It is socio-technical in the mode of operation and impact. The method of operation requires critical analysis of the two elements in the processes of cybercriminals. There are human actors in the cybercrime ecosystems including promoters, preventers, victims, and offenders. It is characterised by the socio-technical interactions involved in the crimes. The crimes occur in a cyber-physical context, thereby integrating the social and technological aspects of the human actors.

Despite the prominent acknowledgement of the socio-technical quality of the crimes, this is not necessarily always true. Cyber-dependent crimes (see Section 2.3.4) often have limited or no interaction with the physical space of humans: e.g. the cyber-warfare among states where the target is only technical infrastructure without inducing any human casualty. Also, the purported use of Stuxnet (a malware) to disrupt the nuclear program of Iran demonstrates the lack of social impact of cybercrime. The sophistication of the crimes potentially negates the socio-technical nature of cybercrime.

Another reality is the symbiotic relationship between the technology and social dimensions of cybercrime. Both dimensions inseparably influence each other. For example, unemployment, a social phenomenon, has been associated with cybercrime (Adesina, 2017; Kshetri, 2013). Also, technology penetration may itself create a social impact. For example, the ransomware25 attack on the National Health Service (NHS)26 directly affects the public health service in the UK. Pawlak (2014) noted that advances in cyber capacity are fundamental to developing social, political, and economic spheres. The Internet possesses massive potential for inclusive socio-

---

25 Ransomware is a type of malicious software designed to block access to a computer system until a sum of money is paid.
26 National Health Service (NHS) refers to the Government-funded medical and health care services that everyone living in the UK can use without being asked to pay the full cost of the service.
economic development and growth. Yet, the social impact remains an absolute risk, as does technological penetration introduced into society.

Crimes such as fraud, cyberbullying\(^{27}\), cyberstalking\(^{28}\) have both a social and technical side to their perpetration. Despite acknowledging these crimes, they continue to occur and remain an integral part of the future of the internet.

### 2.7.1 Technological Development and Dimensions

Technology remains fundamental to cybercrime but comes in different dimensions. Some aspects of technology discussed earlier include the technological effect on classification (see: Section 2.3), the role of technology in terms of definition (see: Section 2.2) and the skills for implementation (see: Section 2.4.1). Technological penetration is the focus of this section. The impact of technological penetration contributed to criminal behaviour in terms of perpetration and victimisation.

Technological competencies have enhanced the propensity and commitment of cybercrime. Technological availability and new network-reliant services provide numerous advantages for society (Gercke, 2012). While the benefits of technology are evident in productivity, health and environmental improvements, the negative impact remained prominent in expanding cybercrime. Li (2017) noted that internet usage expands and allows perpetrators to acquire more skills in criminal behaviour. It provides various means for conducting crime that will only advance as people and organisations continue to embrace technology.

Also, technology expands the risk and vulnerabilities of every user on the internet. It has also reduced the entry barrier for criminogenic activity (Hargreaves & Prince, 2013). The various possibilities and activities online have opened a new risk platform for crime. For example, the adoption of electronic processing exposed Adobe to hacking in 2013. The recent prominence of video conferencing exposes numerous users to hacking and intrusion. Technological penetration provides different dimensions of victimisation in an unprecedented manner.

There are different patterns of implementation. The mode of operation can be derived from the dual classification by McGuire and Dowling (2013). Cyber-enabled crimes include phishing, romance scam, business email compromise, identity theft, card fraud, and other crimes that can

\(^{27}\) Cyberbullying is the use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature.

\(^{28}\) Cyberstalking is the repeated use of electronic communications to harass or frighten someone, for example by sending threatening emails.
be committed traditionally. Cyber-dependent crimes include hacking\(^{29}\), database intrusion\(^{30}\), DDoS, website defacement\(^{31}\), Ransomware, cyberespionage\(^{32}\), and others that depend on internet technology.

### 2.7.2 Social Dimensions

There are many areas involving social dimension of cybercrime. Some were discussed earlier and included economic hardship (see: Section 2.5.2), social learning (see: Section 2.5.3), and motivation (see: Section 2.6). This section focuses on organised crime (OC) in the perpetration of cybercrime.

Organised groups are becoming prominent in the conduct of cybercrime. Historically, OC captured the attention of the press, television, movies, and media internationally (Pinotti, 2015). For example, Italy has the Sicilian Mafia, Escobar has the Colombia OC while Joaquín Guzmán (El Chapo) controlled the Sinaloa cartel in Mexico. The evolution of crime resulted in the emergence of different organisations. OCs directly normalised criminogenic behaviour by encouraging the subculture. McGuire (2012) argued that cybercrime trends reflected the fourth significant era of OC by combining both offline elements and digital tools. The OC migration to cyberspace has however, continued to gain attention.

Defining OC is subjective and based on the perspective of the individuals or organisations explaining its meaning. After extensive consultation and scholarly research, Varese (2010) explain OC as the attempt to control and regulate the illegal production and distribution of an illicit specific service or commodity. OC is about governance and the creation of hierarchical authority of the criminal community. Criminal organisations operate using intimidation, killings, and terror to obtain power and territorial control (Lusthaus, 2013; Varese, 2010). OC creates an established illegal market for criminal behaviour, control and proceed.

Organised groups have been recorded in conducting cybercrime. OC in cybercrime implies that offline groups are operating online. Lusthaus (2013) cites the first Russian cybercriminal trading forum (Carder Planet), having various mafia titles such as Capo (“Captain”). Groups such as the Colombian cartels, Brazil’s PCC, organised crime groups in Malaysia, and Chinese gangs have diversified into cybercrime (Choo & Grabosky, 2015; Kshetri, 2010a, 2013).

---

\(^{29}\) Hacking is the gaining of unauthorised access to data in a system or computer.

\(^{30}\) Unauthorised and malicious access into a database

\(^{31}\) Website defacement is an attack transform the visual display of web pages or website.

\(^{32}\) Cyberespionage is the use of computer networks to gain illicit access to confidential information, typically that held by a government or other organisation.
Grabosky (2015) argues that a significant number of notorious cybercriminals now work in a group. Online trading forums are the most documented and visible cybercrime organisational formats. Lusthaus (2013) notes that this forum usually demonstrates a clearly defined agenda and hierarchy. They formed a close-knit social group for committing cybercrimes. McGuire (2012) stated that the social threat of cybercrime hinged on the evolving engagement of OC. The possibilities that abound on the internet fuelled the argument of the organised nature of many cybercrimes. In some cases, attacks on the internet can be initiated simultaneously from different locations. The involvement of many participants indicates the engagement of OC, especially in big scale crimes.

But the concept of OC is also perhaps a convenient definition in law enforcement and government representation of crime. OC is a catchphrase to enhance public anxieties about illegal markets and their increasing impact on political institutions and legal economy (Hobbs, 2013; Lavogna & Sergi, 2016; Sergi, 2016). The rhetoric in International and European public discourse lacks evidence. There is limited evidence or statistical support for the prevalence of OC among cybercrime perpetrators. The involvement of many individuals or groups of people cannot be regarded automatically as OC. It is a fundamental misrepresentation by law enforcement around the world. Admittedly, a typical cybercrime combines considerable skills and expertise. It is only friends and acquaintances that engage in criminal behaviour and not an established cybercriminal gang. Some of the OC characteristics include division of labour, collation of financial investment, and commitment of the crime on a commercial scale (Choo & Grabosky, 2015; Sergi, 2016). Most of the crimes do not demonstrate the scale where their actions might be depicted by Lusthaus (2013) to resemble La Cosa Nostra’s organisations (Sicilian Mafia).33

Besides, there is insufficient agreement about OC within the cybercrime context. Lavorgna and Sergi (2016) state that individuals could exploit cybercrime without necessarily requiring groups for its perpetration. McGuire (2012) found that an average of the 6-member group was responsible for the core of numerous cyberattacks. Associating OC with cybercrime fails to attract empirical findings that could generate any consensus among criminological researchers. Lavorgna and Sergi (2016) note that inferences from previous studies are misleading as a varying number of perpetrators are involved in various crimes. They cannot find substantial evidence that new cyberspace criminal actors created organised groups or whether traditional

33 Highly prominent Italian mafia
OC groups now operate in cyberspace. Instead, Martin (2014) and Wall (2014) discovered that cyberspace organisation is a loose, flat and fluid network with no general functional unit. Thus, OC within a cybercrime context remains mostly unproven. Scholars fail to reach a substantial level of confidence that OC is present in cybercrime. Most groups at best remains a loosely organised enterprise without strict internal rules or ethics.
Chapter 3: Understanding Cybercrime in Nigeria

As explained in Chapter 1, Nigeria is a viable case study (see: Section 1.3). The country is a prominent cybercrime source and possesses ethnocultural, socioeconomic, law enforcement, and technological characteristics, which influence cybercrime development (Ibrahim, 2016a). Using available literature, this chapter first gives an overview of Nigeria and then discusses cybercrime in the country using different criminological concepts.

3.1 Overview of Nigeria

Nigeria is a West African country of some 190 million people (World Bank, 2019), with various languages and cultures. English remains the official language, although several hundred other languages are spoken. Nigeria’s value system derives from the diversity of its people, religion, and cultures:

“The elements of this (the Nigerian) value system include respect for elders, honesty and accountability, cooperation, industry, discipline, self-confidence and moral courage.”

(Nigerian National Planning Commission, 2005)

Nigeria has adopted democracy in 1999 with a presidential government system. It has six geopolitical zones, each consisting of six states. It has three arms of government: Executive, Legislature and Judiciary.

3.1.1 Economic Situation

The Nigerian economy is currently struggling. The traditional reliance on Agriculture has declined in recent years. The nature and status of some aspects of the economy provide an insight into its potential influence on cybercriminal activities.

Human Development

The economy is characterised by dire conditions, including unemployment, poverty, and a high inequality level (Oburota & Olaniyan, 2020). In 2018, the Human Development Index (HDI)\textsuperscript{34} score of the country was 0.534 (UNDP, 2019). This score meant the country is in the low human development category with 158 out of 189 countries and territories. With 75 million illiterate adults and 10 million out of school children (Vecchiarelli, 2018), the country is struggling for productivity. Health care is also poor, with infant mortality rate of 74 out of 1000

\textsuperscript{34} The HDI is an average measure of basic human development achievements in a country. Areas of interest include inequality in income, inequality in education and inequality in life expectancy at birth.
births (Plecher, 2020). In the country, 17 per cent of hospitals have no access to any water source, while 45 per cent do not have basic water supply services (NBS, 2019d).

Poverty and unemployment are two core economic challenges of the country. At the second quarter of 2020, unemployment was 7 per cent and youth unemployment 34 per cent (NBS, 2019b). It was reported that 40 per cent of the entire population (out 83 million) live below the country’s poverty line of N137,430 (about £200) per year (NBS, 2019c). The World Poverty Clock report that over 105 million Nigerians (51 per cent) experience extreme poverty by living below $1.90 (about £1.50) per day (World Data Lab, 2020).

Fiscal Economy

Because oil is essential to the economy, it generates over 75 per cent of government revenue (Nweze & Edame, 2016). Any fall in the crude oil price has a profound economic effect. In 2016 there was a 25 per cent revenue loss because of the drop in global oil prices (Ahmed, 2019). It results in government not meeting its obligations or invest in critical infrastructure. Moreover, successive governments, despite the abundance of oil reserves, have not invested in refining capacity. So much so that Nigeria is the largest importer of petrol and diesel. It is evident in the fall in the value of the Naira\(^{35}\), which in turn feeds into inflation, is currently at 12 per cent (Central Bank of Nigeria, 2020) and expected to rise.

The basic needs of people are becoming more expensive: the price of Kerosene - a popular household cooking energy source - continues to increase, making life hard for the average family (Uche, 2020). Food inflation remains high, thereby weakening the purchasing power of the citizens. A year-on-year food price resulted in 26 per cent increase for tomato, 5 per cent for eggs, 79 per cent for rice, and 29 per cent for yams (NBS, 2020a). The average fare paid by commuters for bus journey within cities increased by 63 per cent year-on-year. Also, 24 per cent increase is recorded for Inter-city bus journeys, and air travellers experience a 20 per cent increase (NBS, 2020b).

3.1.2 Agriculture

Agriculture in Nigeria is struggling despite having 79 million acres of arable land (Nwajiuba, 2013). Initially, agriculture was a significant employer across all of Nigeria (Ogen, 2007). At independence, the country was the second-largest exporter of cocoa and palm oil. Cotton, hides and skins, rubber and groundnuts were also significant exports. Agriculture was responsible

\(^{35}\) Nigeria’s local currency
for 55 per cent of GDP and employed 70 per cent of the adult workforce. The sector was labour intensive, and unemployment was minimal (Alkali, 1997).

However, the coming of oil made agriculture less important, agricultural production dwindled, resulting in the need to import food. The growth rate of the agricultural sector remains low (Nwajiuba, 2013). About 80 per cent of farms are used for subsistence farming (Ayantoye et al., 2011; Ebhuoma, 2020; Omona & Agoi, 2007). There are some recent government action improvements, but much remains to be done in this sector.

3.1.3 Rural-Urban Migration

Like other developing countries, Nigeria has seen massive urban population growth at the rural settlement expense. In 1974, 75 per cent of Nigerians living in rural areas (Sulaimon, 2014). However, the urban population grew to 51 per cent by 2011 (Nwajiuba, 2013). Figure 2 identifies the factors responsible. This migration has fuelled the rise in urban poverty and crime because of few job opportunities. Migrants find it challenging to find city jobs as they lack the required skills (Abbass, 2012; Pam, 2014). The failure to access job opportunities has given rise to insecurity by theft, armed robbery, and housebreaking.

Figure 3: Factors for rural-urban Migration in Nigeria (Ajaero & Onokala, 2013; Aworemi et al., 2011; Jamila et al., 2009; Nwajiuba, 2013)

Even when the migrants are employed, they are usually in low skilled paying jobs. Those employed often engage in criminal activities to afford the high cost of living in urban areas.
Most of the employed have numerous dependants requiring them to look for extra income from criminal activities to take care of their responsibilities.

3.1.4 Social Stratification

Nigerian society reveals inequalities that cut across religious, economic, political, and social spheres. Stratification divides people into different relative social categories: rich and poor; literate and illiterate; commoners and aristocrats; and peasantry and industrialists (Nayebi & Abdollahyan, 2006). The social strata difference influences quality of life, standard of living, and influence in society.

The country inherited the colonial system of capitalism that hinges on individualism, as reflected among the ruling class, who have failed to create common wealth for people (Imhonopi & Urim, 2013; Iorkongoso, 2014). The economic system has utilised a superstructure that always favours the few economically unproductive bourgeoisies. For example, the salary and allowances of an average Senator in Nigeria outweigh the American President. The five top wealthiest Nigerians are now worth $29.9billion (about £24billion) and collectively could end extreme national poverty, yet 5 million people face hunger (Oxfam International, 2017).

3.1.5 Technology in Nigeria

Nigerians have embraced technology irrespective of their socioeconomic conditions. Technology in Nigeria can be examined in five areas.

Internet penetration

The country is experiencing significant growth since introducing the Global System of Mobile Communication (GSM) (see Appendix E for more detail). The country is ranked 7th in the number of internet users with around 46 per cent penetration (Internet Live Stats, 2019). Penetration is 52 per cent for those aged 18-32 years and 21 per cent for those over 35. (Poushter, 2016). As of the third quarter of 2019, there were 190 million lines with 141 million active subscribers (Nigerian Communication Commission, [NCC], 2020) and 97 per cent of internet connections through mobile devices.

Despite the poverty level in Nigeria, the communal nature of society and strong family bonds make communication imperative. It prompts the use of mobile phones. Phone calls in the country are equivalent to visiting and physical socialisation (Smith, 2006). This has resulted in the widespread use of GSM and the internet for social media and communication.
Despite the high number of current internet subscriptions, some parts of Nigeria are struggling with insecurity. Residents in this area have no GSM or internet access, implying that internet access is still elusive for some Nigerians. Residents in this area are mostly internally displaced persons (IDPs) who are poor and could not afford these technologies.

Access to devices

Devices such as smartphones, laptops and computer systems have become more accessible. The prominence of cheap Chinese mobile phones means the use of smartphones is almost universal (Ahaiwe et al., 2015). Tecno\textsuperscript{36} has established an assembly plant in Nigeria, making affordable Android smartphones. Also, the cost of fast internet connection has reduced because of high competition among service providers. Nigerians are using internet both on mobile phones and on their multiple devices.

Local software markets

The Nigerian technology entrepreneurship ecosystem has evolved considerably. Technology companies in the country have attracted over $100million (about £89m) between 2012 and 2015 (Otori, 2018). There is increasing use of local technology solutions to service the agricultural sector (World Bank Data, 2019) and the financial sector. A suburb of Lagos (Yaba) has been named the ‘Silicon Valley of Nigeria.’

Global Brands

Foreign Brands that previously neglected Nigeria are increasing their presence, thereby enriching its technology space. Brands such as PayPal, eBay, Amazon, Uber, Facebook and Twitter have opened operations. Recently, Netflix extended its services to the country. The country has become a significant market in the global technology ecosystem, although currently, this is concentrated in the urban environment, especially Lagos.

Capacity Building

The final area of technology in Nigeria is the increasing avenue for capacity building and learning various aspects of technologies. Notably, some start-ups and entrepreneurs are focused on developing capacity in the country. For example, Andela has received over $80 million (Over £76million) in investment towards training software developers in Africa, among which

\textsuperscript{36} A Chinese telephone manufacturer.
Nigeria is a significant market (IFC, 2018). Other companies investing in Nigeria are Co-creation Hub, Aptech, and NIIT.

3.2 Characteristics of Cybercrime in Nigerian

The characteristics of cybercrime in Nigeria include sub-culture evolution, crime exportation, practitioners, and the prominence of banking services.

3.2.1. Sub-culture evolution

“Yahooism” has developed into a sub-culture that influences the lifestyle and overall conduct of the perpetrators. Members can be identified easily by their lifestyle. They usually brag, are extravagant, loud, and drive expensive cars (Aransiola et al., 2011). They possess unique ways of dressing and lavish money on material things, including night parties. Usually, they move in groups and use colloquial terms to communicate. Among cybercriminals, the term “Maga” or “Mugun” refers to victims, which literally means a “fool”.

“Yahooism” is an offshoot of AFF (see: Section 3.2.5) and achieved prominence in the early 1990s. It represents defrauding of victims using the Internet (Igba et al., 2018). Different perpetration methods include password sniffing, Logic Bombs, Spam, Phishing, Hacking, Malware, Drug, and Software Piracy.

Individuals involved in Yahooism are popularly known as “Yahoo Yahoo” or “Yahoo boys”. They are cyber deviants that specialise in different internet crimes (Aransiola et al., 2011). The name originated from email deployment to dupe victims (Adesina, 2017; Saulawa & Abubakar, 2014). Members of this sub-culture are usually young and often educated (May et al., 2010: Adeniran, 2008). Their studentship of Universities, Polytechnics and Colleges of education often provide an avenue for them to collaborate and improve their skills. Also, their education enables them to communicate with victims convincingly.

This subcultur is primarily ascribed to financially motivated criminals (see: Section 2.6.2). However, there are members with high technical skills driven by other purposes, such as altruism and revenge. Members are very skillful in deploying technology for criminal purposes (Igba et al., 2018). They crave for where to demonstrate and deploy their skills. Thus, membership has transcended the AFF perpetrators into experts in different cybercrimes.

3.2.2. Diverse Cybercrime Practitioners

There are numerous roles and responsibilities within cybercrime in Nigeria. Some skilled professionals provide services for cybercriminals. These are services patronised by
cybercriminals, including trading, language, and document forgery (Ablon, Libicki & Golay, 2014). Such individuals provide intricate or acquired skills needed for advanced attacks or crimes on the internet.

Another type of practitioner are the investors who are often regarded as ring leaders. For example, the case of Aroke demonstrated an investor in prison but still controlling criminal activities (Adepegba, 2019). Some of these investors are highly influential individuals in society. For instance, the EFCC arrested Maurice Ibekwe (a member of the National House of Representatives) for his cyber-related crime involvement (Kshetri, 2013). These investors are the head of the entire criminal enterprise and often remain above the law.

There are also individuals primarily concerned with financial aspects of cybercrime. Idowu (2016) noted that these are specialists who mostly conduct money laundering services for criminals. They often have a relationship with officials in the banking sector or play roles such as investors, organisers, team leaders or managers.

There are protectors that deal with the manipulation of the criminal justice system. The protectors are influential individuals who ensure that arrested perpetrators are freed and not prosecuted. Some cybercriminal syndicates use their influence to sabotage the criminal justice system (Chukwuemeka & Egbegi, 2019). They might be professionals such as police officers (see: Section 3.5.1), lawyers or financial consultants. In some cases, they exploit corruption in the system (see: Section 3.6.3) to ensure the failure of the process.

Furthermore, some professionals are involved in the marketing and distribution of goods and services. Some cybercrime markets involve the trade of services such as tools, stolen data, and escrow services (Leukfield, 2017). They use different platforms, both online and offline, in conducting this aspect of the crimes.

### 3.2.3 Crime Exportation

Nigerians are well-travelled people with up to 17 million citizens living outside of the country (Fidelis, 2017). It leads to an outflow of potential cybercriminals: e.g. Ayodele Salisu committed $500,000 cybercrime in the USA (IC3, 2012). This migration is evident in countries that border Nigeria. For example, cybercrime in the Benin republic originated from Nigerian immigrants in the mid-2000s (Affougnon, 2012). These countries continue to provide a fertile ground for Nigerian cybercriminals.
Migration has further made West Africa notorious for crimes including black money, crude oil, immigration, education, credit card theft, employment, inheritance, reshipment, religious/spiritual, internet dating, transfer of funds, property sale, transfer of funds and contract scams (Levi et al. 2015; Ogunlere, 2013; Oludayo, 2013). A crackdown on cyber fraudsters in Nigeria by the EFCC resulted in migration to other West African countries (Ribadu, 2007). This migration created the West African Syndication. Free movement in this region encourages the export of criminals. The syndication in West Africa exhibits “Nigerian connection” (Akuta et al., 2011; ANMT, 2010; Wada & Odulaja, 2012). Ghana, Nigeria, Sierra Leone, and Togo are high-risk countries for sending money from Australia (Levi et al., 2015). Cybercriminals from Nigeria are successfully using other African countries as a hub for growth.

3.2.4 The Prominence of Banking Services

Another vital factor is the proximity of cybercrime to the banking industry. The financial proceeds from these crimes must pass through the banking sector. Banking officials have played an active part in the financial system of cybercrime in Nigeria. An investigation of 180 participants in 10 banks of Idowu (2016) discovered that educated youths, bank staff, customers and non-bank customers were the primary perpetrators of this crime. Nigerian cybercriminals often use domiciliary accounts, Western Union, and MoneyGram37 to launder their financial gains (Okeshola & Adeta, 2013; Peel 2006, 2010). The financial sector is key to the evolution of Cybercrime in Nigeria.

Banking officials collaborate in criminogenic behaviour because of social and occupational pressures. Cybercriminals take maximum advantage of the banking environment where officials are unethical and fraudulent (Euronews, 2020; Hassan et al., 2012). In their quest for wealth, bankers often engage in activities that aid retrieving the proceeds of crime. In the banking industry, forgery and fraud, and money laundering have been recorded primarily in international money transfers.

3.2.5. Advance Fee Fraud (AFF)

The dimensions of AFF are extensive. Some of the means of conducting AFF include romance scam, inheritance scam, lottery scam, online dating, Business Email Counterfeit (BEC) and social networking sites. Common are email solicitations based on a general theme of multi-
million compensation payment to free up a personal fortune. Cybercriminals from Nigeria play an integral part in the fleecing of unwitting victims (Adesina, 2017). Many types of internet scam and fraud are assumed to originate in Nigeria. Chambers-Jones (2013) affirmed the country is a hub for internet financial crime with a weak framework for combatting this.

### 3.3 Emerging Trends

There is evidence of changing trends regarding technology, motivation, victims, and typology of crime. Cybercrime in the country thrives as different technical skills continue to advance (Wada & Odulaja, 2018). Technological progress and means of deployment are developing much more rapidly than regulatory controls.

#### 3.3.1 Increasing Local Targets

Cybercriminals are targeting domestic victims as part of the changing focus of their activities. The growth in digital ventures, the penetration of global brands, enhancement of the digital economy (Reed et al., 2014) has increased local victimisation. The fast rise of mobile communications, deployment of smart technology in government, the drive towards a cashless economy has extended the cybercrime risk within Nigeria (Wolf Pack, 2013). Moreover, cybercrime is increasing and becoming more sophisticated.

Although the overall narrative is that victims are foreign, Nigerian companies are becoming more concerned about their cybercrime risk level (Tahiru, 2013). Industries such as e-commerce, telecommunications and education are also cybercrime victims (Omodunbi et al., 2016). The number and type of victim are expanding at an alarming rate.

Nigerian banks and other organisations continue to conceal information. The National Deposit Insurance Corporation (NDIC)\(^{38}\) reported cyber-related fraud losses in the banking industry to be N10billion (about £33million) in 2007 and N6.2 billion (about £20.7million) in 2014 (Ahmed, 2008; Udo, 2015). However, a Kenyan IT group estimated that Nigeria lost $649 million (about £698million) to cybercrime in 2017 (Kshetri, 2019). The volume of actual loss to the economy is much larger than admitted.

Nigerian organisations are susceptible to different types of crime. The Nigerian banking sector is exposed as a cybercrime victim through scams, internet frauds and financial fraudsters

\(^{38}\) NDIC is an independent agency of the Federal Government of Nigeria to protect depositors and guarantee payment of insured funds in the event of failure of insured institutions. It is used to safeguard depositors fund.
(Ojeka & Ikpefan, 2011). Omodunbi et al. (2016) noted that cybercriminals conduct fraudulent activities against local banks to access user details or transfer funds illegally. There is evidence of previous attacks against the reputation and services of banks through DDoS (Raghavana & Parthiban, 2014). Even phishing has been targeted at local customers by collecting their bank details for fraudulent purposes.

Also, cybercrime in Nigeria targets digital services and products. Intellectual property (domestic and foreign) is pirated and distributed (Omodunbi et al., 2016). Digital piracy is threatening the growth of the Nigerian music industry, despite being one of the fastest-growing globally (Tade & Akinleye, 2012). The telecommunications sector has also been a victim of a different cybercrime penetration. For example, cybercriminals use “cheat codes” to illegally gain unlimited mobile telephone airtime. (Omodunbi et al., 2016). The digital economy in Nigeria is directly affected by this targeting.

There are an increasing number of attacks on government websites, especially their technological infrastructure. (Oni et al., 2019). The defacement of the Nigerian Electoral Commission website on the morning of the 2015 election is an example of this (Abimboye, 2015). Different government technological infrastructure has been adversely attacked and maliciously targeted. Oni et al. (2019) discovered that cybercrimes had impacted digital government implementation across Nigeria’s public sector.

On the contrary, the attacks on the government infrastructure might not originate from the country. There have been cases where other foreign attackers have claimed responsibility for these attacks. For example, Anonymous39 claimed responsibility for hacking the Nigerian Police Website (Guardian, 2020). Thus, attributing Nigerians to local crime is disputable.

Also, isolating government infrastructure from other entities that have been attacked is too subjective. Every entity on the internet is at risk. Businesses and individuals have also been attacked in a significant manner. The local targets are indiscriminate and demonstrate change in the perception of cybercriminals. They are now attaching significant value to victims within the country with the confidence of recording success with limited restriction (demonstrating the deployment of RCT in Section 2.5.4).

39 A distributed hacking team that are not known to have Nigerian members.
3.3.2 Changing Motivations

Cybercrime in Nigeria is moving towards different types of motivation (see Section 2.5). The changing profile of online crime, together with its targets, is an emerging trend. Olumide et al. (2015) noted that cyber-harassment against local targets was motivated by threats, sexual solicitation, and relationship breakdowns. Arimoro (2015) identified revenge as an important motivation in recorded cases of revenge pornography in Nigeria. On the other hand, motivations related to altruism have emerged through the absence of legitimate opportunities for skilled individuals.

Another crime type that demonstrates changing motivation is sexual crime, especially cyberstalking, cyberbullying, pornography, revenge pornography, and paedophilia (Arimoro, 2015; Ahmed, 2019). These crimes are prominent, with cyberspace becoming a platform for threatening victims (Mbanaso et al., 2015). The crimes sustain the patriarchal characteristics of Nigerian society, a further motivation that fuels cybercrime. Gender-based violence against women is prominent on internet-enabled platforms (UN Broadband Commission for Digital Development, 2015). Sexual rewards remain a primary motivation that deviates from the predominant financial aspects of cybercrime.

Nigerians are also experiencing internet-facilitated offline crime, where it is used to facilitate physical crimes. Victims of traditional physical crimes such as murder, kidnapping, manslaughter, rape, and robbery have been contacted or monitored using the internet (Ibekwe, 2017). The change in the mode of operation has been influenced by motivations that transcend money.

3.3.3 High Technology Cybercrime

Another emerging trend is the shift towards highly technical implementation. These technologies are used to develop malware and complex cyber-attacks. Nigeria and Romania are currently producing the highest number of Black-Hat Hackers⁴⁰, who violate computer security for personal gain or maliciousness. (Wilhelm, 2012). Moura (2013) states that the collaborative exploration of technology has increased the success rate of hacking in Nigeria. Cybercriminal behaviour in Nigeria is maturing into a sophisticated and advanced skill-based sector. Mbanaso et al. (2015) stated that cybercrime in Nigeria has developed coordinated and

---

⁴⁰ Black Hat hackers are criminals who break into computer networks with malicious intent.
organised hacking attacks. Ahmed (2019) noted the rampant nature of cyber-terrorism\(^{41}\) with the effective use of advanced technologies. Hawes (2015) reported that a Nigerian graduate was prosecuted for hacking to the tune of $340 million (about £363 million). Recently, the crimes in Nigerian cyberspace include infrastructure hacking, transatlantic website defacement and other sophisticated cyber-attacks (Wilhelm, 2012). Palo Alto Networks (2014) identified Nigerian actors as organising attacks against their customers in South Korea and Taiwan. Cuthbertson (2014) testified that Nigerian scammers had transcended general malware campaigns using sophisticated espionage and criminal groups.

The thriving mobile application market opens another frontier of cybercrime opportunity after years of slow growth (Agwu & Carter, 2014; GSM Alliance, 2014). Yakub et al. (2013) stated that close to 100 mobile money services exist in Nigeria, highlighting the growing appreciation of the mobile application market. Cybercrime on mobile telephone platforms and devices is becoming a significant part of these activities.

Despite the strength in AFF, cybercrime in the country is expanding with the emergence of more criminal groups. There are now many hacking groups with a Nigerian identity. One of the groups is the “Nigerian Cyber Army”, which remains anonymous but claims responsibility for the INEC website case (Ebuozor, 2015). The growing organisation among perpetrators is a trend that provides insight into the future.

Furthermore, Nigeria is only at the dawn of more sophisticated cyberattacks. The top-level Nigerian Internet Service Providers (ISPs)\(^{42}\) contains many sophisticated cybercrimes (Moura, 2013). Kshetri (2019) identified Nigeria as one of the African countries where sophisticated cyberattacks are generated. The rapid increase in skill sets, availability of cyberattack resources online, increased speed and affordability of the internet, and a change in motivation is germinating shift in the Cybercrime in the Nigeria market. Jack and Ene (2016) identified the use of virus, worms, and Trojans as part of current Nigerian crime. Various indigenous developers that can switch their skill set into criminal activities are emerging.

\(^{41}\) Cyberterrorism is the politically motivated use of computers and information technology to cause severe disruption or widespread fear in society.

\(^{42}\) ISPs are companies that provide internet access for users.
3.4 Organised Crime (OC) and Cybercrime in Nigeria

Another aspect of cybercrime in Nigeria is its organised nature. There are different dimensions to the OC implementation of cybercrime in the country. One of the dimensions is the organisation for financial reward through the sale of products from a scam. The proceeds are sent to cybercriminals in the country. For example, IC3 (2012) reported a Nevada case where a payment scam for online goods was conducted on Craigslist, and the suspect acted as a courier by shipping the goods to Nigeria. This OC implementation of cybercrime is transnational and creating a value chain for crime optimisation.

Another dimension is that Nigerian criminal organisations and networks are unique in both diversity and ubiquity. They are active in every country that possesses crime opportunities. They use a hierarchical and structured gang pattern in committing cybercrime (Williams, 2014). Nigerians constitute one of the most notorious cyber gangs in the United States. AFF by Nigerians has been globally claimed to involve expatriates with cells across the world. Ellis (2016) stated that Nigerian AFF cells are present in Japan, United States, Hong Kong, Canada, Europe, and other African countries. The AFF is perceived to have permeated into every level of government in Nigeria and other sub-Saharan African countries. It adapts to any environment to ensure its survival and connection to other cells.

OC remains a significant crime pattern that has grown from offline crime to cyberspace within Cybercrime in Nigerian. Ellis (2016) identified cybercrime as one of the critical areas in which the Nigerian OC is active. The arrival of the internet has provided an opportunity for various criminal organisations. The arrest of 320 Nigerians by Spanish Police in 2008 concerning an Internet fraud scheme demonstrated the cyber-based features of this characteristic (Williams, 2014). The successes recorded by law enforcement remain limited in terms of OC impact because identity theft and numerous internet fraud continue to expand.

However, previous theoretical and empirical discussion has failed to explain the organisational structure of cybercrime in Nigeria. Non-acknowledgement of this aspect remains a gap in criminological research. Cybercrime globally is a full business enterprise with viable vocations (Anderson et al., 2012; Merritt, 2009; Veenstra et al., 2015). Cybercrime in Nigeria has grown to now being a viable part of the national economy with fully-fledged characteristics.

Every cybercriminal has a certain level of independence in their actions. The perpetration is less structured and hierarchical. Evidence shows that cybercrime perpetration in Nigeria is uncoordinated. Anybody is free to participate without allegiance to any superior body, group
or individual. Losthaus (2018) discovered that cybercrime in Nigeria is witnessing Mafia infiltration in different roles such as a protector, guiding hand, investor, and service provider. The criminal conduct of Nigerians in South Africa, for example, has continued to suggest a loose OC organisation. They operate in small cells of five or six individuals, each working independently but networked (Losthaus, 2018; Snyman, 2001). The members of each group have unique skills. Each group controls a distinct operational geographical area.

### 3.5 Regulation of Cybercrime in Nigeria

However, Nigeria has adopted three core approaches: law enforcement, cyber surveillance, and strategy as obtainable in other countries.

#### 3.5.1 Law Enforcement of Cybercrime

Law enforcement in Nigeria within the context of this research involves the Nigeria Police Force (NPF), the Nigeria Security and Civil Defence Corps (NSCDC) and the Commission of the Economic and Financial Crime (EFCC).

The NPF has constitutional responsibility for crime prevention and detection, offender apprehension and prosecution, the protection of life and properties of citizens, together with enforcing and maintaining law and order (Inyang and Brown, 2011).

Cybercrime typology is becoming more advanced, resulting in increasing sense of insecurity in public. A rethink of the internal security system leads to creating the NSCDC (Invang & Brown, 2013; Otto & Ukpere, 2012), which is tasked with providing measures that combat any form of threat, disaster and attack against the country and its citizens. They usually offer intelligence and investigation of cybercriminals.

The EFCC was established and empowered to fight financial crime in 2004. It is responsible for investigating, arresting, and prosecuting any form of economic and financial crime (Ethelbert, 2016). Some of the EFCC jurisdiction crimes include advance fee fraud, counterfeiting, futures market fraud, money laundering, negotiable instruments fraudulent encashment, contract scam, computer fraud and credit card fraud.

The law enforcement agencies have developed particular ways of dealing with crime: Firstly, they use the profiling of young Nigerians for intelligence gathering, arrest and prosecution (Ekhoma, 2018). The approach hinges on the identified features associated with Yahoo subculture features (see: Section 3.2.1) regarding dress and behaviour. Any individual that
dresses or behaves in a certain way is automatically regarded as a potential suspect. Notably, the Special Anti-Robbery Squad (SARS, a special NPF task force) uses profiling in arresting cybercrime suspects.

This approach generated widespread outrage. The public accused these officers of extortion, extrajudicial killings, and indiscriminate arrest (Ekhoma, 2018; Odunsi, 2018; Punch, 2018). In recent times, officers have been punished for unprofessional activities. In December 2017, a social media campaign using the hashtag #ENDSARS was started to show dissatisfaction with the action of the Police (Oloyede & Elega, 2020). The technology industry complained about excessive police brutality, especially when they see professionals with laptops or other devices (Kazeem, 2019). In February 2020, SARS and its satellites were disbanded after the killing of Tiamiyu Kazeem in Sagamu (Erezi, 2020). Profiling has been ineffective in law enforcement in cybercrime.

Secondly, the NPF adopted international partnerships because it has struggled to combat cybercrime on its own. Traditionally, law enforcement is based on localised, routine-based practices by mapping crime within clear geographical areas. However, the trans-border nature of cybercrime transformed the nature of investigations (Bregant & Bregant, 2014). It supported the position adopted by Wall (2011) that the Police should acknowledge being a small part of the security networks in cyberspace. Wall further suggests establishing new relationships with other stakeholders in the network. Thus, there is a need for increased integration and synergy across countries to combat cybercrime.

There are partnerships with different enforcement agencies such as the FBI, MI5\(^\text{43}\), and other law enforcement agencies worldwide. The relationship is based on the effectiveness and advanced cybersecurity regulation of these countries. Law enforcement agencies such as FBI, GCHQ, and MI5 continually demonstrate increased success and curtailing of the activities of cybercriminals. For example, the arrest of 77 Nigerians who are members of a cybercrime ring demonstrate a huge way of curtailing criminal activities (Premium Times, 2019). Effective law enforcement adversely affects the growth of cybercrime in some countries.

The relationship relies on cases and investigation. The approach has resulted in significant success in many instances. For example, the EFCC partnered with the FBI to arrest 28

\(^{43}\) MI5 is also known as Military Intelligence, Section 5. It is domestic counter-intelligence and security agency in the United Kingdom.
cybercrime suspects in Nigeria (Nwafor, 2019). The partnership focuses on solving individual cases and not based on mutual intelligent sharing.

However, collaboration has only happened for “cases” where crimes have already been committed. There remain limited integration and synergy between international law enforcement partners for proactive and preventive cybercrimes. This reactive approach means that prevention is not the focus but investigation where victims have been exploited. This remains inefficient as the relationship is based on the discretion of the investigating law enforcement and not a standard integrative process.

The International Criminal Police Organization (INTERPOL) has focused on cybercrime to oversee the overall collaboration of Police among 194 member countries. Its approach is still extending the case-oriented paradigm. Its Cybercrime Collaborative Platform – Operations (CCP – Operation) and Cybercrime Knowledge Exchange (CKE) services remain restricted and ineffective. The overall operation is not based on risk analysis but gathering information from voluntary participants. Thus, it remains ineffective and does not contribute much to global cybersecurity.

This problem is not limited to cybercrime. Many fugitives and criminals have been aided and protected by member countries. Calcara (2020) note the organisation is vulnerable to abuse, with some states exploiting its tool for political oppression. Hence, the willingness to collaborate and trust among nations has been eroded. In its current state, it cannot be an effective vehicle for global cybercrime law enforcement.

Another critical point is the independent and inefficient investigation of trans-border crimes. In some cases, cybercriminals being investigated in other countries often escape to Nigeria to evade arrest. For example, the FBI has announced six wanted cybercriminals residing in Nigeria and were not arrested by EFCC (BBC, 2020). Despite international collaboration, law enforcement agents are regularly not informed because they are independent and do not involve input from Nigeria. This problem means that international partnerships are inefficient as investigations worldwide remain in silos rather than encouraging inter-agency collaboration.

The recorded success cannot hide the inefficiency of the case-by-case relative to the proactive intelligence sharing approach. Despite the increasing recognition of law enforcement collaboration against cybercrime, there are fundamental problems that limit this efficiency. Bregant and Bregant II (2014) acknowledged these factors: underreporting, incompatible laws
and jurisdictional difficulties. Solving these problems and developing a free flow of intelligence is vital for local and global cybersecurity strategies.

### 3.5.2 Cyber-surveillance in Nigeria

Nigeria is exploring cyber-surveillance. Criminal justice agencies continue to advocate measures to lower internet privacy using surveillance and user activity monitoring (Yar, 2013). Developed countries such as the UK, USA, France, Germany, and Canada have corresponding cyber-surveillance systems and laws.

There is increasing political will in deploying cyber-surveillance. Every successive government wants social media to be monitored and censored (Dada & Tafida, 2014; Jimada, 2019). From the government perspective, monitoring internet usage will ensure the discovery of cybercriminals who can disguise their activities and protect themselves from detection.

There is clear evidence suggesting surveillance of Nigerians. In July 2015, the publication of the records of Hacking Team (an Italian cyber-surveillance company) displayed the practise of cyber-surveillance by various tiers of the Nigerian government (Ogala, 2015). The Bayelsa state government (South-South Nigeria) was a Hacking Team client for surveillance services (Taiwo, 2015). The media further noted that the mobile phones distributed by the state government contained surveillance malware. The office of the Nigerian Security Adviser (NSA) and the Akwa Ibom State (South-South Nigeria) were accused of actively engaging the Hacking Team in the acquisition of surveillance technology (Sesan, 2015).

Despite the emphasis on the merit of this approach, there are critical points that impact its feasibility and suitability. Cyber surveillance and its implementation are likely to become highly problematic and abused in Nigeria. Firstly, the country lacks the technological infrastructure to conduct effective surveillance. There are weaknesses in Nigeria’s information systems and critical information infrastructure (Adelola, Dawson & Batmaz, 2015). The government relies on third party companies for surveillance (Iorliam, 2019). For example, the award of a $40 million (about £36 million) surveillance contract to an Israeli firm (Elbit Integrated Systems) for monitoring internet communication within Nigeria (Johnson, 2013). This move was in response to the role of social media in the January 2013 oils subsidy removal protest (#occupyNigeria) and the subsequent social activism (#BringBackOurGirls), which demanded the release of over 200 young girls kidnapped by the terrorist group Boko Haram.

Secondly, there is no law for either controlling or guiding government action in terms of surveillance. The country has no data protection law or legal framework to deter aggression
Sesan (2013) stated that the government could deploy these technologies to suppress freedom on the internet as there is no legal framework for restraint in its pervasive use. With cyberspace now subjecting government to global scrutiny, surveillance might be a means of silencing critics. Also, the recorded impunity and failure to respect the rule of law by successive Nigerian governments have further strengthened the public scepticism of the surveillance without infringing on their rights.

3.5.3 The Nigerian Cyber Security Strategy

Governments acknowledge the cyberspace risk profile of their respective countries in developing their cybersecurity plan. Different perspectives and philosophies have been adopted to respond to regulation and combating malicious use of the Internet by various governments (Flowers, Zeadally & Murray, 2013; Redford, 2011). The nature of cybercrime in a country often influences the type of strategy that is adopted. Hence, the variation in the philosophy of cybersecurity around the world.

The Canadian strategy focuses on critical infrastructure protection. The three core pillars are helping Canadians stay secure online, partnering to secure all vital cyber systems outside the Federal Government, and obtaining government systems (Department of Public Safety and Emergency Preparedness, 2018). The strategy suggests an ultimate focus on state sponsored military activities, cyber terrorism, cybercrime, and cyber espionage. Japan adopted the same approach as the government view large scale cyberattacks as presenting the highest risk.

On the other hand, the UK’s strategic position focuses on social and economic value through resilient, secure, and vibrant cyberspace. The Cyber Security Strategy of 2011 consists of objectives that concern robustness, economic resilience, and overall safety from different threats. The goals include shaping safe cyberspace that supports an open society; increased strength to cyberattacks and being better positioned to protect national interests in cyberspace; building essential knowledge capability and skills to cater for all its cybersecurity objectives, and tackling cybercrime to make the UK one of the most secure parts of the world to conduct business relating to cyberspace (Cabinet Office, 2011). It is an inclusive approach where the safety of every aspect of British cyberspace must be protected.

The strategy in Kenya acknowledges the infant position of their cybersecurity infrastructure despite increasing sophistication in crime (Quarshie & Martin-Odoom, 2012). It is more citizen-oriented with an emphasis on protecting national cyberspace interactions against threats that are unavoidable. The French government is more interested in National Information
Infrastructure protection while the Netherlands moved from an awareness focused strategy to capability through intensifying actions to combat crime (French Network and Information Security Agency, 2011; National Coordinator for Security and Counterterrorism, 2014). The reality of the risk and vulnerability, risks and the nature of experience cybercrime continue to influence the strategy design type.

Nigeria responded to its cybercrime risk and vulnerabilities by developing a National Cyber Security Policy and The National Cybersecurity Strategy (NCSS) in 2014. The country wants to be active in the Global Cyber Security Agenda, together with securing its cyberspace. The strategy focused on addressing the current and future cyber risks for the nation. The threats are taken seriously in Nigeria to allow citizens to optimise the benefits of information technology.

The purpose of the NCSS is to confront threats, support and uphold cyberspace openness. The strategy focuses on achieving a balance between security with fundamentals and respect for privacy. Nigerian policy focuses on the channels and sources used to perpetuate cybercrimes (Olayemi, 2014). It aligns with the national objectives, vision, principles, doctrines, and goals depicted in National Cybercrime Vision (2014). It identifies core risks to include Cybercrime, cyber terrorism, cyber espionage, and hacktivism (Osho & Onoja, 2015). These areas are paramount and form the focal points for the development of the policy and the strategy.

However, the strategy implementation is experiencing significant critical challenges. Firstly, funding for various aspects of the strategy has been limited. Funding has limited the creation of forensic laboratories, personnel training and the acquisition of equipment, infrastructure development and public awareness. The country is currently struggling economically and socially concerning income and finance (Blanchard & Husted, 2019), which has affected the strategy implementation.

The second critical point of the strategy is limited public and law enforcement awareness about NCSS. Despite the increasing adoption and usage of the internet, the level of cybersecurity knowledge or the NCSS remains extremely low within Nigerian society. There is low level of cybersecurity awareness, mass illiteracy, and the inability of internet users to take precautionary measures (Adelola et al., 2015). Hence, the increasing likelihood of victimisation and the vulnerability of Nigerian cyberspace.

Thirdly, there is an argument that sufficient awareness does exist, but that implementation has been weak. There is low enforcement of both the strategy and the laws (Adeniran, 2020; Boniface, Michael & Victor, 2015). Almost every member of society understands that the
malicious use of the Internet is a crime. However, adopting the best practices to reduce risk remains extremely limited.

Moreover, many government agencies are developing their cybersecurity systems outside the national strategy. The Central Bank of Nigeria is developing a risk-based cybersecurity framework for financial institutions (Kshetri, 2019). The current situation replicates the homeland security experience in the USA pre-9/11, where agencies worked independently without information sharing or collaboration with others.

Another issue is the administrative flaws that undermine the impact of the strategy. Olayemi (2014) noted that organisations involved in implementing the strategy lack of institutional memory where trained personnel are held in positions not relevant to their skill level. Bureaucracy and internal management often result in restructuring where tasks are assigned to staff without considering their skills and competency.

Within the cybercrime strategy, the Cybercrime Act 2015 was a significant component. The Act consists of provisions to prosecute any arrested cybercrime perpetrator. Oke (2015) stated the Act contains conditions and laws concerning the use and misuse of computer or electronic devices. Its impact is yet to be seen because some cases are still being prosecuted using the previous laws. Mohammed et al. (2019) noted that this Act is not significant, with no landmark prosecution record. There are no resources or dedicated support for law enforcement or prosecutorial process. Thus, there have been arrests but few prosecutions.

The overall strategy by Nigeria has further highlighted the weakness of various International conventions. Notably, the country has failed to ratify or Sign the Budapest treaty which remains voluntary and creates a cogent framework for local deployment. This treaty remains ineffective because it is not a global standard, the operational modalities are not defined, and involvement of different stakeholders were not clearly defined. For example, the role of research, private businesses and law enforcement is not adequately presented. In addition, the treaty was defined in 2007, and changes in the cybercrime and technology require an update to the entire provision.

---

44 The Convention is the first international treaty on crimes committed via the Internet and other computer networks. Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international cooperation.
3.6 Challenges of Combating Cybercrime in Nigeria

The fight against cybercrime in Nigeria is subject to some challenges. The challenges reflected the unique contextual characteristics of the country. This section discusses some of the problems.

3.6.1 Issues of Expertise

An area of critical challenge is the shortage of expertise and competence required to solve most cybercrime cases. Mohammed, Mohammed and Solanke (2019) stated that Nigeria has not been able to have a landmark cybercrime case prosecution using the 2015 Act because the criminal justice system lacks any effective prosecution expertise. The evident inefficiency of law enforcement cannot be associated with corruption (see: Section 3.6.3) alone but reflects the lack of competence and skills to combat cybercrime. The Nigerian Police Force lacks appropriate training to prevent, investigate, and detect electronic crimes (Eze et al., 2016; Olayemi, 2014).

A lack of trained personnel and technology experts is not limited to Nigerian law enforcement but a challenge to law enforcement worldwide. Harkin et al. (2018) identified insufficient skills and training, a slow increase in resourcing and expanding workload as law enforcement challenges in Australia. Research in South Korea, Taiwan, China, and Netherlands have confirmed limited training and skills as a significant problem (Chang, 2013; Lepanen, Kiravuo & Kajantie 2016 Leukfield et al., 2013; Nalla, Yong-Tae & Seung-Yeop, 2016).

Also, criminals are usually far more advanced and skilled than law enforcement agents. In addition to computer literacy, the Police Officer must have explicit knowledge of cybercriminal capability (Boniface et al., 2015). The advance in technology puts law enforcement at a comparative disadvantage with criminals. Cybercriminals can quickly develop their skills based on their social and professional networks (see: Section 2.5.3) while Officers will have to wait for training programmes or grants.

3.6.2 Measurement Challenges

The extensive impact of cybercrime is challenging to determine as no record exists as to the full facts of each incident. Criminologists, law enforcement and regulators struggle to understand different characteristics of these crimes because of minimal and reliable empirical data (Jang & Lim, 2013). There is excessive reliance on estimation and prediction.
The classification (see: Section 2.3) of cybercrime remains challenging to achieve because of different perspectives and operational considerations. Some of the relevant factors include diversity in definition and differences in the scope of the crimes (Leukfeldt et al., 2013b). Cybercrime measurement remains a significant challenge in both global and national understanding of its evolution. In Nigerian, crime data is not up-to-date and does not count cybercrime separately.

Within a regulation and law enforcement context in Nigeria, the failure to measure cybercrime conviction and perpetration remains challenging. While EFCC publishes the number of convictions, the Nigeria Prison Service does not categorise this type of crime (NBS, 2019). Convicted perpetrators are often categorised under crime such as economic sabotage, white-collar crime, forgery and altering, and currency offences. Oguntade et al. (2018) highlighted that lack of data limits insight into criminal activities in Nigeria. Without accurate information, the reduction effort must rely on speculation or general assumptions.

There are fundamental areas of impact for the measurement challenges. Firstly, the development of cybersecurity strategy, policy and capacity require reliable data (Babuta, 2017). It influences the development of management frameworks and mitigation of strategy in a proactive manner (Agrafiotis et al., 2016) and provides insight into sources, consequences, and the scale of the crime.

Another impact area is the limited understanding of the crime resulting in inefficient decision making (Armin et al., 2015). Hyman (2013) states the lack of a standard mechanism for accounting for losses and failure to report is a challenge for analysing the seriousness of these crimes. The importance of accurate measurement and information is demonstrated by countries such as the USA, Germany, India, and the UK that publish up-to-date annual crime statistics.

Also, its impact is in the area of criminal justice. The punishment of convicted cybercriminal remains lenient and not commensurate with the crime. For example, the recent conviction of Kolade Balogun, who was sentenced to pay N50,000 (about £100) or a three-month traffic control (EFCC, 2020). It is generally believed that convicted cybercriminals often enjoy lenient or no punishment. It is worthy to note that lenient punitive measure is not limited to only Nigeria. There was a similar case in the UK when victims express their dissatisfaction with the sentences based on the impact of the crime (Button et al., 2013). The failure to understand the primary and secondary effects will remain a significant challenge for cybercrime mitigation.
3.6.3 Corruption in the Nigerian Criminal Justice System

Corruption is widespread in Nigeria and has permeated through the social fabric, so it is a way of life for many individuals within both the public and private sector (Agbobai, 2013). Wealth is a significant barometer for power and influence. Nigeria is a country where the source of wealth is inconsequential and not scrutinised. Chukwuemeka and Egbei (2019) highlighted that corruption and high regard for money in the Nigerian value system contributed to cybercrime.

Nigeria is a highly corrupt country: Transparency International’s Corruption Perception Index (CPI)\(^{45}\) reports regularly place Nigeria among the highly corrupt nations in their global index. In 2017 Nigeria ranked the 148th most corrupt country out of 177 countries while ranking 144 out of 180 in 2018 (Transparency International, 2019). Corruption remains a significant reality in Nigerian society.

3.6.3.1 Corruption in the Judiciary

The Judiciary is required to uphold the rule of law in resolving any dispute and dealing with any transgresses (Salihu & Gholami, 2018). The failure to fulfil their role has increased criminality while reducing deterrence. There is a general belief that the Nigerian Judiciary is not adequately fighting cybercrime:

Firstly, many corrupt practices, including bribery, financial compensation, extortion, and file misplacement, are rampant within the system. The recent arrest and dismissal of some justices exposed illegal and corrupt practices prevalent within the judicial system (Gafar & Odukoya, 2014; Salihu & Gholami, 2018). Even senior lawyers are known to be part of the corruption. For example, a Senior Advocate of Nigeria (the equivalent of a QC in the UK) confirmed to having given a presiding Judge N225 000 (about £400) for the Funeral of his Father (Ezeamalu, 2016).

Secondly, accusation and prosecution of judicial administrative staffs have become a frequent occurrence. It is public knowledge that judicial officials are in collaboration with Judges in corrupt practices. Gafar and Odukoya (2014) note that the Judges in their corrupt practices use proxies such as court clerks, prosecutors, and registrars. The case of Mr Nwobike (a lawyer) showed that lawyers often bribe court clerks for their cases to be referred to compliant judges (Premium Times, 2018).

\(^{45}\) CPI is a metric used to rate corruption in countries by Transparency International.
Thirdly, it is a commonplace that justice has been perverted or stalled through corruption in the Judiciary. Despite the legal frameworks for criminal prosecutions, the law empowers the Judiciary to interfere in the operations of investigating institutions (such as the Police Force, the NSCDC, and the EFCC). Ugochukwu (2011) stated that courts exercised their power in many cases to restrict the arrest, investigation, and detention of some of the accused. The exercise of this power has resulted in many inconclusive cases or judgements that are not generally acceptable.

Also, many Nigerian Judges belong to an elite group with evidence of unexplained wealth. John-Salakov (2011) reported that Nigerian judges live luxurious and extravagant lives above their regular income. In a survey conducted by the NBS, the Judiciary was adjudged to be the second most corrupt institution in the country (Okakwu, 2017). The Nigerian Judiciary is currently weak and ineffective in the face of severe corruption. The punishment of judges by the Nigerian Judicial Council (NJC) is influenced by socio-political interference (Akinkugbe, 2020). Thus, corruption and favouritism affect the effectiveness of the Judiciary.

3.6.3.2 Corruption in the Nigerian Police Force

The Nigerian Police Force (NPF) is a core institution responsible for crime prevention, life and property protection, law and order enforcement, regulation, and peace and order maintenance. Clear evidence of corruption in Nigerian society is evidenced in the activities of its officers. Many individuals regard the Police as the initiator and practitioner of corruption (Enweremadu, 2019; Uhakeme, 2009).

The activities and motives of many members of the force showcase corruption resulting in the entire criminal justice system lacking integrity (Owen, 2014). The Independent Corrupt Practices and Other Related Offences Commission (ICPC, 2008) state the Nigerian Police has always had a culture of lack of accountability and transparency, brutality, incivility, and impunity that has now grown into full-scale corruption. Inyang and Abraham (2013) noted that bribery had become a police force culture, encouraging criminal activity. The widespread corruption is prominent and widely publicised in the media.

The Police also aid the perpetration of cybercrime. One example is the influence on prosecutions by superior officers. Social exchanges often result in superior officers ordering their juniors to drop an investigation and release suspects (Adongoi & Abraham, 2017). The influence makes junior officers less efficient and encourages future corrupt practices.
Corruption in the NPF often involves bribes and other tangible incentives being exchanged for favours and unethical practices. Members of the public compromise Police through gifts during the investigation of a specific case (Cook & Rice, 2006; Enweremadu, 2019). In some instances, Police demand specific fees for bail or to quash an investigation (Oluwaniyi, 2011). This social exchange between the Police and members of the public undermines the purpose of creating the force.

Although reports from other countries show some Police corruption is present everywhere, NPF corruption is unprecedented and of primary public concern. The process of prosecuting cybercrime and other criminal cases is undermined by NPF corrupt practices (Bakare & Aderinola, 2019). One core characteristic of Police involvement is collecting private gifts and bribes, leading to increasing lawlessness, armed robbery, political assassination, and a high level of social unrest across the country (Enweremadu, 2019). Political influence on the Police also increases, thereby making politicians limit investigations and slow down prosecutions (Saidu et al., 2019).

Another aspect is the failure to transform the culture of the NPF. Since its inception, policing in Nigeria has been a para-military system characterised by limited public accountability. Three decades of military rule inhibited policing development into a professional service (Owen, 2014). There is a lack of training and overall strategic intervention to improve the organisational culture. The public perceives the current system as being corrupt, unethical, and ineffective.
Chapter 4: Research Methodology

Methodology specifies the activities and process involved in research. The process starts from research initiation, continues throughout the research, and ends with the production of the findings. Criminological research usually implies the types of data to be collected, the methods adopted in the collection and the process involved in the analysis (Wincup, 2017). Empirical research is a rigorous and systematic process of investigating a phenomenon of developing explanatory theories and concepts. Thus, it is vital to define a specific methodology.

In social sciences, the adopted methodology influences the entire research paradigm. Numerous scholars have argued that no singular research methodology is the best for criminological research (Davis & Francis, 2018; Fellows & Liu, 2015; Gelsthorpe & Sharpe, 2005; Jennings & Reingle, 2019). Each available methodology possesses unique underlining philosophies and paradigms that influence their suitability to research. It is left to the researcher to select the paradigm that will provide the best approach to study the focused topic. Kuhn (1970) describes ‘paradigm’ as the foundational intellectual structure upon which research and development in a study field are situated. Thus, the need for a critical review of various philosophies before selecting those most suitable.

Conducting critical analysis and selecting a methodology is not sufficient. The overall process must be explained, especially when it is qualitative (Chiovitti & Piran, 2003). When describing the inquiry process, it is essential to demonstrate: (a) what the research explored; (b) the searched literature; (c) The developed research question; and (d) the number of involved participants (Cutcliffe, 2000; Lincoln & Guba, 1985; Stern, 1985).

Besides, explaining the research methodology remains critical towards showcasing the rigour involved in every stage. As discussed earlier, there is no single way of conducting research. Even when a qualitative approach is preferred, there are multiple ways of implementing the methods (Chiovitti & Piran, 2003; Whittemore et al., 2001). It ensures clear explanation of the role played by researchers and participants together with measures of protecting confidentiality. The diverse choices of implementing research necessitate the need for description demonstrating the quality of the process.

Another reason for the explanation is to enhance future research by ensuring effective duplication or repetition in other contexts. A clear and concise methodology chapter contributes to possible replication of the study (Fellows & Liu, 2015). The chapter explains how
philosophy influences the choices of research method, data collection, and data analysis. It concluded with the discussion of research ethics.

4.1 Research Philosophy

Research philosophy is vital to the way data about a phenomenon is gathered and analysed (Robson & McCartan, 2016). The selection of suitable philosophy is crucial in achieving a quality outcome. This research focuses on meanings that emphasise the collation and analysis of various subjective participant responses. There are differing opinions concerning cybercrime in Nigeria, and it is imperative to adopt a paradigm that will illuminate these perspectives in a scholarly discussion. Hence, the usefulness of interpretivism for the research.

Phenomenology was preferred to deal with the different aspects of the study. It describes reality through diverse information concerning the subject area (Saunders et al., 2016). It enabled the derivation of in-depth information and supported the investigation of the individual perspectives through the collation of assumptions and patterns of perception (Seth, 2015). It enabled the accurate subjective perception of participants by providing a layer of enhanced understanding of previously derived details in a theoretical analysis.

Phenomenology was preferred because it allowed the emergence of new knowledge and meanings from the different subjective information provided by participants. As this research area had limited focus, the methodology enabled a unique insight and understanding based on the experience of various participants (Robson & McCartan, 2016). Thus, it directly supported Interpretivism as the preferred model of conducting the research.

Reality should emerge from the perception of the participants. Hence, the subjective and variant understanding of truth should arise from the collected information (Willis, 2007). Phenomenology is a type of interpretivism that was preferred in this research. It derives knowledge through the interpretations given to the recollections of the experiences by participants (Saunders et al., 2016). It focuses less on recollection but more on the insights and meanings associated with the phenomena. In this research, the methodology derived its quality from the characteristics of interpretivism (Robson & McCartan, 2016). The underpinning assumptions stress that humans create meanings and thereby differed from physical phenomena.

Phenomenology was also suitable for the research because it supports exploring previous experiences of research participants (Aspers, 2009). Adopting the methodology ensured that
findings rely on understanding and the interpretation of occurrences. It enabled the extraction of meanings that reflect the truth concerning the research phenomenon. It allowed the research to base finding on the individuals involved in the study on the subjective perspectives given by the individuals involved. Its deployment enhanced the creation of new and richer understandings that rely on the interpretations of social contexts and worlds.

The inductive nature of phenomenology was critical in discovering new motivations and modes of operation concerning cybercrime in Nigeria. It enables the movement from generalised to specific ideas. (Robson & McCartan, 2016). This characteristic allowed participants to contribute information to determine the themes and concepts of the research. It supported fresh insights newer than previously obtained in the subject area. Its adaptation to this research resulted in the derivation of new knowledge in areas such as cybercrime motivation, impact of technology penetration, modes of operation, emerging trends, and Government intervention.

The choice of phenomenology was strengthened by the lack of reliable data in the research area. Statistical data about cybercrime in Nigeria is limited, thereby making the exploratory characteristics of the qualitative method more suitable. Prior data to give in-depth inferential meaning were not available, and it was necessary to rely on the interpretive explanation of the different participants.

4.2 Research Design

This research was designed in two stages: the literature review, already covered in Chapter 2 (concepts and background) and Chapter 3 (a deeper understanding of cybercrime in the context of Nigeria.) These chapters have explored cybercrime by providing detailed information on the background of the empirical research.

The second stage is the primary research. It focuses on cybercrime in Nigeria as a case study of the more general investigation. The methods adopted for this research included documentary analysis, focus groups and interviews.

The stakeholders involved were current actors of cybercrime in Nigeria (Section 4.4). The collected data in this research is unique and new in the understanding cybercrime within the Nigerian context. The collected data from convicted criminals (Section 4.6.1) provided a new insight and perception never presented before: data from other stakeholders give new perspectives about different aspects of cybercrime.
4.3 Qualitative Method

The qualitative method was selected for this research based on three factors. Firstly, the study explores an under-researched area where new insight is essential for advanced knowledge. There was no substantive background information that has captured the scope and depth of the relevant information. The research focuses on learning about one of the most potent cybercrime countries in the world. Qualitative research supports the collection of information that provides new definitions in a research area (Fyfe-Green, 2018). Thus, the preferred method should support rich and contextual meaning where every possible strand of knowledge can be gleaned without any restriction.

Secondly, there was a need to collate in-depth contextual information concerning the subject area. It supported the involvement of stakeholders through the collection of their subjective ideas. Combining the experiences and corresponding meanings requires a method to collect detailed information from different perspectives (Saunders et al., 2020). The qualitative method provided a means for which experiences can be shared using focus groups while individual experiences can be shared using interviews. The diverse subjective perspective helped determine the changes and potential emerging trends of cybercrime in Nigeria.

This research sought to unravel opinions from hard-to-reach areas such as the Judiciary, convicted criminals and various paramilitary organisations. Collected information need not be restricted by allowing free expression and information provision. Robson and McCartan (2016) identified rich contextual information retrieval as a significant strength of the qualitative method. Hence, the adoption of the qualitative approach provided sufficient information that substantiated the findings.

Thirdly, qualitative method aligned with the adopted phenomenology approach. Using this method enabled this research to collect and analyse data that demonstrate the preferred research philosophy. The method became suitable for effective reflection of the operational implementation of phenomenology.

4.4 Access

In this research, access was critical as a fundamental component of data collection. Because of the need to collect hard-to-reach data from convicted criminals, members of the National Assembly and the Judiciary, it became essential to achieve access to develop trust and
confidence. In the explanation by the European Commission (2018), when research focuses on organisations or stakeholder groups, access is about achieving the necessary approvals and then gaining the trust of participants. Gatekeepers were used for the different stakeholder groups because they belong to organisations that play sensitive cybercrime roles in Nigeria. The gatekeepers were senior officials that could grant permission to subordinates to take part in interviews.

The core challenge in access was the bureaucracy involved in getting approval. Researching a Nigerian organisation is often challenged by the consent of the management (Chukwu et al., 2016). The applications were applied early, while the gatekeepers were recruited through academic and professional recommendations. Initially, five gatekeepers were recruited for the stakeholder groups comprising the EFCC, Nigerian Police Force, Judiciary, NSCDC, and legislature. The first gatekeeper was at EFCC, who recommended others in the remaining stakeholder groups.

The gatekeepers facilitated the application process and ensured the timely recruitment of participants. The approvals were verbal for these five stakeholder groups as the gatekeepers were involved in the data collection. They facilitated the use of their respective organisations’ premises for recruitment and data collection.

However, the Nigerian Prison Service (now Nigerian Correctional Service) involved a formal request letter to be approved by the Osun State Commandant. The gatekeeper facilitated a personal audience with the officer, where the purpose of the research was discussed. This meeting enhanced the approval process as the constituted authority became familiar and convinced with the investigation. The approval was given, and access was granted to interview the convicted criminals at the Ilesa Prisons.

From the onset, the criminology researcher group and the Ministry of Justice were not part of the stakeholder group. However, advice and suggestions from other gatekeepers made their involvement significant. Contacts of gatekeepers for the two were provided by one of the participants. Personal communication and eventually recruitment were achieved. For the Ministry of Justice, the gatekeeper was the only participant, thereby making access easier. At the Federal University of Technology in Minna, the gatekeeper enhanced access to researchers in the Cyber Security Science (CSS) department. Overall, the stakeholder groups identified for this research are outlined in Figure 4.
The agreement of gatekeepers in each stakeholder group enhanced the credibility and acceptance of the research by subordinates. Gatekeepers also provided anonymity and privacy by protecting the interest of research participants (Crowhurst & Kennedy-macfoy, 2013). Table 2 details the gatekeeper and their role for each stakeholder group.

**Figure 4: Crime Stakeholders in Nigeria**

The agreement of gatekeepers in each stakeholder group enhanced the credibility and acceptance of the research by subordinates. Gatekeepers also provided anonymity and privacy by protecting the interest of research participants (Crowhurst & Kennedy-macfoy, 2013). Table 2 details the gatekeeper and their role for each stakeholder group.
Table 2: Gatekeepers Details

<table>
<thead>
<tr>
<th>Participant Group</th>
<th>Number of Gatekeepers</th>
<th>Role Played</th>
</tr>
</thead>
<tbody>
<tr>
<td>EFCC</td>
<td>1</td>
<td>Provided the permission and link to the other participant and the Ministry of Justice Participant.</td>
</tr>
<tr>
<td>Nigeria Police</td>
<td>1</td>
<td>Gatekeeper did not participate in this research. However, provided the link to the most senior Police Officer that participated.</td>
</tr>
<tr>
<td>Nigeria Legislators</td>
<td>1</td>
<td>Provided the entry point into contacting potential participants. Ensured that communication and recruitment were achieved.</td>
</tr>
<tr>
<td>Researcher</td>
<td>1</td>
<td>Gatekeeper did not participate in this research. Provided the link to the top academics that enabled access to other participants.</td>
</tr>
<tr>
<td>NSCDC</td>
<td>1</td>
<td>It provided access by gaining verbal approval from the sector command to research the state headquarters.</td>
</tr>
<tr>
<td>Nigeria Prison Service</td>
<td>1</td>
<td>Provided the overall guidance on the process of seeking approval to interview convicted criminals. It assisted in securing the approval letter.</td>
</tr>
<tr>
<td>Judiciary</td>
<td>1</td>
<td>Provided access to Judges that enabled the conduct of the research. Assisted in getting approval for conducting the research.</td>
</tr>
</tbody>
</table>

Follow-up communication with the gatekeepers was carried out after ethical approval from the department. After the initial contact of the samples, permission was sought (verbally or in writing) from the gatekeepers. Invitation letters were sent to each potential participant for the interview (Appendix B) and Focus Group (Appendix C). Both email and telephone were used to communicate with the initial samples.

4.5 Sampling

Sampling was adopted in this research because of the members of each stakeholder group. The research population of the study was vast because each stakeholder group, apart from the research group, was extensive. Sampling was imperative to allow participants to reflect the opinion and position of the broader research population (Kuada, 2012). The stakeholders had direct dealings and relationship with cybercrime in Nigeria. (Table 3).
### Table 3: Participant Breakdown

<table>
<thead>
<tr>
<th>Participant Type</th>
<th>Number</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSCDC Officers</td>
<td>7</td>
<td>These are officers that deal with different aspects of crime investigation in the command. Areas such as fraud, intelligence, research, and the legal department providing the participants</td>
</tr>
<tr>
<td>Nigerian Police Force</td>
<td>5</td>
<td>The participants span the different areas of Police work. Two participants were low ranked officers (Investigating Police Officers), one was the head of a state cybercrime investigating unit, one was in a State Intelligence Unit, one is the Head of communication team of the Federal Criminal Investigation Unit.</td>
</tr>
<tr>
<td>EFCC</td>
<td>2</td>
<td>One is a deputy director of the legal department focused on cybercrime. One is the head of the Cybercrime Investigation Unit.</td>
</tr>
<tr>
<td>Nigerian Judiciary</td>
<td>2</td>
<td>Two are Judges that have dealt with criminal prosecution of cybercrime</td>
</tr>
<tr>
<td>Ministry of Justice</td>
<td>1</td>
<td>Director in charge of cybercrime</td>
</tr>
<tr>
<td>National Assembly</td>
<td>2</td>
<td>Two Legislators at the Federal House of Representative</td>
</tr>
<tr>
<td>Convicted Criminals</td>
<td>6</td>
<td>Convicted cybercrime criminals that are serving jail terms</td>
</tr>
<tr>
<td>Criminology Researchers</td>
<td>3</td>
<td>They are lecturers at the only University that is rendering a Cybercrime Degree Course in Nigeria.</td>
</tr>
</tbody>
</table>

Snowball sampling was adopted as the primary recruitment strategy. It enabled the reliance of the study on finding participants through the suggestions of other participants. (Saunders et al., 2016; Robson & McCartan, 2016). This approach was effective, considering that the stakeholder category of this research belongs to a concealed population and sensitive agencies. Two reasons were responsible for this sampling approach. Firstly, snowball sampling was adopted because it provided practical advantages for this research, which is descriptive, explorative, and qualitative (Handcock & Gile, 2011). Because this research is exploratory, this sampling approach provided an efficient means of accessing and recruiting informed participants. Its suitability was evident in its support for individualised, in-depth, and quality results.
Secondly, it supported the collation of information within a network of highly informed and qualified participants. It allowed participant selection and recruitment to reflect a link-tracing model that used the advantage of the networks of subjects (Emerson, 2015). Snowballing was advantageous by enabling the use of the networks of subjects to develop quality participant distribution.

The gatekeepers (Table 2) were selected based on two factors. The first was their experience evident in their organisational positions. High ranking officials were preferred to enhance the participant recruitment approval process and provide a valid link to credible lower-level officials. The second was the organisation where the officials work. These factors were critical in ensuring that the initially selected participants could facilitate snowballing sampling.

There were eight initial samples, representing one for each stakeholder group (Table 2). The gatekeepers were the starting point at each of the stakeholder agencies except the Judiciary. They were consulted and asked to suggest possible participants within their organisation or stakeholder group. The step-by-step consultation with potential participants continued until enough participants had been reached. In total, this research involved 28 participants after contacting 83 potential participants (Table 3).

4.6 Data Collection

The adoption of qualitative method influenced the technique for collecting data. The available techniques for data collection included interviews, a focus group, observational methods and document analysis. In this research, focus groups and interviews were selected for the empirical data. Both were chosen collectively after critical analysis of their strengths and suitability to the research method.

Firstly, they allowed the collection of in-depth information and underlining reasons for the opinions held by participants. The adoption was based on the research problem and the research questions (Cresswell & Cresswell, 2017). Since this research was delving into a niche context of cybercrime, it was essential to access the subjective information that provided new insights. Both techniques enabled the retrieval of in-depth information concerning the experience of participants (Button et al., 2015; Gibbs, 2018). Participants were able to present their opinion without any restriction. Thus, the research could provide an in-depth understanding of cybercrime motivation, changes in the crime, mode of operation, societal factors, and regulation.
Also, both techniques allowed the researchers to explore new areas. They let the collection of information that provided fresh insight concerning the way that cybercrime in Nigeria operates. They integrated with the phenomenology and qualitative method in enriching the contextual knowledge that was the research focus.

A focus group was selected because of its support for deriving in-depth meanings and new ideas based on the discussion and exchange of ideas by participants. Nyumba et al. (2018) explained that it enabled a means for which discussions between participants contribute to the emergence of new ideas and information hitherto neglected. Participants and the researcher had close contacts, which enhanced the exploration of emergent issues (see: Chapter 5). The focus group involved three participants, and considering that they were from paramilitary organisations, the focus group enabled them to be affected by sharing their experiences through interaction with colleagues. Initially, three focus groups were scheduled for participants in the NSCDC, Police and the EFCC staff. However, the geographical distance and other logistical challenges reduced the deployment to one session for NSCDC participants (see: Section 4.6.2).

The two methods, including interviews and focus group, complemented one another in answering the multi-dimensional questions presented in this research. However, priority was given to interviews, as these turned out to be highly flexible, able to be conducted by telephone, face-to-face, audio calls or video calls, which enhanced the data collection process. Carr and Worth (2001) and Farooq (2015) affirmed the efficiency of the telephone interview. Considering the size of Nigeria and the need to engage critical stakeholders, the telephone interview enabled many geographical areas to be covered.

Secondly, the support for incremental changes of questions through the data collection process was a significant factor. Interview questions could be shaped to reflect the unique experiences of different participants (Cresswell & Cresswell, 2017). It enabled incremental development of research findings through the modification of questions (Fyfe-Green, 2018). There were different stakeholder groups (Section 4.4) in this research with different cybercrime industry experiences.

4.6.1 Data Collection Process

Semi-structured interviewing was adopted to reduce the risk of deviation from the research scope. In agreement with Saunders et al.’s (2020) position, as demonstrated by Marshall and Rossman (2014), it ensured that interviews, irrespective of the type, stayed within scope.
Outlining the questions before the research enhanced the concise nature of findings and reduced irrelevant information.

The findings from the theoretical analysis were used for defining questions for the semi-structured interview. The questions (Appendix E) were designed to exploit the knowledge gaps found in the literature review. They were fine-tuned and structured to reflect the reality of each participant type. The emphases in the interviews varied, reflecting the strength and context of each participant: e.g. questions for convicted criminals focused more on the actual perpetration and the mode of operation, whereas those to the Police Force focused on law enforcement. These differences enabled the collation of contextual and interpretation-based information from a different perspective.

In this research, some participants opted out of recordings, giving them more confidence to discuss and explain their experience. In the case of convicted criminals, the Nigerian Prison Service policy (now Nigerian Correctional Service) was that no interviewed inmate could be recorded. Interviewing and jotting down findings were therefore used.

The data were collected between February 21 and March 29, 2017. Participants worked in five cities (Abuja, Minna, Lagos, Osogbo and Ilesha). Figure 3 shows the stages in the data collection, with the concluding stage being the focus group. Three of the participants, from the NPF, EFCC and MOJ were members of the Federal Government Cybercrime Advisory Committee and provided top-level policy formulation and implementation advice. All three were involved in face-to-face interviews.

![Figure 5: Data Collection Stages](image)

The first stage was the collection of data from the NSCDC participants at Osun state headquarters in Osogbo. Data was first collected from the focus group with three of the participants in NSCDC. After completing the focus group, the findings were reviewed before proceeding with the five interviews of the participants from the same stakeholder groups.
The second stage of the data collection involved officials of the EFCC and the Ministry of Justice. As the participants from these two groups are located in Abuja, it was feasible to conduct the data collection. The two participants from the EFCC were interviewed at the national headquarters because they were top-level managers within the legal and the Cybercrime Investigation Department. For the MOJ, it was a face-to-face interview at the office of the participant.

The third stage of data collection involved cybercrime researchers, who were nominated to have current and objective information about cybercrime trends. They are lecturers at the only University (Federal University of Technology, Minna) delivering cybercrime to Nigeria. Face-to-face interviews were conducted in their respective offices.

The fourth stage is the legislature and the NPF. Three Police officers were interviewed face-to-face and two on the telephone. Three of the five Police Officers are directly involved in the street level investigation of cybercriminals; one is a technological investigator of cybercrime, while the last is the Director of Communication in a Federal division. The two legislators interviewed are members of the National House of Representatives. The face-to-face interviews took place at their respective offices in the National Assembly building in Abuja.

The last stage is the interview of Judiciary members and convicted criminals. Two interviews were conducted for the Judges over the telephone, as Judges preferred this approach based on the increasing focus and investigation into the Judiciary during the data collection period (Azu, 2017; BBC, 2016). The interviews were collected without recording but jotting of the key findings from the responses to the questions. Finally, attention moved to convicted criminals, a hard-to-reach and challenging but core stakeholder group. Chakraborti and Garland (2017) noted the difficulties of collecting data from hard-to-access communities.

The data collection was carried out individually and face-to-face for the six convicts that agreed to participate. The convicted criminals were interviewed at the Nigerian Prison Service, Ilesa. Ilesa is one of the most critical prisons in the country, hosting a substantial collection of convicted cybercrime offenders. The electronic recording was not allowed for this group, but notes and jottings were used. A dedicated room in the prison was used for the interviews.

In summary, twenty-eight (28) participants were involved in the data collection. Most were face-to-face and were recorded and transcribed. Four interviews were done via telephone. Exceptions to the recording included a Police Officer, convicted prisoners, the two Judges and NSCDC Officers.
4.6.2 Research Constraints

Several different types of constraints were experienced during the data collection, although they are not unique to Nigeria. The security architecture (see: Section 3.2.11) means that senior and junior staff work in different places. Most senior managers in the agencies researched work in HQ in Abuja while junior staff work elsewhere. Although previous research in Africa has focused on junior officers (Beek, 2012; Faull, 2018; Sowatey & Tankebe, 2018), it was felt that, for this research, it was vital to interview senior officers. This enabled the researcher to achieve the methodological insights derived from Robert Reiner’s (1991) study of chief constables in England and Wales.

4.6.2.1 Participant Reluctance

Previous researchers of Police and other paramilitary organisations reported low response rate and poor cooperation as a core constraint (Alemika, 2009; Nix et al., 2019; Perkins, 2018; Skogan, 2015). This could be associated with some factors. Firstly, many potential participants refused due to the fear of loyalty to their hierarchical organisational structure. Sollund (2005) stated that hierarchical structure often makes Police Officers (and other law enforcement personnel) weary of research involvement. Officers do not want to offend their superiors or colleagues by stating unwanted truths. Their participation might be seen as betraying police culture or as revealing sensitive information.

Also, trust between the Police and outsiders (researchers) often affects openness and willingness to participate. Skogan (2015) noted that police (and other law enforcement agencies) are close-knit and distrustful of outsiders, resulting in their reluctance to participate in empirical research. This belief hinged on the general assertion that police research has always been negatively accepted (Cordner & White, 2010) because it often showcases flaws that the senior hierarchy does not want to be in the public arena (Aas, 2019). Thus, recruitment of participants in such research is often challenging and sometimes impossible.

The reluctance in participation could result from the wide gap between research and practice within the criminal justice system. Police worldwide accept research findings differently. While the UK and the US have gone through five Police research stages (Reiner, 2010), other countries still find limited use of academic research. Numerous African countries suffer from low research culture as the various crime control institutions are not receptive to research outsider study (Alemika, 2009; Faull, 2018; Thurman, 2017). The absence of research culture often deters participation. In some cases, the necessity of obtaining formal approval from police
supervisors often compounds the reluctance. Thus, the level of refusal and reluctance was significant.

An example in this research was from the Judiciary, where many contacted Judges were unwilling to participate because of the perceived risk. The reluctance of the potential participants influenced the entire data collection process (Archibald & Munce, 2015). It was also apparent in the focus group that some potential participants believed that others could identify them and their opinions during the discussion.

4.6.2.2 Security

Physical safety is a fundamental challenge in the conduct of qualitative research. Brougham and Uttley (2017) acknowledged that researchers are faced with many dangers, such as injury, emotional distress, violence, illness, and death during data collection. An example was the death of a Caribbean criminologist (Ken Pryce), whose body was washed up on a beach after mysteriously disappearing while studying criminality in Jamaica (Bloor et al., 2007). It is challenging to ensure that researchers are entirely free from every security risk. However, reasonable steps must be taken to avoid these risks and enhance the physical safety of researchers (Williamson & Burns, 2014). Thus, the need for attention to such dangers while collecting data for this research.

The high level of insecurity and risks associated with travelling between the cities was another factor. Nigeria struggles with internal security, with an increased number of armed robbery and kidnapping cases on main roads (Badiora, 2015; Nnam, 2020). In the same year of collecting data, ten geology researchers were kidnapped in the northern part of the country (Africanews, 2017). Eight lecturers were also kidnapped at Esa Oke, a few kilometres from Ilesa (the venue for collecting convicted criminal data) (Vanguard, 2018). Because data were collected in five cities across both the northern and southern part of Nigeria, the researcher needed to travel at odd hours, itself a safety risk. During one night journey from Abuja to Ilesa, the researcher encountered armed robbers, resulting in emotional distress.

4.6.2.3 Infrastructure

Research risks are associated with the environment, topic, and participants under study. Conducting fieldwork in developing countries provides unique challenges compared to developed countries (Amerson & Strang, 2015). Many of these countries have weak infrastructure to promote the safety of researchers (Igoumenidis & Zyga, 2011). The infrastructure challenge directly increases the danger and risks for researchers.
Accessing and collecting data from the various participants in this research attracted significant risk on both personal and physical levels. Firstly, the roads’ dire state (Enwerem & Ali, 2016) increased the risk of an accident and other physical dangers. The researcher travelled over 6000 miles on roads within the period of data collection. The travelling attracted risks that endangered both the physical and emotional wellbeing of the researcher.

4.6.2.4 Diseases and Sickness

On the other hand, Amerson and Strang (2015) stated that researchers in developing countries have high risk of disease and infection. Sicknesses such as Malaria, Cholera and Typhoid are part of the health risks that characterise sub-Saharan Africa. Travelling to these countries for research can make researchers experience deadly diseases such as dysentery (Bulled, Singer & Dillingham, 2014). Thus, care must be taken towards maintaining optimum wellbeing during and after data collection.

These risks directly reflected on the entire research process as the safety of the researcher remained paramount (Brougham & Uttley, 2017). The researcher had to lodge in different accommodation and was exposed to various health risks during the data collection. The experience resulted in a bout of malaria two weeks into the data collection. He also took two weeks to recover from stress and general weakness after returning to the UK.

4.6.2.5 Interviewing Convicted Criminals

Conducting qualitative prison research remains a controversial core area of criminology worldwide. There are numerous challenges, but three were relevant to the experience in this study. Researchers have continually emphasised access as one of the core challenges. An experienced qualitative prisons researcher, Liebling (2014) described many barriers to entry while researching prisons. They are of all types and levels and can be ethical, cultural, formal or informal. These barriers might create seemingly insurmountable obstacles to standardised research conduct. Beyens et al. (2015) stated that the procedure of gaining access might be time-consuming and often require convincing numerous gatekeepers about the legitimacy of the research and the soundness of the study. It also required constant negotiation.

Despite the general belief about access, it depends on the country and prison research support. For example, Beyens et al. (2015) noted that Belgium provided smooth access to prisoners without any barrier. However, sub-Saharan African countries have high level of barriers to access for outsider research. Mhlanga-Gunda et al. (2020) noted that societal views on incarceration that imprisoned people are devalued citizens, and as punitive rather than
restorative process compound the barriers to access. The ethical and cultural barriers are enhanced by lack of focused oversight and international standards. Hence, it is difficult to achieve effective access for prison research in countries like Benin, Ghana, Niger Republic, and Nigeria.

Also, obtaining the required approval and permission was another major challenge. Apa et al. (2012) acknowledged that gaining approval from the Institutional Review Board and the Department of Corrections was a significant challenge while researching two New York State maximum-security prisons. Fox et al. (2011) acknowledged this difficulty to the time it takes to review protocols that involve vulnerable populations such as prisoners. Within this research, the challenge came from getting approval among core groups, including administrative staff, security staff, and inmates.

Access and approval do not necessarily imply successful prison research. The data collection process relies on the facilities available at the prison. Apa et al. (2012) noted that prison facilities vary in design and influence how the process is conducted. Lack of sufficient conducive facility for ethically and standardised research is a significant constraint. Considering the congestion recorded in most prisons worldwide (Carranza, 2014; Human Rights Watch, 2020; McCarthy, 2018), having a suitable facility for empirical research is a universal challenge. This constraint was replicated in this research and made it impossible to conduct a group data collection session (focus group) for the inmates.

4.7 Data Analysis

A thematic analysis was adopted for analysing the data. This approach enabled the coding and presentation of findings in distinct themes that satisfy the research objectives (Braun & Clarke, 2013). The method supported the discussion of the findings that represent different knowledge themes.

The thematic analysis enabled the identification of numerous cross-references between the collected data concerning the evolving themes. It allowed the analysis to rely on the research for extracting information that relates to the variables and other situational evidence in the same study (Alhojailan, 2012). It also supported the description and identification of explicit and implicit ideas by linking themes to the raw data (Namey et al., 2008).

Adopting the thematic approach made the discussion and findings easy to understand. The derived themes from the collected data provided points that enhanced the understanding of the
research subjects (Vaismoradi & Snelgrove, 2019). The collected data was transcribed using the tape recording of both the recorded interviews and the focus group.

The main themes were derived from the research questions. This approach was effective because it addressed each focused research area. Extracts from the findings were used to present different opinions and explanations to illustrate the research questions.

Sub-themes were derived because they answered different aspects of the research questions. Quotations were placed under each of these themes to illustrate each knowledge area. After deriving the codes represented by the sub-themes, the analysis was conducted using quotes to establish different strands of knowledge. Both inferential and interpretive analysis was used to present the different information and details derived from the findings.

4.8 Ethical Considerations

Achieving reliability and validity in the research was imperative in demonstrating the authenticity and quality of the findings. There are five considerations, which demonstrate core areas, in which action was required to uphold the integrity that reflected the expected standard.

The first consideration was the achievement of necessary approval for primary data collection, analysis and archiving. An ethical bundle consisting of 9 documents was submitted to the Departmental Ethics Committee at the Institute of Criminal Justice Studies at the University of Portsmouth. The documents contained the research plan and the process for conducting the primary research. The approval of the research ethics initiated the empirical research undertaken. This process started in April 2016, and the approval was secured in November 2016 (Appendix D). Various amendments were made to ensure that it conformed to the standardised research practice. These amendments included access, data collection process and analysis.

The second aspect of the research was the protection of the participants from any physical or psychological harm (Bryman, 2016). Because the study did not involve anybody below eighteen years (minor) or vulnerable participants, there was no need for parental or guardian approval. The involvement of individual participants did not interfere with occupational or legal responsibilities. The information sought was general, and personal meanings were associated with their experience and not with any incriminating details of their job.

Another step was through voluntary participation. Participants were also told they could retrieve their information before the publication of the thesis. This decision further enhanced
the confidence of the participants in the process. The three steps were achieved through informed consent (Appendix A). The participants signed the form to prove their understanding of the research and its purpose and acknowledged they participated willingly.

The third aspect of the ethical consideration was the anonymity of participants. Maintaining the anonymity of participants was essential in achieving research reliability (Silverman, 2011). There was no collection of personal information (e.g. name, address, telephone number, organisation, gender or email). This also enhanced their participation.

Also, communication was conducted in a way that anonymity was upheld. Every communication with the participants was over personal channels (Appendix B and C for the invitation letter). The personal communication insulated participants from any official recognition or identification that might threaten their participation. Work-based electronic mail or telephone numbers were ignored for the research. It was essential to eliminate any consequence that could result from management’s access to correspondence or collected information. In upholding anonymity, each participant was coded in the data analysis. It increased the discreet and anonymity of ethical consideration.

The fourth ethical aspect was confidentiality. Participant details or given information would not be disseminated outside the scope of the study without permission (Saunders et al., 2016). All data involved in this research was strictly used for the stated purpose. Identifiable information that could affect the participant is not presented in the findings. Any information or data not approved by the participants has not been released.

Confidentiality was achieved by directly giving every participant assurance in writing. Before every interview, guarantees were made to participants of the findings of privacy. It was proven that no participants will be traced or linked to any of their opinion in the research. This was important as some participants are in the paramilitary or police forces where their comments could expose them to risk.

The last aspect of ethical consideration was data integrity. It was fundamental and essential for data integrity to be upheld to ensure the validity and integrity of findings. One way of enhancing integrity was through the prevention of unauthorised or third-party access to information and data. It was achieved through careful storage of collected data and passwords to protect electronic records stored in computer systems.
Bias was avoided during data collection by allowing the participants to express themselves freely (Robson & McCartan, 2016). The researcher did not suggest any research direction or make comments that could influence the discussion during the interviews or focus groups.
Chapter 5: Data Analysis

This chapter presents findings from the fieldwork conducted in Nigeria in the Spring of 2017. The focus is to answer the question, "What is the current state of cybercrime in Nigeria?" The other research questions were derived from this question to inquire about the status of different aspects of cybercrime from the country. Interviews and a focus group were the primary means of collecting data for this research.

Overall, 28 participants were involved in the data collection. Acronyms were used to represent the different stakeholder groups of those interviewed (Table 4).

Table 4: Research Stakeholder Group Acronym Details

<table>
<thead>
<tr>
<th>Stakeholder Group</th>
<th>Acronym</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSCDC Officers</td>
<td>NSCDC</td>
</tr>
<tr>
<td>Nigerian Police Force</td>
<td>NPF</td>
</tr>
<tr>
<td>EFCC Staffs</td>
<td>EFCC</td>
</tr>
<tr>
<td>Nigerian Judiciary</td>
<td>JUD</td>
</tr>
<tr>
<td>Ministry of Justice</td>
<td>MOJ</td>
</tr>
<tr>
<td>National Assembly</td>
<td>NASS</td>
</tr>
<tr>
<td>Convicted Criminals</td>
<td>CC</td>
</tr>
<tr>
<td>Criminology Researchers</td>
<td>FUT</td>
</tr>
<tr>
<td>NSDC Officers involved in Focus Group</td>
<td>FG</td>
</tr>
</tbody>
</table>

The chapter begins with a demographic analysis that shows the characteristics of the participants. The demographic analysis provides the distribution of the participants across the involved stakeholder organisations. It explores the gender distribution of participants and offers a sociocultural summary of participant distribution.

5.1 Demographic Analysis

Three types of data are used to explain the demographic details of the research participants. The first data type is gender. As presented in Table 5, there are three female participants and 25 male participants (see: Appendix H for participant details). The distribution shows that only the NSCDC and EFCC have female participants, while the remaining stakeholder groups have only male participants. The findings demonstrate the assertion by Evelyn and Adedayo
(2014) that Nigerian society has been patriarchal from time immemorial. Despite growing encouragement for gender equality, cybercrime governance and perpetration in Nigeria still reflect a high gender bias against females.

**Table 5: Gender Distribution of Research Participants**

<table>
<thead>
<tr>
<th>Stakeholder Group</th>
<th>Male</th>
<th>Female</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSCDC Officers</td>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td>Nigerian Police Force</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>EFCC Staffs</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Nigerian Judiciary</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Ministry of Justice</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>National Assembly</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Convicted Criminals</td>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td>Criminology Researchers</td>
<td>3</td>
<td>0</td>
</tr>
</tbody>
</table>

Source: Interview Data

Table 6 presents the stakeholder group and the management level of the participants. Two core law enforcement agencies (NSCDC and the Nigerian Police Force) have participants at the three management levels. It suggests that information at the strategic, tactical and operational level can be retrieved. The distribution also shows that EFCC has two participants at a senior management level. The data reflects the low number of officials (as reflected in the number of participants in EFCC and Ministry of Justice participants) that deal with cybercrime at National headquarters and the lack of official presence in every state of Nigeria\(^{46}\).

**Table 6: Participant Organisation Level Distribution**

<table>
<thead>
<tr>
<th>Stakeholder Group</th>
<th>Senior Management</th>
<th>Middle Management</th>
<th>Junior Staff</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSCDC Officers</td>
<td>3</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Nigerian Police Force</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>EFCC Staffs</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Nigerian Judiciary</td>
<td>0</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Ministry of Justice</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>National Assembly</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Criminology Researchers</td>
<td>1</td>
<td>2</td>
<td>0</td>
</tr>
</tbody>
</table>

Source: Interview Data

\(^{46}\) As at the time of this research, the cybercrime unit in the EFCC is small sized with about 10 personnel while the Federal Ministry of Justice have only 2 personnel in the cybercrime department.
Criminology researchers are academics that have majored in cybercrime and continue to shape understanding in Nigeria\textsuperscript{47}. The Ministry of Justice has only one participant. This number reflected the small size of the cybercrime department in the Ministry\textsuperscript{48}. Overall, the management distribution demonstrates the size of the stakeholder group.

*Table 7: Research Participant Academic Qualification*

<table>
<thead>
<tr>
<th></th>
<th>PhD</th>
<th>MSc</th>
<th>BSc/HND</th>
<th>SSCE</th>
<th>Unknown</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSCDC Officers</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td>Nigerian Police Force</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>EFCC Staffs</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Nigerian Judiciary</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Ministry of Justice</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>National Assembly</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Convicted Criminals</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>Criminology Researchers</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Source: Interview Data

Table 7 contains the distribution of participant qualifications and convicted criminals. The qualification with the highest number of participant is BSc/HND\textsuperscript{49} with 12 participants, followed by SSCE (the equivalent of GCSE) with 7 participants. From the qualification details, most participants are literate and have primary education. Because the participants have basic education and literacy, communication was conducted in the English Language while reading and signing the consent forms.

All the criminology researchers have completed their doctorate. One of the researchers studied outside the country with first-hand knowledge of the perception of cybercrime in Nigeria;

“*While I was in Malaysia, the indigenes often think all Nigerians are Yahoo boys. Most times, I have been addressed as a scammer because of the perception that some Nigerians in the country have given them*”. (FUT2, Interview conducted on the 21\textsuperscript{st} of March, 2017).

\textsuperscript{47} They are lecturers at the Federal University of Technology, Minna. The only Nigerian University offering a degree course on cybercrime as at the time of data collection.

\textsuperscript{48} It had only 3 officials as at the time of collecting data for this research.

\textsuperscript{49} An equivalent of University first degree
5.2 Financial Motivation

Financial gain remains the initial motivation of cybercrime in Nigeria. From the early stage of these crimes, financial incentive was the dominant and primary motivation. Since the inception of public access to the internet in Nigeria\(^{50}\), it became a primary source for defrauding unsuspecting victims (Igba et al., 2018). One of the convicted criminals acknowledge that young people are interested in cybercrime for monetary gain:

“When we started those days around the 1990s, the money we were making was the reason why people wanted to be part of the crime. It was easy money, and people envied us.”

(CC2, Interview conducted on the 19th of March 2017).

Some fundamental environmental factors have contributed to the motivation pattern that ignited the growth of these crimes. Some of these factors are the justifications and underlining reasons for the initiation and evolution of the crimes. Factors such as poverty, unemployment, low living standards and corruption are potent stimulants to crime in society (Webster & Kingston, 2014; Yaacob, 2015). Some of these factors are highlighted and explained by the participants of the empirical research.

There are different levels of support for each underlining contributor to financial motivation. Table 8 provides a summary of the numbers of participants that suggested or supported each of the factors.

Table 8: Factors that influence Financial Motivation

<table>
<thead>
<tr>
<th>Participants</th>
<th>Contributing Factor</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>MOJ1, EFCC1, NPF 1, 2, 3, 4, 5; NSCDC1, 2, 3, 4, 5; FUT1, 2, 3; CC1, 2, 3, 4, 5; FG1, 3; NASS1, 2; JUD2;</td>
<td>Financial Gain</td>
<td>25</td>
</tr>
<tr>
<td>MOJ1, NSCDC1, 2, 4, 5; CC1, 2, 3, 4; FG1, 2, 3; JUD1, 2; FUT1, 2, 3; EFCC2; NPF1; NASS2;</td>
<td>Unemployment</td>
<td>20</td>
</tr>
<tr>
<td>EFCC1, NPF2, JUD1, 2; NASS 1, 2; CC1, 2, 3, 4, 5, 6; NPF 1, 3, 4, 5; NSCDC3</td>
<td>Poverty</td>
<td>17</td>
</tr>
<tr>
<td>All Participants (Table 7)</td>
<td>Standard of Living</td>
<td>28</td>
</tr>
</tbody>
</table>

\(^{50}\) Through cybercafes in the mid-1990s.
5.2.1 Financial Gain

Financial gain regarding monetary reward remains a significant factor in the perpetuation of this crime. It is intended to satisfy the material tastes of cybercriminals. Culturally, Nigerians exhibit a strong preference for materialism, leading to increased pressure to engage in any vices (Okoli & Ugwu, 2017). For example, a common phenomenon is for Nigerians to have multiple mobile phones and other digital devices. A member of the national cybercrime governance team stated that;

“The motivation has always been how to get the money out. So, apart from one or two politically motivated attacks on government websites and all, the criminal efforts have been focused more on getting the money.”

(MOJ1, Interview conducted on the 2nd of March, 2017)

“The other one we are experiencing is political interest, and the cybercriminals that engage in pushing forward a particular political interest are involved in it for the money. They are paid to do it. So, for the cybercriminals, behind his mind is the money he gets.”

(EFCC1, Interview conducted on the 2nd of March, 2017)

Financial reward remains a significant factor for cybercrime in Nigeria (Hassan et al., 2012). The cash inflow from victims in different parts of the world point to the expected outcome among the perpetrators. Adesina (2017) noted that financial gain was the first notable motivation since the inception of such crimes. About ninety per cent of participants agreed that money or monetary gain is a significant motivation for the crime. As respondents commented;

“The major reason for cybercrime, especially in Nigeria, is for people to defraud people.”

(NSCDC1, Interview conducted on the 8th of March, 2017).

“What was going on until 2006 .... what the fraudsters were looking for was money. At that time, money was the deciding factor and not to tarnish anybody's image or not to harass anybody but to get money, to defraud and to obtain monies.”

(EFCC1, Interview conducted on the 2nd of March, 2017)

“It is the money they will get from the people they defraud and other activities that continue to make them commit the crime. They will continue until they get another person that will give them money.”
One of the convicted criminals agreed that cybercrime involvement was to make money to support the family after his father was suddenly sacked from government service in 2000.

“I became a Yahoo boy because the government sacked my father. He is a teacher and cannot provide any money for my education, and feeding the family becomes hard. The only reason I started was to make money.”

(CC5, Interview conducted on the 19th of March 2017).

Since the inception of cybercrime in Nigeria, financial gain is a primary motivation that has driven the AFF\textsuperscript{51} prominence. Participants agree that money remains the oxygen that has driven criminal activities.

5.2.2 Unemployment

Unemployment is a socioeconomic factor that puts a strain on society and can affect the entire dynamics of a country and its people. Idris (2016) noted that the increase in the unemployment level could directly result in a rising crime rate. However, the findings point to conflicting beliefs about the contribution of unemployment to crime.

Seventy (70) per cent of the participants believe that unemployment\textsuperscript{52} and the need to be financially independent are why they engage in cybercrime.

“There is a lot of unemployment. A lot of graduates, a lot of uneducated youths are unemployed, and so they are interested in whatever to do to get the buck, the fast buck.”

(MOJ1, Interview conducted on the 2\textsuperscript{nd} of March, 2017)

“A graduate, somebody who went to school who spent years in school, hopeful for a better future. But after graduating, after youth service, he becomes astonished, no jobs, no nothing. Even they go for a master’s degree, they come back; you still find out no job. So unemployment. When you don’t have employment, and you are growing, you want to have a family; you want to marry. So people take crime and thanks to this IT something.”

(NSCDC4, Interview conducted on the 8th of March, 2017).

\textsuperscript{51} Advanced Fee Fraud

\textsuperscript{52} The Nigerian case is explained in Section 1.5.1
Despite the unemployment emphasis among participants, the profile of some convicted criminals points to the contrary. For example, one of the convicted criminals admitted that the family is not poor, and he was a university student.

“We are ok, financially. I was given everything as a student. I cannot say unemployment was the reason for me being involved in this crime.”

(CC3, Interview conducted on the 19th of March 2017).

Of the six convicted criminals interviewed, three of them are undergraduates being sponsored by their families. Hence, this finding challenges the unemployment argument. Also, one of the participants (an NSCDC staff) questions the unemployment argument by stating that even the employed engage equally in cybercrime.

“Most Nigerians, even if they have jobs, they don’t feel the job is enough for them. They still want to cut corners and have extra income to live. And they feel that because of the nature of online activities that if they are into online crime or cybercrime, it will be difficult for them to be detected.”

(FG1, Interview conducted on the 8th of March, 2017).

Further substantiating evidence is the involvement of gainfully employed individuals such as bankers, law enforcement agents, and other professionals among the perpetrators. The contrary evidence suggests unemployment is not necessarily a factor in cybercrime perpetration. Two participants from the Judiciary and the cybercrime researchers point to greed.

“When you commit a crime, it hurts people, and you cannot say that economic conditions are responsible. It is a choice that the criminals take and an easy way out of illicit gain.”

(JUD1, Interview conducted on the 27th of March, 2017)

“Greed from the people that are involved in such thing (cybercrime). Though we have a lack of employment, that should not push people to do what is not correct.”

(FUT1, Interview conducted on the 21st of March, 2017)

Concerning the role of unemployment, it may be logical to argue its influence on the conduct of cybercrime. However, it does not explain the motivation for every cybercriminal. Some individuals are from an affluent or middle-class background yet still engage in crime. Greed can be a significant reason rather than unemployment.
5.2.3 Poverty

This sub-theme is one of the most contentious in this research. Participants within the criminal justice system continue to demonstrate different opinions and argument over the significance of poverty. It is another justification generating the financial motivation to commit the crime. Webster and Kingston (2014) stated that poverty creates many causal chains for potential criminogenic behaviour. Eleven of the participants identify poverty as a significant contributor to motivation. The comment below by one of the EFCC participant captures the poverty argument;

“There is an economic downturn; there is poverty. I am not saying that poverty excuses scam, but it aggravates it. A man who is not predisposed would have committed crime. If he had food to eat and could pay his bills, he may end up getting into crime because he cannot meet his daily requirement. He cannot feed, accommodate himself and things like that.”

(EFCC1, Interview conducted on the 2nd of March, 2017).

Yet, some law enforcement participants (EFCC, NPF and NSCDC) state that poverty cannot justify crime. Their argument is that crime was wrong irrespective of the cause. Summing up this argument from 4 of the participants is NSCDC2;

“There is no justification. If it is justified, offline crime can also be justified. Economic condition is not viable or a justification.”

(NSCDC2, Interview conducted on the 8th of March, 2017).

However, there is a contrary opinion. A member of the Nigerian Police Force highlights poverty and lack of opportunities as clear justifications for youths to engage in these crimes:

“Yes, the life of crime can be justified based on the economic situation of the country. There is no employment, lack of employment is one of the causes. Secondly is the bad leadership we have in this country.”

(NPF2, Interview conducted on the 20th of March, 2017)

From his responses, this participant highlights that the economy is in recession, and people find it difficult to cope. Engaging in cybercrime from this perspective is an economically viable means to generate wealth. The example of the two Judicial participants demonstrates the sharp differences between the two sides of the argument. One member of the Judiciary stated that;
When you commit a crime, it hurts people, and you cannot say that economic condition is responsible. It is a choice that the criminals take and an easy way out of illicit gain.”

(JUD1, Interview conducted on the 27th of March, 2017)

While the other stated that;

Yes, the economy is hard, and people have to find a way to survive.”

(JUD2, Interview conducted on the 28th of March, 2017)

However, the difference in opinion seems to highlight the gap between the economic reality of the Nigerian elite and the poor masses. There is a general belief that politicians in government are privileged and cannot feel the pain and difficulties of the lower class. The difference is evident when the opinion of convicted criminals and members of the National Assembly are compared (NASS).

The two participants at the National Assembly agree that poverty necessitated by harsh economic conditions is not a sufficient justification for cybercrime;

“We can say they (cybercriminals) are borne out of the economic problem we have in Nigeria. But, that does not mean it is enough reason.”

(NASS2, Interview conducted on the 26th of March, 2017)

Three convicted criminals agree that poverty and severe economic conditions are a significant contributor to their involvement.

“I have no job, no income and I need to make money to eat and do other things. Government is not helping. I have no other option than to join boys in doing yahoo on the internet”.

(CC1, Interview conducted on the 19th of March 2017).

“We are poor and have no access to money. This work (cybercrime) is the only way available for boys to make money.”

(CC6, Interview conducted on the 19th of March 2017).

Poverty remains a controversial topic among participants. Within law enforcement circles, there remains an argument as to whether it is justified or not. From the discussion, it is agreed that it is a contributing factor. It suggests the criminal justice system includes many individuals who sympathise with the poor of the country in perpetrating this crime.
Another finding is the difference in perception between Nigerian politicians and convicted criminals. This could be based on social class. The difference in class coincides with the difference in views. While politicians at the top do not experience poverty, most of the masses see poverty as a convincing reason for committing cybercrime.

5.2.4 Standard of Living

The growth of poverty and unemployment established in both the documentary analysis (see Section 1.3.1) and empirical research (see Section 5.2.2 and Section 5.2.3) have lowered the standard of living for most Nigerians. Many Nigerians struggle for decent accommodation, primary health care facilities, education, security and even food (Omoniyi, 2018). Some of these individuals are educated and computer literate but without limited substantial work opportunities. Cybercrime can act as the ladder to an improved standard of living among young people. This situation is seen as quite evident among the participants. The entire participants agree that crime on the internet had provided an avenue for financial income that improved their everyday living.

One of the NSCDC participants stated that;

“Everybody likes money, there is nobody that does not like a good life. They (cybercriminals) believe that maybe, there is no employment opportunity, they are not creative, and see that the only way they can have means of livelihood is to identify with Yahoo boys.”

(NSCDC1, Interview conducted on the 8th of March, 2017)

It is a general phenomenon that cybercrime provides easy money that enables perpetrators to achieve their desired financial goals. In the focus group, one of the participants highlights how online crime can improve living standards. She stated that:

“They are enjoying what they are doing due to what they want to become in their social life. Maybe like flashy cars, different types of cars, houses or even dresses\(^{53}\) and some actions concerning the financial aspect of their enterprise. So, they are enjoying the work they are doing.”

(FG2, Interview conducted on the 8th of March, 2017)

\(^{53}\) The cybercriminals buy flashy dresses and designers towards looking wealthy and acceptable in the society.
Another argument is that an improved standard of living may not be a persuasive argument. Nine participants felt that flamboyance and excessive greed were driving forces for engaging in this crime. For example, two of the participants stated that:

“Some of them see it as a means of climbing the affluence ladder. Some are caught (arrested), even as young as they are, you see them riding big cars, having so many properties for themselves and showing off as a big boy in society.”

(FUT1, Interview conducted on the 21st of March, 2017)

Three NPF participants state that cybercriminals could justify their actions because the economy of the country was tough, and they needed to improve their standard of living.

“Because, when there is no job, they see cybercrime in such a way of getting money easily through cybercrime. A lot of male youth engage in cybercrime. It ensures that cybercriminals make ends meet.”

(NPF2, Interview conducted on the 2nd of March, 2017)

Some of the convicted criminals argue that improving their standard of living contributed to financial motivation. Some of their opinions were that:

“I am poor, and where my family is living is not good. Our life was bad. So, I have to join the Yahoo business to better our lives.”

(CC1, Interview conducted on the 19th of March 2017).

“I lost my Sister (******.54) to ordinary typhoid. Since that day, I have made up my mind to make money through any means. Cybercrime provides a way to make this money.”

(CC6, Interview conducted on the 19th of March 2017).

“Approximately 45% of young people think cybercrime can increase their chances in society. It helps to take care of the family.”

(CC2, Interview conducted on the 19th of March 2017).

The argument on the standard of living reflects differences in opinion between working Nigerians and the masses experiencing economic hardship. However, one result of the improved standard of living sub-theme is the evolution of the Yahoo-Yahoo subculture (it can be called Yahoo, Yahoo plus). The Yahoo-Yahoo subculture is fundamental and synonymous

---

54 The name of the sister was withheld to uphold the anonymity requirement of the research.
with cybercrime in Nigeria. The emergence of wealthy young people because of criminal proceeds directly created a niche trait used to identify crime participants. Ferrel (1998) stated that many youths often carve out their personal or group identities after being excluded from public involvement.

Most cybercriminals are not respected in a society based on their low-income family background or class. Adeniran (2008) noted the subculture evolved as acceptance of Internet technology by youths. The characteristics of the subculture include lavish spending, partying, extravagant dressing, and buying imported drinks. Omeire and Omeire (2017) noted that perpetrators are also called “Guymen” who live extravagantly and demonstrate outward opulence beyond their apparent means. This subculture fuels the cybercrime perpetration with a distinct outward appearance and actions that make them identifiable in public.

All the participants agree that cybercriminals, over time have developed a sub-culture that differentiates them in society. Two factors characterise this sub-culture viz use of the internet to defraud victims and an extravagant lifestyle (Igba et al., 2018; Saulawa & Abubakar, 2014). Participants attest to the two characteristics. A member of the National Assembly and the NSCDC point to the “Yahoo-Yahoo” terminology and its meaning. He said:

“I am talking about Yahoo. You know, we call it Yahoo here. When we call you Yahoo, that means you are an online scammer.”

(NSCDC4, Interview conducted on the 8th of March, 2017)

“There are some (young people) that are using it (technology) for the dubious process regarding fraud, frauds of any type, especially the Yahoo Yahoo.”

(NASS2, Interview conducted on the 26th of March, 2017)

On the other hand, participants establish a clear lifestyle in this subculture;

“They build mansions, duplexes, flats. They are the ones visiting clubs when you visit clubs, nightclubs and they drink the latest most expensive wines, and have beautiful ladies.”

(NSCDC4, Interview conducted on the 8th of March, 2017).

Over time, this subculture has been accepted in society55, thereby increasing its prominence. The Yahoo subculture is making young Nigerians financially empowered, thus making them become respected among people. The prominent Nigerian entertainment industry glorifies this

55 The increasing acceptance of the cybercriminals by the Nigerian public strengthens the belief of the cybercriminals thereby enhancing the relevance of the Technique of neutralisation.
subculture in music and movies (Adebayo, 2017; Adesina, 2017). Decades of continuous perpetration and apparent affluence is changing public perspective about it as a crime. Eight participants acknowledge the increasing societal acceptance negatively. They stated:

“Well, some people are into cybercrime, they are able to make it. They call them ‘Yahoo plus’. Because they are well accepted within society, they are on the increase. So it seems as if society is not ready to wage war against them. And that is why its occurrence is still rising.”

(NSCDC2, Interview conducted on the 8th of March, 2017).

Five of the convicted criminals affirm both its increasing popularity and acceptance in society. They state that the material nature of society, together with increased economic hardship, create a view of the Yahoo lifestyle as a means of financial gain. They argue that:

“We are part of society. People want to join because they see that we make money. Parents bring their children and encourage them to join us.”

(CC3, Interview conducted on the 19th of March 2017).

“Because of the money, we are accepted. Some of us own businesses, have chieftaincy titles, are in politics and so on”.

(CC4, Interview conducted on the 19th of March 2017).

One significant worry of the government is the increasing acceptability of cybercriminals in society. It is argued that:

“The perception issues, the values in the society has gotten to a level where nobody cares how you make money. The man who suddenly became very rich is revered. He even has police escorting him all over the place while the honest man that not rich get shoved off the way by the police so that the criminal will pass.”

(MOJ1, Interview conducted on the 2nd of March, 2017)

Despite the seeming popularity and social acceptance of the Yahoo subculture, two convicted criminals state that the immediate family and surrounding society are not happy with the lifestyle despite their increasing financial power.

“For me, I cannot say that society accepted my work. My parents detest my participation. My Dad never collected any proceeds from the crime and was never supportive even when he was struggling financially”.

(CC6, Interview conducted on the 19th of March 2017)
Other participants identify the resentment to the perpetration of the crime.

“Cybercrime is directly or indirectly robbing an original owner of any property on the computer or electronic media to access and dupe those people that own the original thing. So society is not according to a positive impression of that.”

(NASS2, Interview conducted on the 26th of March, 2017)

Improving the standard of living demonstrates a socioeconomic dimension to the financial motivation of cybercrime. Most participants support and justify the financial gain motive of the cybercriminals. The acceptability of the Yahoo culture remains a point of substantive argument. A shared culture exists among young perpetrators of crime. However, support from society appears to be subjective. While participants, including convicted criminals, agree to have been accepted by the participants, a significant dissenting opinion exists. Hence, it will be wrong to claim, as a result, that Nigerian society supports the Yahoo-yahoo subculture.

5.3 Behavioural motivation

Over time, cybercrime in Nigeria has evolved, and motivations have changed. Despite the financial gain that remains a significant factor, other motives regarding behaviour are emerging. Cybercrime in Nigeria is changing in motivation and execution. This theme focuses on non-financial incentives. Evolution has resulted in changing explanations for committing a crime.

“But, as much as I am concerned, people are motivated into a crime based on different factors. It may even be political, revenge; political revenge may even be involved.”

(NSCDC3, Interview conducted on the 8th of March, 2017)

As identified in the quotation above, different factors are responsible for a new set of motivations. The factors attracted different levels of support among participants. Table 9 shows the various participants that supported each element towards demonstrating the proportionality.

56 Responsible for AFF prominence among cybercriminals from Nigeria.
Table 9: Factors Responsible for Behavioural Motivation

<table>
<thead>
<tr>
<th>Participants</th>
<th>Contributing Factor</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>NPF1, 2, 3, 4; CC1, 2, 5, 6; JUD1, 2; EFCC1, 2; MOJ1; NPF1, 5; NSCDC1, 2, 4; FG2, 3; NASS2</td>
<td>Revenge</td>
<td>21</td>
</tr>
<tr>
<td>NSCDC1, 4, 5; CC1, 3, 4, 5, 6; NPF1, 3, 5; FG2, 3; MOJ1, CC2, 3, 5, 6; NPF2, 4; EFCC1, 2; JUD1; NASS2; NSCDC 4</td>
<td>Frustration</td>
<td>13</td>
</tr>
<tr>
<td>CC1, 4, 5, 6; MOJ1; NSCDC4, 5; FG1; FUT1;</td>
<td>Anger</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>Creativity and skills</td>
<td>9</td>
</tr>
</tbody>
</table>

5.3.1 Revenge

Revenge is becoming a recurrent basis for cybercrime in Nigeria, with different reasons and dimensions identified by respondents. The nature of revenge is deemed to be subjective. The first aspect concerns passion and emotion. Leukfeldt et al. (2017) discover passion as a primary driver of cybercrime\(^{57}\). Different people have weaponised the internet in committing passion-driven vendettas against other individuals. Cybercriminals could be motivated by disappointment and the need for revenge against a previous lover. One of the convicted participants highlights a case of revenge pornography:\(^{58}\)

“a case involved a situation where an ex-lover in anger sent the nude picture of a lady to her relatives.”

(NPF4, Interview conducted on the 28th of March, 2017)

Three convicted criminals affirm the emergence of revenge pornography.

“We are seeing cases where boys are exposing naked pictures of their previous girlfriend because they are angry or want to embarrass the girl.”

(CC2, Interview conducted on the 19th of March 2017).

\(^{57}\) The findings from the interview agreed that passion exhibited in the form of revenge is a major motivation among Nigerian cybercriminals.

\(^{58}\) This is emerging problem in Nigeria with numerous sexual contents uploaded on the Internet without the consent of the owners. It has generated limited research focus among researchers in Nigeria.
Different relationships often result in this type of crime. One fundamental differentiation is that the offence can reflect a form of retaliation;

“I have seen cases where nude pictures of ladies are released online as retaliation by other people or their ex-boyfriend. Revenge is to hurt the lady because she decided to leave them.”

(JUD1, Interview conducted on the 27th of March 2017).

Yet, other forms of revenge pornography involve blackmail. One of the interviewed convicted criminals narrates a case involving a client in Nigeria using the nude picture of her friend in the UK for ransom. The money was collected, and the images were returned and destroyed:

“Revenge pornography often involves a setup by friends who want to make money from their other friends in the UK. I was involved and stopped them from publishing the pictures. I contacted the owner and collected the money. Without me, they would have put the picture on the internet.”

(CC6, Interview conducted on the 19th of March 2017).

The law enforcement agents agree with convicted criminals that blackmail and extortion stimulate revenge motivation behind this crime of passion. Fifteen participants confirm the way financial motivation has multiplexed into revenge using indecent images of victims.

“Some of the crime we see associated with this (revenge pornography) most especially cyberbullying, we can see people using it for blackmail.”

(EFCC1, Interview conducted on the 2nd of March, 2017)

Yet, while acknowledging the revenge element, some argue that financial gain has multiplexed into revenge motivation. The argument is that sextortion is responsible for the core perpetration of this crime. Participants from the Ministry of Justice stated:

“Things like revenge porn are growing in Nigeria. It is more of sextortion than revenge porn. Again, the reason, the threat, to expose some of this stuff is tied to financial gain. From cases that we have seen and that have been reported, that have come to the attention of the authorities, for the most part, you find out there is some blackmail, some demand for payment.”

(MOJ1, Interview conducted on the 2nd of March, 2017).

Another angle to the revenge motivation can be between staff and their work organisation. Dissatisfied employees can decide to hurt their organisation through the internet (Arora,
2016). Four participants identified that insider cybercrime resulted from employees that are not being happy within their organisation.

“Employees often use their position to leak vital information to colleagues so that their IT system can be attacked. The motivation is to get back to the company.”

(JUD2, Interview conducted on the 28th of March 2017).

“Staff can initiate cyber-attacks to take revenge for their ill-treatment or score a point within the organisation. For example, we have seen cases where staffs used a cyber-attack to justify an increase in funds for the IT department.”

(NPF4, Interview conducted on the 28th of March 2017).

The most critical aspect of revenge increasingly appears to be revenge against the Government. Eighteen (18) participants agreed that the technological infrastructure of the Government has been attacked by youths that see it as revenge.

“We see youths using their skills to attack government websites and other institutions. They are taking revenge against poor governance and the bad state of the country.”

(NSCDC5, Interview conducted on the 8th of March, 2017)

One of the Judiciary participants commented that defendants often state that their crime does not affect any individual. Cybercriminals often accuse the elite of stealing resources, so any crime to extort or disrupt Government technical capability is justified.

“He (one defendant) said the attack on the government database was not a crime because they have not been responsible to the masses. There is a need for the masses to make their feelings heard through technology skills.”

(JUD1, Interview conducted on the 27th of March 2017).

Despite increasing support for revenge as a significant contributory factor to focused Government attacks, three participants argued that the core motivation remained money. For example, one of the EFCC participants stated that;

“The other one we are experiencing is political interest, and the cybercriminals that engage in pushing forward a particular political interest are involved in it for the money.”

(EFCC1, Interview conducted on the 2nd of March, 2017)
"So, apart from one or two politically motivated attacks on government websites and all, criminal effort has been focused more on getting the money."

(MOJ1, Interview conducted on the 2nd of March, 2017).

Revenge can be a motive for cybercrime for different reasons. It results in the evolution of crime against individuals, organisations and government without aiming for financial gain. Yet, despite the increasing occurrence of these types of motivation, some stakeholders still argue that financial gain is the background to revenge. Revenge is the result of a desire for financial gain. Overall, it remains evident that revenge is stimulating new motivations that do not necessarily reflect the quest to make money.

5.3.2 Frustration

Frustration is another motivation that may stimulate cybercrime. When an individual is frustrated, crime can become attractive. Nigeria has a societal stratification that has resulted in inequality, limiting opportunities for the poor in society (Imhonopi & Urim, 2013). Frustration at not achieving basic needs as pointed out by Maslow (Maslow, 1954), results in the feeling of being inferior, weak, worthless, or helpless. Among criminals, this feeling makes a crime a means of achieving self-legitimacy. Broadhurst et al. (2014) attest that perpetrators can resort to a different range of offences based on economic frustration. For example, many frustrated individuals in the lower strata of society are fostering terrorism (Nasim & Yunusbek, 2013).

Within cybercrime in Nigerian, frustration has been a significant source in driving the growth of cybercrime. As discussed earlier, most of the participants recognise the economic hardship in the country. As a result, frustrated individuals can become cybercriminals. Thirteen participants state that frustration contributes to criminal usage of the internet by Nigerians.

“You know, it encourages cybercrime because somebody good cannot get a job because he is 26 years old. He becomes frustrated and goes for another thing.”

(NSCDC4, Interview conducted on the 8th of March, 2017)

Five of the six convicted criminals point to frustration arising from different aspects of Nigerian life. Notably, one participant claims the high level of corruption was the basis of the problem;

59 As postulated by Strain Theory in Section 2.5.2.
“Lack of opportunity for young people. For example, 32 Billion naira was embezzled, and people are poor. People are frustrated because there is no judgement for big offenders.”

(CC5, Interview conducted on the 19th of March 2017)

One general frustration among young people is the perceived failure of governance;

“Boys are tired....nothing to show for the years of schooling. The country has no plan for us, and it is frustrating. It makes everybody do bad things on the internet.”

(CC1, Interview conducted on the 19th of March 2017)

Another element to the frustration factor is the impact of urban-rural migration on public security. Rural areas lack amenities, thereby necessitating the movement of their citizens to urban areas. This is prominent among thirteen law enforcement agents that participated in this research. They argued that:

“There is an influx of people to the town. People are leaving the villages because they don’t have some of these basic amenities. No light (electricity), no road, basic amenities, it is only in town that you can have it. There are no jobs in rural areas. So, people tend to look for greener pastures in the urban areas.”

(NSCDC1, Interview conducted on the 8th of March, 2017)

Ajaero and Onokala (2013) stated that those migrating from rural to urban areas often struggle to find a job or effectively settle into the social and economic settings of their new location. The failure to achieve their desire often results in extreme frustration among the migrants. They usually end up living in slums and becoming economically underprivileged within the urban centres.

“We have seen that individuals from the rural area are frustrated from not having a better life in urban centres. They become frustrated and engage in crime.”

(NPF3, Interview conducted on the 28th of March, 2017).

Nineteen participants acknowledge that rural-urban migration has contributed to the rise in cybercrime. The law enforcement participants establish the role that this migration is playing within cybercrime perpetration.

“People are migrating from rural areas en mass to urban areas. And this migration comes with a lot of criminal activities including cybercrime, and other types of crime.”

(NSCDC3, Interview conducted on the 8th of March, 2017).
“There is an effect, but the percentage, I cannot say. Movement from the rural area to urban area influences or has an impact in causing cybercrime.”

(FG2, Interview conducted on the 8th of March, 2017)

Another area of frustration is the efficiency of law enforcement. All eight participants in the NSCDC affirm their frustration with cybercriminals among the rural-urban migrants.

“Because when crimes are committed in urban areas, they go back to the village. They are making it very difficult for law enforcement agents to fish them out. When they get to the village, they tend to influence those that are in the village too. When they want to surface again, some of their friends will also surface with them, thereby making it difficult.”

(NSCDC1, Interview conducted on the 8th of March, 2017)

Frustration is derived from different sources and often fuels behavioural cybercrime. Sources of frustration include poor governance, lack of opportunity and a failure to meet basic needs. Rural-urban migration often increases the number of frustrated perpetrators as migrants fail to meet their basic needs. Law enforcement is difficult when perpetration is based on the mobility caused by rural-urban migration.

5.3.3 Anger

Anger is another contributor to behavioural motivation. Agnew (2001) noted anger as a negative emotion that can result in criminal behaviour. It can emanate from strain factors that perpetrators are experiencing. People suffering failure to achieve their goals experience anger that can stimulate crime. It has translated into different types of crime among perpetrators.

“In some cases, I have come across cybercriminals that have been driven by anger. They commit a very dangerous crime and affect people.”

(MOJ1, Interview conducted on the 2nd of March, 2017)

The anger theme identifies in the responses from twelve participants. One of the convicted criminals provided a vivid example of the contribution of anger. It is summed up in the quote below:

“I am usually angry with the government for sacking my Father. I always support any plan or attack on the government system. They deserve it.”

(CC6, Interview conducted on the 19th of March 2017)
The quotation from the convicted criminal highlights a hatred of the Government. Anger arises from the action or inaction of Government. A law enforcement agent justified the anger from cybercriminals:

“When the leaders fail to do the right things for the people. Even we that we are police sometimes are angry with the way the country is going. I can imagine these boys getting angry from poor treatment by the government.”

(NPF2, Interview conducted on the 2nd of March, 2017)

However, ten law enforcement agents state that anger on its own is not a viable contributor in any motivation towards cybercrime:

“I know the youths are angry. But, it is not enough for committing this type of crime. These criminals use anger to justify their wickedness against victims.”

(NPF4, Interview conducted on the 28th of March, 2017)

On the other hand, participants identify different crimes against individuals that anger can cause.

“When perpetrators are angry, some of the crimes can be cyberbullying, cyberstalking, and paedophilia.”

(EFCC2, Interview conducted on the 2nd of March, 2017).

From the responses, anger stimulated crime can be behavioural and not necessarily financial. The assertions contrast with the claim of another participant from EFCC;

“Cybercrime in Nigeria is still not strong. They still focus on money, and nobody can convince me that other reasons such as anger, animosity, and so on.”

(EFCC1, Interview conducted on the 2nd of March, 2017).

The two different arguments among the law enforcement agents demonstrate in their responses. Despite the recognition of anger, there is still an argument as to whether it is enough to motivate a crime on the web.

5.3.4 Creativity and skills

Creativity and skill are fundamental factors in the behavioural motivation of cybercrime in Nigeria. The need to demonstrate acquired skills is fuelling criminogenic activity by young people (Igba et al., 2018). There are limited opportunities for the productive and positive use
of technological skills. Hence, proficient young Nigerians deploy their competency criminally. The opportunity to use their skills can motivate highly skilled perpetrators. Four of the convicted criminals highlighted creativity as a significant contributor to the perpetration of different cybercrimes. The quotation showcases their ideas.

“It (cybercrime) involves investment and returns. It involves stress, knowledge and skills.”

(CC4, Interview conducted on the 19th of March, 2017)

“It promotes creativity and skills. It provides an avenue for perpetrators to use their skills and be creative. It helps people to develop skills. It allows fast learning and produces ground for experimenting.”

(CC3, Interview conducted on the 19th of March, 2017)

Five participants believe that irrespective of the different skills, creativity is not the ultimate goal. Financial gain still provides motivation:

“He is not defacing a website for defacing sake. No, he is going to get money from it. Somebody else pays him to do that.”

(EFCC1, Interview conducted on the 2nd of March, 2017)

The creativity issue is based on the acknowledgement by 19 participants of the increased skills within the cybercrime perpetration:

“But the people perpetrating this, they are highly skilled. They are technical in their approach.”

(NSCDC1, Interview conducted on the 8th of March, 2017)

“To some extent, many of them are graduates or undergraduates of Nigerian Universities. So they know about it. They are skilled.”

(FUT1, Interview conducted on the 21st of March, 2017)

However, some of the participants argue that cybercrime in Nigeria is not that sophisticated or highly skilled. These participants mainly were within law enforcement. One of the EFCC participants state:

“Yes, I still say that the cybercrime landscape in Nigeria is not very developed. They are still trying to find their feet. The types of cybercrime they are involved in are not developed.”

(EFCC1, Interview conducted on the 2nd of March, 2017).
Yet, participants from other law enforcement agents acknowledge the growing skillset and sophistication of the criminal perpetration:

“Right now, we have a lot of Nigerian actors who can launch any form of attack at any level. Even now, some attacks are coordinated that are being launched.”

(MOJ1, Interview conducted on the 2nd of March 2017)

“We have some Nigerians creating viruses deliberately to either disrupt data. For instance, financial institutions like a bank.”

(NSCDC4, Interview conducted on the 8th of March 2017)

It became clear that creativity is viable as most participants affirmed that skill abounds in the perpetration. Furthermore, all convicted criminals state that skill and creativity are a significant factor for criminal behaviour:

“There are master hackers that are knowledgeable in Cisco network.”

(CC5, Interview conducted on the 19th of March 2017)

“The criminals and people who possess different skills are getting more. Everything I have needed, I have seen people hack different websites and do a lot of technical things.”

(CC6, Interview conducted on the 19th of March 2017)

This argument partly reflects the evolution of the crime. Smith (2008) affirmed that Cybercrime in Nigeria started from the low skilled AFF. Researchers in the field continue to argue about the skill level of perpetrators, as noted below:

“Yes. Initially, the skill level of Nigerians may not be that high. But recently, due to the Android platform, which is like open source. In no time, their skill level is on the increase in perpetrating these crimes. But from my interaction with some of the youths, I discovered that the skill level is there.”

(FUT1, Interview conducted on the 21st of March 2017)

Another researcher argued, however, that the skillset currently was not sophisticated but low level.

“But still, I don’t believe that the skill level is high because we still have the high rate of those that have no access to these devices. It means a larger part of the population is still in rural
areas, and most of them still have low access to these data devices. So, if you consider that, we may rate them medium.”

(FUT2, Interview conducted on the 21st of March 2017)

Creativity and skills are non-financial factors that border on the deployment of acquired knowledge. The technological competence among the perpetrators means an expansion in criminogenic behaviours. Creativity is a demonstration of skills, as shown by most participants, and the skill level is increasing. However, a significant number of respondents felt that the level of skills was not enough for sophisticated creativity. The convicted criminals unanimously state that the cybercriminals are highly skilled and competent to launch any attack.

5.4 Modes of Crime

The mode of crime is another characteristic of cybercrime in Nigeria that emerged from the findings. The growth has resulted in changes and advances in the manner of perpetration.

Table 10: Modes of crime Typology Distribution

<table>
<thead>
<tr>
<th>Participants</th>
<th>Contributing Factor</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>EFCC1, 2; JUD1; MOJ1; NASS2; CC1, 2, 3, 4, 5, 6; NPF 1, 4, 5; FUT2; FG2;</td>
<td>Phishing</td>
<td>16</td>
</tr>
<tr>
<td>FUT2, 3; NPF1, 2, 3, 4, 5; NSCDC1, 3, 4, 5; MOJ1; CC1, 2, 3, 4, 6; NASS1, 2; FG1, 2, 3; JUD 2;</td>
<td>Identity Theft</td>
<td>22</td>
</tr>
<tr>
<td>FUT2, 3; EFCC1, 2; NPF1, 4, 5; NSCDC1, 3, 4, 5; MOJ1; CC1, 2, 4, 5, 6; NASS1, 2; FG1, 2, 3; JUD 2;</td>
<td>Romance Fraud</td>
<td>23</td>
</tr>
<tr>
<td>NPF3, 4; JUD1, 2; NSCDC3; EFCC1, 2; MOJ1; NASS2; CC3, 4, 5, 6; NPF1, 4, 5; FUT2; FG2; NASS2</td>
<td>Hacking</td>
<td>19</td>
</tr>
<tr>
<td>NPF3, 4; JUD1; NSCDC4, 5; EFCC1, 2; MOJ1; NASS2; CC3, 4, 5, 6; NPF1, 4, 5; FUT1; FG2; NASS1</td>
<td>Cybercrime as a service</td>
<td>19</td>
</tr>
<tr>
<td>EFCC2; FUT2; NPF2; MOJ1; NSCDC4; CC1, 2 3, 4; FG3;</td>
<td>Attacking Government Infrastructure</td>
<td>10</td>
</tr>
<tr>
<td>CC1, 3, 4, 5, 6; EFCC1; NASS1, 2; NPF 4, 5; NSCDC2, 4, 5;</td>
<td>Kidnapping</td>
<td>12</td>
</tr>
</tbody>
</table>
There are many ways of committing cybercrime, ranging from social engineering to advanced technological attacks. Technology-dependent and technology-enabled crime provide a scope that is very wide for these types of crimes. It currently demonstrates a different mode of operation ranging from beginner, intermediate and expert level. This section explains different crime processes (Table 10) as presented by the participants.

5.4.1 Phishing

The concept of phishing among the perpetrators has graduated from an offline practise before the internet. Seven participants attest that Nigerians were already sending mail to addresses in foreign countries to establish communication for criminogenic behaviour. These respondents span law enforcement, Judiciary, and researchers.

“Dating back to the late 1990s, when the internet became prominent, should I say in Nigeria. By then, some Nigerians are involved in what we call the 419 scams. So, from the 419 scams, they were using snail mails, sending messages using post offices before the advent of the internet. So, when the internet came on board, it became effortless for people to reach what we term as first respondents.”

(EFCC2, Interview conducted on the 2nd of March, 2017).

“From the late 90s to early 2000, that was when there was a shift in the criminals from the way they do business; now they use technology to do that business. Initially, postcards and mail cards were used to communicate with people outside the country before they started their criminal work.”

(JUD1, Interview conducted on the 27th of March, 2017).

Because email is the most popular service at the introduction of the Internet, scams using a popular service such as Yahoo (hence the coinage of Yahoo Yahoo) is the foundation of these crimes. Seven participants highlight the migration from email to other platforms such as social media:

“Initially, all that was happening were people sending off emails, going on social media and pretending, opening an account on Facebook.”

(MOJ1, Interview conducted on the 2nd of March, 2017).
Migration is not as rapid as some participants claimed but was a gradual combination of both online-offline implementations. Five participants identified the mixture in the initial introduction of the Internet;

“Before 2003, there was an upsurge of these crimes (cybercrime) with the popularity of computers and computers. There came a new strain of crime, you know, that was committed partly online and partly offline. That was the crime called Advanced Fee Fraud (AFF) wherein emails are sent to unsuspecting individuals.”

(EFCC1, Interview conducted on the 2nd of March, 2017).

However, five participants argue that the internet was the primary reason why phishing was practised in Nigeria. This argument is that Nigerians were not prominent in offline implementation, and such practice was negligible. One of the National Assembly participants note that;

“I have heard people sent mail through NIPOST was used. I do not believe it because of the time, cost and inconveniences. This way of phishing does not work for me; it was not popular.”

(NASS2, Interview conducted on the 26th of March, 2017)

Irrespective of the argument, Nigeria has currently become a significant source of phishing on the web. Twenty-one participants noted the presence of various phishing activities.

“So, you have a lot of cloned, phishing going on…. So basically, what happens is that you find a group of people who are good at sending out all those phishing and social engineering.”

(MOJ1, Interview conducted on the 2nd of March, 2017).

All convicted criminals assert that phishing is a significant practice and continues to thrive.

“Every yahoo (cybercriminal) knows how to send an email to many people. It is the start of the job, and everybody does it.”

(CC3, Interview conducted on the 2nd of March, 2017)

One convicted criminal admits to having trained over twenty individuals stated that phishing is part of the first phase of training potential criminals;

“I always make sure that every new boy I trained knows how to send mass mail to different people. It is one of the starting points and always works because people will reply.”

(CC6, Interview conducted on the 2nd of March, 2017)
Most of the participants across the different stakeholder groups agree that the perpetrators are now significant phishing activity players. Yet, there remains a debate concerning the global perception of Nigeria being a leading source of crime. Seven law enforcement participants argued that phishing in Nigeria is highly exaggerated and convenient to label the country. The quote below shows the opinion:

“I have seen cases where people in places like China conduct phishing using the Nigerian IP address. I investigated the case and discovered the real IP address. This kind of case can paint Nigerian in a bad light.”

(NPF3, Interview conducted on the 28th of March, 2017)

“Some of the cases that are associated with Nigeria are not committed here. Sometimes, criminals use IP spoofing to make the crime look like it is coming from Nigeria.”

(EFCC2, Interview conducted on the 2nd of March, 2017).

However, some of the respondents agree that Nigeria is indeed a significant source of phishing. It is rampant, and it is felt that the global perception is appropriate;

“Let us say phishing, maybe Nigeria is not number 1, but it is in the leading pack, you get it.” (MOJ1, Interview conducted on the 2nd of March, 2017).

Phishing has been a strength within cybercrime in Nigeria. The web has created an avenue for advancing and enhancing the perpetration of this crime. Despite differences in opinion, it remains the reality that cybercrime in Nigerian is heavily involved in phishing and has successfully transformed the offline practice on the online platform. The fact is that a lot of phishing attacks originate from Nigerian cyberspace.

5.4.2 Identity Theft (Hurt the wealthy)

Identity theft is another sub-theme that is identified from the opinion of different participants in this research. Of the prominent crimes identified by three researchers, Identity crime is one of them;

“We have identity theft, we have denial of service attacks, and we have steganographic attacks in which a strange message is hidden in another cover.”

(FUT2, Interview conducted on the 21st of March, 2017).

Identity theft is often regarded as impersonation by law enforcement agents;
“You will just see people transfer money; they will hide their identity, withdraw the money through the system application; they transfer it to another place.”

(NPF3, Interview conducted on the 28th of March, 2017).

All law enforcement respondents (17) that participated in this research agreed that identity theft drives criminal activity. The participants cited different examples of identity theft among cybercriminals. Some participants believed that cybercrime perpetrators rely on identity theft to commit crimes.

“All law enforcement respondents (17) that participated in this research agreed that identity theft drives criminal activity. The participants cited different examples of identity theft among cybercriminals. Some participants believed that cybercrime perpetrators rely on identity theft to commit crimes.

“Some people presented themselves as political figures, a big name in the political circles, or celebrities. They clone the website of such person, or the Facebook, Twitter account. They put the real figure’s picture there. You will think it is the real figure.”

(NSCDC4, Interview conducted on the 8th of March, 2017).

“… (victims) don't know the identity of whom they are dealing with (on the internet). They (cybercriminals) tend to hide their identity while committing the crime. They must have made their way before the person on the other side is aware of it.”

(NSCDC1, Interview conducted on the 8th of March, 2017).

Other practitioners in the criminal justice system also attest to the prominence of identity theft; “running through all of these (crimes) has always been a consistent threat of identity theft.”

(MOJ1, Interview conducted on the 2nd of March, 2017).

Another factor in the discussion of identity theft discussion is the increasing adoption of the identity of the wealthy and elite in society. Using the identity of a Nigerian elite relies on the wish to tarnish their image and dent their reputation. Three convicted criminals identify this approach as an increasing trend and adaptation to cybercrime perpetration.

“We impersonate rich people and government officials in Nigeria. We sometimes use the identity of rich Nigerians to defraud people. It is easy to use because most of them don’t even use the internet.”

(CC6, Interview conducted on the 2nd of March, 2017)

“Using the identity of the rich and powerful people in Nigeria often helps to convince the victims more. It hurts them and often spoils their image. I see some of them granting an interview to say it is a lie. But, we already gain what we want to gain.”

(CC3, Interview conducted on the 2nd of March, 2017)
Five law enforcement respondents affirm the identity theft of Nigerian elites;

*Cybercrime may be targeted at high profile personalities in Nigeria, impersonation, opening fake Facebook or Twitter account in the name of a high-profile personality.*”

(NSCDC3, Interview conducted on the 8th of March, 2017).

Despite the increasing acknowledgement of the use of local identity, all the participants agree that identities of foreigners are still primarily used per perpetrators. One of the Police Officers provide details by stating that;

“They (criminals) use other white women picture or white men’s picture to impersonate it, to make money fraudulently. Some of the people doing some of the internet scam men pretending, impersonating as if they are men using another person’s picture, scam a woman in the UK, in the US.”

(NPF2, Interview conducted on the 2nd of March, 2017)

Identity theft is a core mode of perpetration in cybercrime in Nigeria. It plays an essential role in prevalent crimes. Initially, the identity of foreigners is the most lucrative and highly used. However, the focus is shifting towards the Nigerian elite, with their identity used for different criminogenic purposes.

5.4.3 Romance Fraud (Social media and dating site)

Romance fraud is also prominent among the perpetrators. This crime is a core element of cybercrime in Nigeria. Twenty-three of the participants reflecting every stakeholder group affirm that love-related fraud continues to be prevalent.

“What you call romance scam, pretending to be one person, cultivating, social engineering.”

(MOJ1, Interview conducted on the 2nd of March, 2017)

“Some of them were an inheritance; some were romance. I am in love with you kind of thing. I love you, I need a flight ticket.”

(NSCDC1, Interview conducted on the 8th of March, 2017).

“Popular crimes in the Nigerian cyberspace include romance scam, Yahoo Yahoo, Internet fraud and Email fraud.”

(CC1, Interview conducted on the 2nd of March, 2017)
“We still witness it, and even this photoshop is not even helping. Where, it will manipulate the photo of somebody, so that you are thinking you are talking to another person, you have the feeling maybe you are talking to a lady.”

(NSCDC1, Interview conducted on the 8th of March, 2017).

One area of interest in romance fraud is the focus of the perpetrator. There is a debate on the location of romance fraud victims. Eleven participants maintain that focused victims reside outside of the country. Nine participants referred to the prevalence of local victims. Interestingly, these divergent views remain stronger among law enforcement agents. Two NSCDC respondents for example, provide different opinions in the same command;

“One, the category of victims includes foreigners, non-Nigerians, maybe through a dating site, online contract scam, online job scam and all the rest targeting non-Nigerians. Cybercrime can be targeted at females, especially online dating and likes.”

(NSCDC1, Interview conducted on the 8th of March, 2017).

Another agent stated that;

“If it is dating, online dating, that one is directed at mostly male and female, mostly females in the country (Nigeria). They only target well to do Nigerians and even young people that are often fleeced.”

(NSCDC3, Interview conducted on the 8th of March, 2017).

The convicted criminals also attest to their uttermost focus on foreigners in their perpetuation. One of the identified reasons is foreign exchange.

“Regarding the victim, foreign magas (victims) are preferred to be met on Facebook.”

(CC6, Interview conducted on the 2nd of March, 2017)

Eight participants (including five convicted criminals) conclude that anybody can be a potential victim worldwide. However, the Police and convicted criminals agree on the importance of romance fraud to cybercrime in Nigeria. Deployed services here include Facebook, Badoo, and WhatsApp.

---

60 Trans-Atlantic victim focus is the characteristics of the early cybercrime in Nigeria.
61 Facebook in this context represent other social media platforms such as dating site, Instagram and others
“If somebody sells an idea to you, or let me talk about internet dating, or online dating or Facebook dating. Dating a woman, or dating a man and saying you want to marry and all that. We have people around the world that are victims of stuff like that.”

(NPF1, Interview conducted on the 6th of March 2017)

Finally, the gender orientation of the perpetrator and victim appear to be highly skewed. Cybercrime in Nigeria is patriarchal, with perpetrators mainly being male, while victims are primarily female.

“Although the other crime which I did not mention is there, it is the fake love romantic something. I have seen experiences women are victims of that because they succeeded in duping the women after they are told where I will marry you or I love you,“

(EFCC1, Interview conducted on the 2nd of March, 2017)

Romance Fraud remains a significant crime. It has become a foundation of Cybercrime in Nigeria perpetration with the adoption of numerous platforms such as dedicated dating websites, social media websites and phishing. Despite an argument about the target audience and the location of potential victims, all participants affirm its prominence.

5.4.4 Hacking

As discussed earlier, identity theft is a significant crime within cybercrime in Nigeria. Hacking has now become a complementary crime that seeks access to information details that can be useful for identity theft. Nineteen participants identify hacking as a present and increasingly popular mode of crime in cybercrime in Nigeria. Both law enforcement participants and convicted criminals agree on the prevalence of this crime. A Police participant explains that hacking is used to retrieve individual information for identity theft online;

“Hacking into a system is prevalent in Nigeria. Using other people’s account to send letters and contact and communicate with others.”

(NPF3, Interview conducted on the 28th of March, 2017)

“Before, we always struggle to find hackers. But now, many of them are good at helping us get information.”

(CC3, Interview conducted on the 19th of March 2017)

---

62 See discussion in Section 5.1.
At the EFCC, the two participants agree that hacking is a sign of cybercrime growth. It shows that cybercrime in Nigeria has come of age, thereby demonstrating increased technological skills;

“So after a while, other forms of cybercrime began to emerge within the Nigerian environment. That is when we started having hacking and all other forms of cybercrime.”

(EFCC1, Interview conducted on the 2\textsuperscript{nd} of March, 2017)

Five of the convicted criminals interviewed also agree hacking is one of the professional designations among perpetrators. Hackers are highly respected and often dictate their terms during the crime. It has become a significant area of expertise readily available.

“There is collaboration among various segments. There are professionals in hacking, account hijack and diversion, and credit card stealing and usage. Experts exist among the boys. A code of conduct exists among experts.”

(CC5, Interview conducted on the 19th of March 2017)

Most participants agree as to the prominence of hacking in cybercrime in Nigeria. However, there is an argument about the level of sophistication exhibited by Nigerian hackers. While some believed in the high level of skills in the Nigerian hacking sector, others argue that competency and perpetration are still low.

The most substantial view of the low level of technological competence of Nigerian hackers came from the two EFCC participants. They argue that financial gain dominates the perpetration, and hacking is not necessarily required. The technical expertise needed to become a hacker might be beyond local reach:

“Let me give you an example; it happened if they come to somebody in Alaba market that sells electronics, and they buy stuff. They could buy stuff, nine hundred (thousand), one million from the man. They hack into the alert system of a bank and give him an alert; they say we are at the bank, and we have transferred the money. The man gets the alert and releases the goods to them. He goes to his bank on Monday; there is no money there. To me, it is very childish; it is not mature. That is the kind of hacking we have.”

(EFCC1, Interview conducted on the 2\textsuperscript{nd} of March, 2017)

In support of the EFCC opinion, the Ministry of Justice (MOJ) representative agree that financial motivation drives hacking. However, there is a difference in their belief as to hacking
competency. One participant argues that hacking into the banking system requires significant skill.

“We have people hacking into bank systems, well some government institutions not as much as commercial entities because the trend has also been that the motivation has always been how to get the money out.”

(MOJ1, Interview conducted on the 2nd of March, 2017)

Furthermore, within the NSCDC, all the eight participants agree that hackers in Nigeria are skilful and profoundly proficient.

“The level at which technical knowledge is going. People are even going into hacking as a course. With the availability of the internet, a reduction in the price of data, and civilisation, Nigerians are having the capacity to launch internet or online fraud on a massive scale. There is a gradual increase in their knowledge, their capacity and ability to wreak havoc online.”

(NSCDC3, Interview conducted on the 8th of March 2017)

Despite the different methods of hacking, one approach is deemed central. One way of hacking is through the installation of illegal applications into the computers of victims.

“I can talk of Hacking whereby these criminal elements install illegal applications on people’s personal computer and another digital system. They install it mischievously. The way they do that is another thing. We have hacking; we have cyber theft.”

(NSCDC3, Interview conducted on the 8th of March 2017)

Another aspect of hacking that enjoys support from about 21 participants focuses on more local targets than on foreigners. From the quotation above, the participants are focused on domestic victims. For example;

“Hacking has targeted local victims, both individuals and organisations. It is easier to retrieve and access the victim computers and details in Nigeria.”

(NPF4, Interview conducted on the 28th of March, 2017)

Because local victims are rising, other types of crime are on the rise. One identified crime involved social engineering usage for gaining insider support in a commercial bank.

“A lot of social engineering is involved in this at a local level. In one of the cases, the cleaner was given some money, was it a hundred or a hundred and fifty thousand (about £320). These
guys came in and told him that while you are cleaning, we will work on something, and they inserted the keyloggers, and they left. The bank person did not know.”

(MOJ1, Interview conducted on the 2nd of March, 2017)

From the responses, hacking is a method that is widely used in cybercrime in Nigeria. While hacking was recognised, the degree of competence and ability among the perpetrators remains a matter of dispute. Some participants argue that local victims were focused, which impacted the mode of operation among participants. The findings also confirm the role of insider cooperation in conducting this type of crime.

5.4.5 Cybercrime as a service

Cybercrime in Nigeria also reflects the global phenomenon where cybercrime is service-oriented. Every individual and group have specific skills that can be referenced as a service. There are now experts that professionally render services. Nineteen participants state professionals who exhibit a particular service orientation level, whereas professionals function for a fee.

“At any time, you need service, and you will always get that service from another source. A lone person can start an operation or an attack, and if there is a need to get any tool in furtherance of the attack or advancing the scam. The sources for that information or source for that tool and makes use of it, independent of that person. So, what he does is, he pays for a service and does his work.”

(EFCC2, Interview conducted on the 2nd of March 2017)

“What we have seen is it is loose. They now harvest information. They contact someone else who is savvy at exploiting banking information. Why I said organised is that there is some connection to get who knows how to use it, who is ready to pay for that information, then the ecosystem goes on.”

(MOJ1, Interview conducted on the 2nd of March 2017)

As financial motivation characterises the initial stages of perpetration. The service-oriented approach reflects this process of perpetration. One of the EFCC participants provide details on the distribution of expertise in the criminal process.
“If he (perpetrator) needs a tool that will infect somebody’s system, they do not do the coding. They buy off the shelf from the underground market and use it in the attack. They get their money and then pay for the services he (the vendor) has given.”

(EFCC2, Interview conducted on the 2nd of March 2017)

There are portals for the purchase of cybercrime services used without having any technical skills.

“You see, the truth of the matter is these guys can call up anyone. Nigerians are accessing crime as a service portal. So, you do not need to know how to hack. All you need is to pay someone to hack for you.”

(MOJ1, Interview conducted on the 2nd of March 2017)

These services are procured for insider attacks and other local criminal activities:

“With the way it is going, the early exposure, premature exposure of the youths to the internet. They do not know the ethics of it. Some of them are doing it for fun. They get the tools free online, and they want to try it and see it work.”

(FUT1, Interview conducted on the 21st of March 2017)

Within this service-oriented implementation, there are also collaborations with counterparts in foreign countries. Twenty-two stakeholders pointed to partnerships and the involvement of different perpetrators from foreign countries:

“These crimes involve services of experts in different countries. I can tell you that we investigated a case. The money was laundered from the US to South Africa before reaching Nigeria using different accounts and names of people involved in the crime.”

(NPF1, Interview conducted on the 6th of March 2017)

“Most of the goods bought with stolen credit cards are collected by professionals63 outside of the country. Even money laundering, cyber laundering, there are collaborators there. These collaborators may be established Nigerians abroad. Even some white people, Europeans do collaborate.”

(NSCDC4, Interview conducted on the 8th of March 2017)

---

63 There are experts in the area of goods collection and selling to launder the money.
Services can be of any type and not limited to technical aspects alone. For example, foreigners are involved in translation services or act as a syndicate in their countries.

“Language service (online translation) is used to seek for victims in other non-English speaking countries.”

(CC5, Interview conducted on the 19th of March 2017)

Practitioners know how to contact the different actors and blocks. A unanimous view among Police participants (5) and the NSCDC officers (8) was that perpetrators of these crimes know each other:

“And they seem to know themselves because there was a time we were looking for a hacker, we were looking for him for almost a year. But, when we arrested some at Ila town, they took them from Ila down to here. They were the ones who gave us the real name of who we are looking for.”

(NSCDC4, Interview conducted on the 8th of March 2017)

The familiarity and rapport among the various players meant the skills of cybercriminals could be harnessed to commit crimes. Sixteen participants suggest that perpetrators often come together based on the demands of a crime. Relationships span different cities within Nigeria and outside the country. For example, one of the three researchers stated that:

“There was an incident last year. Here in Minna, they hire some students to go to ATM points where people are trying to enter their pin, and they get their ATM PIN. It is another student that hires them. They will send the PIN to the agent that links them, and he will now send it to the guy that is using it in Port Harcourt.”

(FUT1, Interview conducted on the 21st of March 2017)

Working together on crime often involves a code of ethics that parties must honour. The code is unwritten but guides the conduct of each cybercriminal in honouring service rendering agreements. In a financial reward-based crime, there is an agreed sharing formula in the case of any financial gain:

“They use percentage for sharing the loot, and the percentage can vary.”

(CC4, Interview conducted on the 19th of March 2017)
“When you engage the service of any specialist, you must obey the terms. Failure to obey the terms will make you be tagged among colleagues, and people will not want to work with you again.”

(NPF5, Interview conducted on the 28th of March 2017)

Cybercrime as a service has become a recurrent feature in the present reality of cybercrime in Nigeria. In financially related crime, different services exist. However, the services are not tied to the local perpetrators but have an international dimension. Some unique services include language translation, marketing goods, money transfers, and identity theft have become available. Committing a crime is not limited to skill acquisition but also the ability to assemble experts in a service-reward arrangement.

5.4.6 Attacking Government Infrastructure

Implementing cybercrime through an attack on Government infrastructure is another increasingly prominent mode of perpetration. From experience, various government agencies have noted that:

“All system that is connected to the internet is surely not immune to cybercrime. It is not only INEC, national assembly and other agencies too were attacked.”

(EFCC2, Interview conducted on the 2nd of March, 2017).

Four out of six convicted criminals agree that hackers often target the Government. Hackers directly use Government websites and infrastructure to gain satisfaction and show their anger. Government infrastructure in Nigeria is fast becoming a target of sophisticated cyberattacks.

“Just like you are a programmer, you are trying it; it is working, you are self-motivated by the result you are getting. Some of them may be political. You know in Nigeria, toward election period, there was a time that the website of the electoral body was defaced.”

(FUT2, Interview conducted on the 21st of March, 2017)

Another driver is a direct attack on the financial sector of the country. Twenty-one participants note that the Nigerian financial industry is the most targeted sector in Nigeria. It makes the financial sector a critical area of attack in the opinion of the participants.

“In cases that we have investigated, attacks have been directed at the various financial institutions in Nigeria. They want to gain access for different purposes.”

(NPF2, Interview conducted on the 21st of March, 2017)
One derivative from the financial institution focus is the various factors that have enhanced direct attacks on the financial sector. The Ministry of Justice (MOJ) respondent outlined the multiple vulnerabilities that have encouraged the attacks. These factors include:

“Software vulnerabilities, botnet attacks, and these guys are hitting payday because when we looked at it in 2015-2016, we find that of the 25 banks, that up to 16 or 12 of them are running a particular software while another seven are running the same software.”

(MOJ1, Interview conducted on the 2nd of March, 2017)

The harmonisation of The National Treasury (TSA) has provided a viable opportunity for cyberattacks. The Central Bank of Nigeria’s technological infrastructure has become a target.

“Even the government now is trying to harmonise its treasury, and one thing with cybercrime is that if you are not attacked today, do not think you will not be attacked tomorrow.”

(FUT2, Interview conducted on the 21st of March, 2017)

“Even recently, there was news that some people attempted to hack CBN, Central Bank of Nigeria system last year. Some people attempted, we learnt that they were apprehended.”

(NSCDC4, Interview conducted on the 8th of March 2017)

As noted, Government infrastructure has become attractive to cybercrime in Nigeria. It has become an active part of local victimisation. Evidence from the findings suggests that the financial sector, which is now adopting significant digitisation and electronic service, rendering it now the most focused target. Currently, advances in knowledge and competency is a direct threat to internet-related government infrastructure.

5.4.7 Kidnapping

This sub-theme is mainly from the views of the convicted criminals. It highlights the online-offline criminality of cybercrime in Nigeria. The murder of Cynthia Osokoghu in 2012 highlights the possibility of online-offline crime integration. Five of the convicted criminals attest to using Internet for supporting offline crimes. Kidnapping is a significant offline crime that has thrived with this approach.

64 A young lady was lured to an hotel by friends that she met on Facebook. She was later murdered, and the entire belongings were stolen.
Participants pointed to using online information of individuals could be used to profile and determine their social worth. The investigation of individuals through online activities is used to direct offline criminals to undertake kidnapping.

“We trace victims now more than before. We research victims to know their capability before supplying their information to the boys that do the job.”

(CC2, Interview conducted on the 19th of March 2017)

This collaboration points to increasing localisation of victims of cybercrime. The use of Facebook, location and additional information online are used to track victims as part of this process. Criminals will often analyse the entire background of their potential victims before committing crimes.

“Sometimes, the location on some of the sites help us to locate them and for the boys to track them.”

(CC6, Interview conducted on the 19th of March 2017)

One of the EFCC participants points to this situation as confusing for law enforcement agencies, making it difficult to classify or prosecute. The transformation of traditional crime to online crimes is apparent in the response;

“Most of the traditional crimes are going online. Either started, continued, or concluded online. For instance, you see a kidnapper; if he is to look for his victims, he goes to the Facebook page. People do all kind of things online, and they even put their locations online. You can't see anything been online but information that aided the physical crime. He received it online. so, how do you categorise that?”

(EFCC1, Interview conducted on the 2nd of March, 2017).

In some instances, the internet is used to entice potential victims. There have been cases where victims have been lured from foreign countries and then perpetrate offline crimes. Convicted criminals state that the internet provides the reach to enable them to meet willing victims of physical crimes.

“Sometimes, I have seen cases where people will be invited to somewhere and robbed or kidnapped using services such as Facebook. It is done after they have been checked out and are capable of dropping money.”

(CC5, Interview conducted on the 19th of March 2017)
Kidnapping and all other offline crime are leveraging cybercrime. It is a significant feature of cybercrime and acknowledged by both the convicted criminals and law enforcement agents. The internet has become a useful source of information about and communication with potential victims. Despite this not being cybercrime, it directly reflects the role that crime online can play in the real world. There is now effective integration of cybercrime with offline and contact crime in cybercrime in Nigeria.

### 5.5 Organised Crime

This theme spans through the entire mode of crimes that are present in Nigerian cyberspace. It focuses on the sociocultural aspect of the social networks of cybercriminals. Three areas of interest include the depth of the organisation, membership and involvement, and the network of perpetrators. These three areas reflect different aspects of cybercrime.

The involvement of experts and individuals in different locations necessitates the need to determine the current cybercrime organisation in Nigeria. There are various angles to the nature of the organisation and insight into the hierarchy (or levels) of the crimes. They include professionalism and how cybercrime has evolved and must be explored, and the extent of the organisation among the cybercriminals.

Nineteen (19) participants agreed that cybercrime in Nigeria was not tightly organised. It implies a lack of command and control among the perpetrators. These participants span law enforcement and convicted criminals;

“Mostly in Nigeria, cybercrime is loosely organised. Individuals are the ones going into it. After investigation, you can only find one or two people that are partners in crime, going to it.”

(NSCDC3, Interview conducted on the 8th of March 2017)

“The association is loose among criminals. You learn from someone. It does not mean you must obey the person, but respect must be shown.”

(CC3, Interview conducted on the 19th of March 2017)

“Well, it is loosely organised. When I say loosely organised, they don’t have a cartel per se. So, they are not like a cartel where they sit down and say they belong to this group, and this group carries the attack.”

(EFCC2, Interview conducted on the 2\textsuperscript{nd} of March 2017)
However, five participants that include convicted criminals, an NSCDC official and Police Force believe there is no organisation;

“No grouping of the cybercrime criminals. There are friends or cliques but not a group where rules are used. We exchange information among friends but no standard organisation among criminals.”

(CC2, Interview conducted on the 19th of March 2017)

“They are individuals working on their own. They don’t have a group, and they are individual. They are based in all part of this country. Like Lagos mainly, Oyo state and other parts, and other states in this country.”

(NPF2, Interview conducted on the 16th of March 2017)

Involvement in cybercrime contributes to the loose nature of the organisation within Nigeria. Recruitment often comes in the form of mentorship, especially from acquaintances:

“I was introduced by a friend online. There is mentorship in this sector. I mentored about 20 to 30 boys.”

(CC6, Interview conducted on the 19th of March, 2017)

On the other hand, two participants (one convicted criminal and an EFCC official) suggest a third opinion. The opinion is that cybercrime in Nigeria is well structured with a dedicated chain of command, together with defined roles and responsibility:

“Hierarchy is being introduced among the boys.”

(CC4, Interview conducted on the 19th of March 2017)

“In Advanced Fee Fraud, we have the catcher that goes to and meet the victims; we have the receiver, the one who receives the money. You have the person who maps out the plot. Then you have the real guy there, that is the man, there is the word they used to call him that is the ‘BOSS MAN’. So, to that extent, but concerning being organised as a network.”

(EFCC1, Interview conducted on the 2nd of March 2017)

A few participants (3) believe a dedicated division of labour assembled to perpetrate a cybercrime. The web of individuals and the social network of perpetrators is evident in the organisation.
“The people that are masterminding it, they are well organised. At times, it is only their agent that is caught. You discover that it is difficult to get the main people behind when they are trying to trace. It is only those people they are using that will be arrested. So, to some extent, they are organised.”

(FUT1, Interview conducted on the 21st of March 2017)

Further evidence is the use of social network and connection to suppress the criminal prosecution of perpetrators. Participants argue the failure alteration of the criminal justice system in cybercrime cases is evidence of the organised nature among perpetrators.

“They are organised, that is why they cannot be easily caught. All these people are organised, they know how to go about their business. They do it in the night, they do it in the day, but where they usually gather to do it, nobody knows.”

(FG1, Interview conducted on the 8th of March 2017)

Overall, the dominant view among participants is the loose organisation among the perpetrators. The structure and strict regimental hierarchy are not prominent with an increasing informal relationship among various practitioners within cybercrime in Nigeria.

### 5.6 Recruitment and Capacity Building

The evolution of cybercrime in Nigeria highlighted the different aspects of capacity building and recruitment. As stated in Section 5.4.5, the local service-oriented approach implies that capacity building is fundamental to criminal behaviour. Both recruitment and capacity building enjoy different levels of support. Table 11 shows the distribution of participants for each aspect of this theme.

**Table 11: Recruitment and Capacity Building Participant Distribution**

<table>
<thead>
<tr>
<th>Participants</th>
<th>Contributing Factor</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>EFCC1, 2; MOJ1; NASS2; CC1, 2, 3, 4, 5, 6; NPF2, 3, 4, 5; FUT1, 2, 3; FG1, 3; NSCDC 1, 4; JUD2; FUT2</td>
<td>Cybercafe and Participant Recruitment</td>
<td>23</td>
</tr>
<tr>
<td>FUT2, 3; NSCDC1, 3, 4, 5; CC1, 2, 3, 4, 6; NPF2, 3, 4, 5; JUD1; NASS2; FG3</td>
<td>Capacity Building</td>
<td>18</td>
</tr>
</tbody>
</table>
5.6.1 Cybercafe and Participant Recruitment

From the start of cybercrime in Nigeria, cybercafés played an essential role in recruitment. The relationships and collaborations that occur in cybercafés initiated both social learning and knowledge exchange among perpetrators. One of the participants established the role of cybercafés at the initial stage of the internet:

“Of course, at the earlier stage of internet penetration, we generally have cybercafés, during that period of early penetration, some of these groups are motivated by quick money through the internet.”

(FUT2, Interview conducted on the 2rd of March, 2017)

Twenty-three participants agree on the fundamental role of the cybercafés.

“Cybercafé is important for recruiting and committing the crime from the beginning. It was used for browsing and knowledge exchange.”

(CC5, Interview conducted on the 19th of March, 2017).

“Cybercafé was where cliques and friendships were formed among young people that visit them. They provide a place where people learn and exchange information for the first generation of cybercriminals.”

(JUD2, Interview conducted on the 28th of March, 2017).

Twelve participants, including researchers and law enforcement agents, identify the role of cybercafés. However, they argue that lack of regulation is the primary reason for the impact of cybercafés. The quotations below captures this argument:

“Unregulated and proliferation of cybercafés have aided cybercrime. Cybercafé is everywhere. You see a mushroom upstairs, cybercafé here and there. And people go there overnight to do their jobs.”

(NSCDC4, Interview conducted on the 8th of March, 2017)

“At the earlier stage of internet penetration, we generally have cybercafés. At the advent of these cyber cafes, no bill or laws regulated their operations. At that stage, some of the youths were unguided and were exposed to the negative aspect of cyberspace.”

(FUT2, Interview conducted on the 21st of March, 2017)
Sixteen participants believe that cybercafes fostered a social relationship that solidified the foundation of cybercrime in Nigeria. Its usage in committing cybercrime contributed to increasing knowledge through social ties:

“The café is where boys meet and make friends. Boys learn about the business, and that was where I was introduced to the scam business.”

(CC4, Interview conducted on the 19th of March, 2017)

“The cybercafe initiates the social nature in the cybercrime activities. It is where people develop this culture that has characterised Yahoo Yahoo syndrome. People who work together in the cybercafé become friends, and they learn from each other.”

(NPF3, Interview conducted on the 28th of March, 2017)

However, technological penetration is transforming the role of cybercafés in cybercrime within Nigeria. Because of easy access and set up for cybercrime perpetrators, the use of the cybercafé is being undermined:

“There is a movement from cybercafé to the use of PC individually in recent times. Cybercafé lacks privacy. The use of PC is cheap, and easy internet access makes it(connection) possible.”

(CC6, Interview conducted on the 19th of March, 2017).

“Its use is becoming not popular because people can be peeping or interfering. Using the PC for this crime promotes comfortability and flexibility.”

(CC4, Interview conducted on the 19th of March, 2017).

The decentralisation and perpetuation of crime is the new reality. There is no social gathering associated with a cybercafé as perpetrators are now setting up in their homes.

“The use of PCs and other smaller devices have to make sure criminals can work anywhere without any problem.”

(NPF5, Interview conducted on the 28th of March, 2017).

Social learning now does not rely heavily on cybercafés as individuals have the internet set up in their homes on laptops. The learning remains informal, with the social relationship being a significant feature.

---

65 This trend of thinking support the social learning theory patterns within the Cybercrime in Nigeria context.
“You learn from someone in their house and secret, not at the café as we were doing before now.”

(CC3, Interview conducted on the 19th of March, 2017)

“In some cases, we have seen that these people consult themselves. They (cybercriminals) share knowledge and tools while committing the crimes.”

(JUD2, Interview conducted on the 28th of March, 2017)

5.6.2 Capacity Building

Discussing the organised crime context of cybercrime in Nigeria must focus on its relationship with other industries. Eighteen participants identify that cybercrime in Nigeria relates to the global network for social learning. They highlight the use of social media in conducting knowledge exchange:

“Most of these tools being used for attacks are also free online. And YouTube is there. Any tutorial is available to go and learn how to carry out attacks, hacking and the rest. So as a result, in no distant time, their skill level is also on the increase in perpetrating these crimes.”

(FUT2, Interview conducted on the 21st of March, 2017)

The availability of different materials and resources online has made social learning a fundamental tool in knowledge acquisition and increased competency. The other side of social learning is collaboration and knowledge exchange with perpetrators in other countries. There are different means of social learning. First is the use of a forum for sharing information and tools:

“Nigerians are collaborating with foreigners in committing cybercrime.”

(NSCDC3, Interview conducted on the 8th of March, 2017)

“The use of the online forum for information exchange and communication. The online information exchange has become necessary.”

(CC4, Interview conducted on the 8th of March, 2017)

Second, clients are exchanged between perpetrators, while individuals who are not physically located in Nigeria are taught and recruited to become a criminal:

“Clients (victims) are transferred among perpetrators. Foreigners are indoctrinated (about 4 in the last three years).”
“I can remember, when goods are purchased online, they do have agents (collaborators) which the store will give it to before sending it down here. Sometimes, it may be a woman; the collaborator can be a white, European or American, which they will collaborate to dupe the foreigner. Even in the desert, North Africa, Arab Africans collaborate with Nigerians to defraud the rich man. They are going to be the interpreter because perpetrators cannot speak the language.”

The third perspective is the exchange of knowledge with Nigerians that reside abroad:

“Nigerians who live abroad teach these people more advanced criminal skills.”

5.7 Government Intervention

The intervention of Government is in different areas. These areas attracted different support from the participants. Table 12 provides a summary of the participants for each intervention area.

Table 12: Government Intervention Participant Distribution

<table>
<thead>
<tr>
<th>Participants</th>
<th>Contributing Factor</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSCDC2, 3, 4, 5; NPF1, 2, 4, 5; CC1; EFCC1, 2; FUT 2, 3; FG3; JUD1; NASS1</td>
<td>Surveillance</td>
<td>16</td>
</tr>
<tr>
<td>EFCC1, 2; NSCDC3, 4; NPF1, 3, 4, 5; JUD1, 2; NASS1; FG3; FUT1, 2</td>
<td>Cybercrime Act 2015</td>
<td>14</td>
</tr>
<tr>
<td>EFCC1, 2; NPF1, 2, 3, 4; NSCDC1, 2, 4, 5</td>
<td>International Collaboration of Law Enforcement</td>
<td>10</td>
</tr>
</tbody>
</table>
5.7.1 Surveillance

Surveillance of digital communication in Nigeria is not generally widespread within law enforcement circles. Sixteen of the participants state that the government does not have the infrastructure to monitor the communication of its citizens. They said:

“...from my experience, we have not been trained or told to monitor the communication of anybody. I don’t think we have the technology in the hand of government.”

(NPF2, Interview conducted on the 18th of March, 2017)

“We were trained on ..... surveillance but not told whether there is a machine or office where there is surveillance of communication people’s activity on the web.”

(NSCDC5, Interview conducted on the 8th of March, 2017)

However, the contract for the Israeli firm is highlighted by three participants. They stated that:

“If we have the means to do the surveillance, the government will not employ the foreign company to do it for them.”

(NPF1, Interview conducted on the 6th of March 2017)

On the other hand, participants believe that private companies within Nigeria that provide services can conduct surveillance on behalf of the Government.

“Companies such as MTN and ISPs can track the location of users if the government want to do surveillance.”

(CC1, Interview conducted on the 19th of March 2017).

5.7.2 Cybercrime Act 2015

Primary intervention by the government is the introduction of the Cybercrime Act 2015. Participants acknowledge the Act as being a significant intervention in ensuring that cybercrime in Nigeria would be deterred:

“In response to which the government enacted a cybercrime act.” (EFCC1, Interview conducted on the 2nd of March 2017)

66 The government awarded a contract to an Israeli firm in 2013 to conduct surveillance of the Nigerian cyberspace. The contract was awarded for $40million (about £34million) and was alleged to focus on monitoring computers, networks, and devices of government critics.
Participants analyse the role and the provisions in the Act as crucial in regulating internet usage and the likelihood of committing a crime. One area is the management and control of cybercafes that has been a significant contributor to the growth of these crimes.

“Thanks to the Cybercrime Act. One of the sections stated that all cybercafes operators must register with a certain national computing society of Nigeria.” (NSCDC4, Interview conducted on the 28th of March, 2017).

The overall purpose and organisation of the Act are credited in providing a concise document to combat cybercrime effectively:

“There has been everything put under one umbrella, and we now have in the governing council every relevant agency coming together to fight cybercrime holistically as a nation under the national security adviser.” (EFCC1, Interview conducted on the 2nd of March 2017).

However, some participants complained about the lack of awareness of the best way to use the Act. This was responsible for the poor deployment in prosecuting cybercriminals.

“Those who are going to use the law should be adequately educated and trained on the provision of this law”. (NSCDC3, Interview conducted on the 8th of March, 2017).

“We were not trained on the new Act. Some of us don’t know how to use or interpret some of the sections.” (NPF4, Interview conducted on the 28th of March, 2017).

5.7.3 International Collaboration of Law Enforcement

Law enforcement agencies in Nigeria have a standing relationship with various counterparts and organisations in other countries. For example, the EFCC has an arrangement and partnership with other international agencies:

“We have worked with FBI in the sense that we have done joint investigation resulted in the arrest, prosecution and conviction. We have done cases with the Australian Police, Canadian police service and National Crime Investigation Agency. We have international mass fraud marketing working group comprising six countries. On the continent that is Africa, we have a working relationship with South Africa.”

(EFCC2, Interview conducted on the 2nd of March, 2017)

However, the government has not been part of core international conventions or framework to enhance governance and cybersecurity.
“Nigeria is not a signatory of the Budapest agreement. We have not actively been involved in the various groups at international law enforcement and regulatory framework. Based on my position, I have advised the government, but it has not been taken.”

(MOJ1, Interview conducted on the 2nd of March, 2017)

The relationship with foreign agencies and countries exists at different levels within the Nigerian Police Force:

“If the money is too much, some women fight it out in which they will send the FBI to Nigeria through the Interpol to arrest the perpetrators. Nigeria Police will arrest the internet scam men and get the details of all the men and women he has defrauded. So, the mail will be sent to the FBI over there and the address of the victims while they move to Nigeria.”

(NPF2, Interview conducted on the 18th of March, 2017)

Despite the relationship, it remains at different levels without coordination or harmonisation. It is based on cases and not integrated so that intelligence can be shared to prevent crime. Six participants from both the EFCC and the NPF note that they only handle cases that are forwarded to them:

“We only deal with cases that are referred to us or any complaint from individuals that are victims.”

(EFCC2, Interview conducted on the 2nd of March, 2017).

“Our partners usually inform us if they are looking for a criminal or they need our help to solve a case. We always assist in arresting any culprit of the crime.”

(NPF4, Interview conducted on the 28th of March, 2017)

5.8 Corruption in Judicial System

Corruption is a significant problem in Nigerian society. Corruption contributes to the risk of cybercrime and insider social engineering. Seventeen of the participants affirm that corruption contributes to cybercrime in one way or another. This sub-theme impacts cybercrime in Nigeria in different ways. The findings from the interviews confirmed prior findings, as stated in Section 3.6.
It promotes inequality in society, thereby limiting economic growth and the belief of individuals in the Government. The first context is its impact on the perception of the public. One of the law enforcement agents stated that;

“corruption of the political class is what motivates a lot of people. Because our political class are so corrupt, we hear billions upon billions being stolen every day. And people are there, a worker who is not paid his salary. When you see people there building mansions around, you will want to take to crime to meet up with them.”

(NSCDC4, Interview conducted on the 8th of March, 2017).

One of the convicted criminals added this context;

“We hear Millions of monies stolen without anybody doing anything, and we don’t see anything. I joined the group to make my own money.”

(CC4, Interview conducted on the 19th of March 2017).

Another context is the role corruption plays in law enforcement. Nine of the Police and NSCDC officers are utterly disappointed and angry about the bending of justice in cybercrime cases due to corruption.

“We have corrupt law enforcement agents. Some law enforcement agents are aiding these cybercriminals by collecting money from them. I do not need to mention the organisation, but it happens.”

(NSCDC4, Interview conducted on the 8th of March, 2017)

“Bigmanism (colloquial) is when Nigerian Police arrest an internet fraudster. Someone from Abuja (National Police Headquarters), because he knows that person from the presidency or the Nigerian Police, maybe an AIG (Assistant Inspector-General of Police), DIG (Deputy Inspector-General of Police), the commissioner of Police, Attorney General of the Federation. They will send an order that the suspect should be released. It might be the son of one of the people mentioned.”

(NPF2, Interview conducted on the 20th of March, 2017)

One of the parliamentarians highlights conspiracy among law enforcement to reduce or water down charges as another example of corruption.
“A person that was arrested for cybercrime, the security agents who are going to charge him in court, might decide not to go into cybercrime. It might try to deviate from cybercrime to something else. But when you analyse it, it is still cybercrime.”

(NASS1, Interview conducted on the 22nd of March, 2017)

Two Police Officers explain the two different challenges within the Judiciary. The first is the inadequacy of Nigerian law and the deliberate violation by members of the Judiciary.

“In some cases, it is difficult to interpret the laws because they are far from reality and does not apply to the crime. For example, the cybercrime law is silent on the crime of behaviour, cyberbullying, online child abuse and others.”

(NPF5, Interview conducted on the 28th of March, 2017)

Indeed, one law enforcement agent argues that instructions often come from superiors to stop an investigation and arrest cybercrime suspects.

Nigeria is infamous for graft across the globe. The engagement of law enforcement agencies has been linked to corruption within the rank and file. The depth of the organisation is demonstrated with law enforcement agents assisting in the evasion of prosecution.

“We have corrupt law enforcement agents. Some law enforcement agents are aiding these cybercriminals by collecting money from them. I do not need to mention the organisation, but it happens.”

(NSCDC4, Interview conducted on the 8th of March, 2017)

“Police collaboration and corruption contribute to the growth of cybercrime in Nigeria.”

(CC5, Interview conducted on the 19th of March, 2017)

Seventeen participants argue that corruption or law enforcement collaboration did not reflect the depth and strength of cybercrime in Nigeria. Incompetence in the criminal justice system is responsible for weak prosecutions and not corruption or collaboration with Police personnel.

“I must be sincere with you; we do not have the skill level of these people. We sometimes need the help of other experts, which is difficult as there is no money for that. We need more technical individuals to work well in fighting this cybercrime.”

(NPF4, Interview conducted on the 28th of March, 2017)
“It is not only the police that should be involved. In the real sense of cybercrime, you need specialist training to deal with the crime of child sexual exploitation. It is something that law enforcement has not grasp what is going on.”

(MOJ1, Interview conducted on the 2\textsuperscript{nd} of March, 2017)

Corruption is a significant factor in the financial motivation paradigm of cybercrime in Nigeria. The majority agree to its core impact on the failure of regulation and law enforcement. The identified effects include individual corruption that increases greed, elite corruption that impoverishes the masses, and judicial corruption that skews or influences cybercrime cases. It remains evident that cybercrime has thrived in the country based on different impacts of corruption.

5.9 Findings Discussion

This section seeks to extend knowledge emanating from empirical findings. It situates the new insight of this research within the contextual meanings elaborated in previous literature presented in chapters 2 and 3. Considering that Chapter 2 provided the theoretical background, and Chapter 3 presented cybercrime in the Nigerian context, this section compares the primary data and the literature towards fulfilling the knowledge gap.

It illuminates different aspects of research by identifying new knowledge based on the aggregation of the subjective ideas of participants. The derived themes allow a clear articulation of the connection that the study has with other scholars about cybercrime in Nigeria. The themes and sub-themes enable the elaboration of different areas of the findings.

5.9.1 Technology Penetration and criminal Sociology

Technology is fundamental to the conduct of cybercrime (see: Section 2.8). Internet access is the foundation and means of conducting these crimes. It impacts the structure, functioning and development of criminal sociology. The empirical findings agreed with the documentary analysis concerning the sociology impact. However, there is core new insight derived concerning the different era\textsuperscript{67} of internet access in Nigeria.

5.9.1.1 Cybercafes

The empirical findings agreed with the documentary analysis that internet access through cybercafes was the foundation of cybercrime in Nigeria. These crimes were conducted

\textsuperscript{67} Cybercafe era and GSM era.
through the public internet access provided by the cybercafes in the mid-1990s (see: Section 4.1). Two factors in the prominence of cybercafes in the criminal world were: Firstly, the high cost of connection promoted the dominance of the cafes because they provided the only means of affordable internet access. Also, the economic state of the country (see: Section 1.3.1) made the low cost of internet access through cybercafes remain attractive.

Firstly, technology penetration through cybercafes promoted centralised perpetration of crime. Young Nigerians converge at the various cafes to form social organisations to commit crimes. Secondly, the cybercafe exposes Nigerians to unregulated and uncontrolled Internet access. They were not regulated or monitored by the Government and allowed the unabated growth of multiple crimes (see: Section 4.2 and 5.6.1). It created a suitable environment for the development of criminogenic behaviour. Thus, the validity of the argument that cybercrime in the country developed because of freedom of operation and uncontrolled internet space.

However, empirical research provides new insight into the role of cybercafes. The cafés also contributed to the fraud-oriented foundation of cybercrime in Nigeria. The perpetrators do not own internet service or connecting devices. They have restricted access and cannot deploy advanced programs as most cafes disallow external memory or any other program outside the browser and word processing software. With this control, the only set of crimes that could be perpetrated are cyber-enabled because they do not require advanced technique or technology knowledge, only the malicious use of online services. For example, Yahoo messenger chat rooms were one of the first services to perpetrate AFF by cybercriminals. This finding highlights the impact of technology on the foundational mode of operations by cybercriminals in Nigeria.

5.9.1.2 Mobile Telephony

The introduction of GSM technology with corresponding mobile and broadband connection transformed the overall cybercrime perpetration in Nigeria. The empirical research agreed with previous findings (see: Section 2.4.3) that cafes became less attractive because the cost

---

As explained in Section 2.3.4. They are crimes that can be perpetrated on the web and off the web.

GSM was introduced as part of the telecommunication reform by the Government in 1999. It allowed the public rollout of mobile telecommunication service.
advantage was eliminated. The social impact of GSM introduction on cybercrime in Nigeria was significant because for the majority\textsuperscript{70}, internet connection is now through mobile devices.

Firstly, the entire cybercrime structure and functioning cybercrime has been decentralised and diversified (see: Section 5.6.1). Cybercriminals now have their computer systems and devices set up in their houses and other remote locations to commit crimes. Hence, the social strata and characteristics of cybercrime in Nigeria became more individualistic.

Secondly, GSM increased the amount of internet penetration, thereby making the country a viable market and active player in the global e-commerce ecosystem. Global brands (such as Microsoft, Apple, PayPal, Andela, and Uber) and local services (such as Taxify, Jumia, Konga, FarmCrowdy, and IrokoTv) enriched internet usage in Nigeria. These services allowed Nigerians to explore criminogenic behaviour based on advanced understanding and access to various services and technologies.

The findings reinforce these two social impacts through the provision of examples and subjective meanings from stakeholders. However, two other insights emerged from the empirical findings.

Firstly, the ease of internet connection made cybercrime in Nigeria complex and unpredictable. Both the convicted criminals and law enforcement agents agreed on the continuous evolution of cybercrimes and the high level of sophistication that is being witnessed. Cybercriminals own the device and the internet connection. They can develop sophisticated infrastructures such as a cybercrime laboratory or an incubation centre for cyber-dependent\textsuperscript{71} attacks. Thus, the ease of technology has changed the typology of the crime.

Secondly, cybercrime is going mobile. The cybercrime in the Nigerian landscape is changing towards mobile device deployment based on the improved processing power of mobile devices. Cybercriminals are advancing their enterprise onto mobile platforms through mobile application developments. The use of mobile phones (such as Bluetooth and Wi-Fi) has allowed enhanced criminal perpetration. Even AFF related crimes such as romance scam have been influenced because most social media (WhatsApp, Facebook, Instagram) services can now be accessed on mobile devices. Thus, the entire development of cybercrime is stimulated by the growing mobile internet access.

\textsuperscript{70} According to the 2019 statistics from the Nigerian Communication Commission, about 92\% of Internet connection in the country is on mobile devices.

\textsuperscript{71} Such as website cloning, hacking, DDoS, BEC and spear-phishing.
5.9.2 Concurrency of Cybercrime Motivation

Cybercrime in Nigeria is witnessing a concurrent evolution of motivations. The role of the crimes reflects far reaching changes in the entire conduct. Cybercrime in Nigeria emanated from financial incentives with emphasis on different forms of AFF. The Anajemba case was a significant example of internet use in financial scam (Ibikunke, 2013). The empirical research affirmed that financial motivation continues to drive the activities of cybercriminals. However, new motivations are emerging and have limited, or no, focus from previous scholarly investigations. These motivations reflect changes in different areas that have strengthened cybercrime and made Nigeria become one of the most crucial cybercrime centres in the world. In the Nigerian context, some motivations were identified that had transcended financial gain (see Section 4.3). From the empirical research, three new motivations emerged: creativity, revenge, and altruism.

Firstly, creativity is a motivation that currently stimulates cybercrime in Nigeria. Skilled individuals without productive opportunity are exploring new knowledge and deploying their competency through cybercrimes. Cybercriminals from Nigeria are evolving the social learning concept in expanding their competency to advance the nature and intensity of cybercrime. Also, technology penetration (see: Section 5.9.1) has a significant contribution to the development and control of technology infrastructure for cybercrimes.

Another emerging motivation is revenge, with cybercriminals seeking retribution from local and foreign victims. It emanates from economic frustration, malice, feeling of being cheated, or passion (Armin et al., 2015b; Aston, 2012; Kopecky, 2017; Leukfeldt et al., 2017). Revenge is multidimensional, especially in the attacks against local victims. There are different dimensions, including revenge pornography, employee revenge against employers, revenge against politicians and political systems and revenge against Government. It is one of the most dangerous new motivations for cybercrime in Nigeria.

Thirdly, new set of cybercriminals, stimulated by altruism, are emerging from Nigeria. Altruism is not a concept that has previously been identified in the cybercrime in Nigeria...
context. The focus is to perpetuate these crimes for social good\textsuperscript{78} so that victims are punished for their erstwhile conduct\textsuperscript{79}. For example, AFF is a means for social mobility with proceeds used in catering for family and other poor needs. It reduces the sense of guilt felt by cybercriminals, thereby extending the theoretical contribution\textsuperscript{80} of the findings.

5.9.3 Cybercrime Evolution

The findings demonstrated that cybercrime in Nigeria could be placed into three phases in terms of crime typology. The first phase was the era where the foundation of cybercrime was instituted. It is fraud-oriented with dependence on cybercafes\textsuperscript{81} and limited internet connectivity. The second phase of cybercrime in Nigeria includes the emergence of multi-skilled crimes, the Yahoo Yahoo sub-culture development, enhancement of local victims, increased cultural acceptance, and technology-dependent crime reinforcement. The era is synonymous with the prominence of the GSM technology,\textsuperscript{82} where criminal behaviour became diversified.

Nigeria is now arriving at the third phase of its cybercrime evolution. This era is characterised by a high level of potency and through sophisticated skilled practitioners. This phase is current but continues to emerge with changes in motivation, typology of crime, and cybercrime arrangement. It reflects the advancement and complexity of the social dynamics of the crimes. Two core social changes include organised crime characteristics and professionalism among cybercriminals. Also, the geographical distribution of perpetration is advanced with increasing evidence of crime exportation. Lastly, the typology of crime has become highly transformed into the realm of behavioural crimes.

5.9.4 Regulation of Cybercrime

The documentary analysis established three core regulation practices to include cyber-surveillance and increasing law enforcement on perpetrators\textsuperscript{83}. The core reference point for regulation is fraud and financially induced crime. The enactment of the EFCC Act, Cybercrime Act 2015, and cybercrime strategy emphasises financial crime. Through the

\textsuperscript{78} Similar to the prominent idea postulated by Robinhood and Aaron Swartz in the technology context.
\textsuperscript{79} This is elaborated in Section 5.2.4
\textsuperscript{80} The theoretical implication of this research will emphasise the theory of neutralisation in Section 6.5
\textsuperscript{81} It is explained in Section 5.9.1.1
\textsuperscript{82} As explained in Section 5.9.1.2
\textsuperscript{83} As explained in Section 3.5
Nigerian Police Force (NPF) and NSCDC, law enforcement forms part of the local crime prevention strategy.

Every aspect of the regulation struggles to be effective. Some of the factors that have affected law enforcement include underreporting, jurisdictional difficulties, incompatible laws, and corruption within the system. Law enforcement continues to struggle as the crimes continue to emerge with changes in motivations and operation modes.

Another challenge is capacity within the various areas of regulation. There is a lack of expertise necessary to prevent, detect and investigate cybercrimes. It emanates from inadequate training within the judicial system. Also, the limited availability of equipment, devices and technological infrastructure limits the effectiveness of the regulation.

Also, the current case-by-case nature of international collaboration by law enforcement agencies is another challenge. Despite the existing relationship with foreign counterparts by various Nigerian law enforcement arms\textsuperscript{84}, this emphasis on case orientation only works in the investigation rather than prevention. The case referral approach implies a reactive collaborative approach rather than a preventative approach.

Lastly, corruption in the overall regulatory structure is a drawback within the cybercrime in the Nigerian context. Its permeation into the Nigerian criminal justice system remains a significant challenge in Government intervention and regulation of cybercrime (Enweremadu, 2019; Salihu & Gholami, 2018). Under the guise of cybercriminal profiling and suspect investigation, the police continue to extort and harass innocent Nigerians (Ekhomu, 2018; Odunsi, 2018). The Judiciary is accused of stalling or delivering wrong judgements to perpetrators (Ezeamalu, 2016; Salihu & Gholami, 2018). The banking industry required for financial evidence has been corrupted, reducing the weight of cases (Idowu, 2016). Cybercriminals financially induce judicial workers including Judges, resulting in favourable judgements.

However, the conviction of the cybercriminals that were interviewed in this research could not be overturned despite the acclaimed corruption. If corruption were so deep, these criminals should be above the law and not in jail. It implies that corruption might be present, but the criminal justice system still functions and not every law enforcement official is corrupt.

\textsuperscript{84} It was evident in the Henry Omoko Case (ABC News, 2014) in which collaboration between EFCC, South African Police and Australian Police resulted in the arrest of the culprit.
From this empirical research, there are new insights concerning the low impact of Nigerian regulation. Firstly, the decentralisation of perpetration is a significant challenge for regulation. Cybercriminals from Nigeria are operating from different countries and locations within the country. Law enforcement struggles to conduct effective investigation and detection due to the geographical complexity of the crimes.

Secondly, law enforcement is part of organised cybercrime in Nigeria. This empirical work established that senior members of different law enforcement agencies are interfering with the prosecution of cybercrime cases. It is an extension of the corruption features where a mutual agreement and relationship exists to shield and protect the overall cybercriminal process.

Thirdly, rural-urban migration has affected law enforcement. It emerged that investigation into migrant communities becomes challenging as they relocate to their rural areas. With logistics and finance struggles, achieving the thorough and effective tracing of criminals becomes difficult. The well-known porous borders between Nigeria and adjoining countries further allow effective migration abroad of cybercriminals resulting in significant regulatory challenges.

85 It is generally believed within the Nigerian society as part of the corruption in the Judicial system (Section 3.6) that cybercrime is aided by top law enforcement agencies who ensured that cybercriminals are not prosecuted.
Chapter 6: Theoretical Implications of Findings

Findings from both documentary analysis and the empirical findings have implications for criminological theories. The findings provided new insights concerning the theories. The implications highlight the variation and adaptation of these theories. The findings reinforced the assertion that cybercrime cannot be explored using a single criminology theory (See Section 2.5). Thus, the analysis of the contextual implications on the five criminology theories considered in this research.

6.1 Routine Activity Theory (RAT)

There are three fundamental implications for RAT within the cybercrime context. Firstly, there will always be perpetrators and potential victims. The internet connection of devices, businesses, governments, and individuals in a way that criminal behaviour cannot be averted. Cybercrime will not go away so far there is internet connection\(^{86}\). Also, every entity on the internet is a potential victim. For example, the prominence of the Internet of Things (IoT)\(^{87}\) implies that devices connected are now viable victims for cybercriminals. Hence, RAT is applicable in terms of these two components of criminal victimology.

Secondly, no Government, product or agency is entirely capable of protecting itself and other entities on the internet. The heterogeneity, complexity and pervasive nature of the internet make the risk of criminal enterprise concurrent without protection. Also, the cost of security (including investigation\(^{88}\)) and lack of central control of the internet contributes to the guidance challenges. Both cybercriminals and potential victims meet on the internet with limited or no supervision. Thus, the entire application of the theory will always remain valid for cybercrime.

Thirdly, cyber vulnerability of internet users is global. As established, regulation has failed in Nigeria as the strategy is not having the expected impact on the perpetuation and vulnerability of the crimes. Regulation challenges are not limited to a country with evidence of cybercrime in countries such as Germany, United Kingdom, United States of America, Australia and Canada. RAT is a fundamental criminological theory to understand cybercrime victimisation.

\(^{86}\) As discussed in chapter 2 where the vulnerabilities and continues use of internet will always provide opportunity for crimes.

\(^{87}\) Internet of Things (IoT) refers to devices that are connected to the internet around the world. The collect and share data over the internet.

\(^{88}\) Law enforcement often ignore petty internet crime because of the cost of investigation (Section 3.5 and 3.6)
6.2 Strain Theory (ST)

The first implication is the validity of the foundation of this theory. The evolution of cybercrime in Nigeria established that strain necessitated cybercrime. Financial motivation as the foundation of cybercrime in the country results from the negative interpretation of stressors from failure to achieve goals and desire. The findings agree with Booth & Anthony (2015) and Polizzi (2015) that delinquency results from stressors.

Despite cybercrime not in existence during the formation and development of this theory, the core basis remains relevant. An average Nigerian youth is economically disadvantaged. Various economic problems\(^\text{89}\) existing in Nigeria, as a third world country lowers the opportunity for young people\(^\text{90}\). The relevance of ST is not by accident for cybercrime in Nigeria because it reflects the challenges faced by its citizens. Thus, the focus on financial gain towards improving their (cybercriminals) challenging standard of living.

Despite the relevance of ST\(^\text{91}\), the plurality of the cybercriminals meant the experience of cybercriminal is not the same. Firstly, the interpretation is individual and can either be positive or negative. For example, unemployment in Nigeria often gives individuals the choice of either bad or good interpretation. While most cybercriminals in Nigeria are stimulated by financial gain, a significant number of participants did not experience those stressors\(^\text{92}\). Motivations such as creativity, revenge and altruism invalidate the ST among some participants. An example is a group named #anonymous\(^\text{93}\) whose activities have not been associated with financial gain or intention to fulfil lack of opportunities.

Secondly, the findings in this research demonstrate that stressors are unique to society. No singular factor is universal because of different distinctive experiences in each country. Even when the stressors are similar, the intensity and dimension differ with varying impact on criminological behaviour. For example, the experience of poverty in Nigeria as a developing country differs from other developed countries. The difference in the effects of stressors results in different cybercrime perpetration from the country.

---

89 These problems include underemployment, unemployment, rising cost of living, poor standard of living, and poverty.
90 As expressed in Section 1.3.1, 2.5.2 and 3.1.4 and 5.2.1
91 It is evident in the documentary and empirical findings.
92 Some are not affected by their inability to achieve their goals. It emerged from the empirical research that some cybercriminals are from a good family background without any financial hardship. Also, some convicted Nigerian cybercriminals in the UK are family sponsored and former students.
93 A hacking group that operates on the internet.
The context of Nigerian society and its environment influence the experienced stressors. Some of them include poverty, Government corruption, loss of job, underemployment, the inability of parents to cater for their needs and the need for survival. While cybercrime in Nigeria evolved from financial gains in response to their stressors, the interpretation of other countries is different. For example, the reaction from Eastern European countries to similar stressors is more pronounced in sophisticated and coordinated cyber-attacks. The environment directly influences the kind of impact that strain will have on potential perpetration.

Also, the impact of rural-urban migration on cybercrime in Nigeria is another reflection of the environmental impact. The core crimes from the migrants are financially oriented and reflected the Get Rich Quick Syndrome (GQRS) that is rampant within society. However, China is experiencing more rural-urban migration but have engaged in cyber-dependent crime rather than financially-motivated crime. From the findings, the migrant community often comes with an increased risk of cybercriminal activities.

### 6.3 Social Learning Theory

Findings from this research provide an insight elaborating the suitability and relevance within the cybercrime context. When Akers (1977) proposed SLT as a viable means of understanding and explaining delinquent behaviour, there are specific nuances of cybercrime that were not considered. The internet provides the domain where the crime is perpetrated. Thus, the cybercrime context directly reflects different interpretations and application of SLT.

One fundamental agreement from both documentary analysis and empirical findings is that criminal behaviour on the internet can be socially developed. The foundation of the theory remains relevant among cybercriminals. In agreement with Fox et al. (2011), some groups influence behavioural and cognitive development of some individuals. Cybercrime in Nigeria demonstrates the social process of learning and knowledge acquisition.

The informal process of recruitment, inducting, and training of cybercriminals in Nigeria emphasise the relevance of SLT. The formation of communities and groups shows the

---

94 These are factors that is experienced as a strain before engaging in criminal behaviour.
95 See section 1.3.1 and 6.2
96 The prominent phenomenon in the society where people are encouraged to seek financial affluence irrespective of engaging in criminality.
97 In 2019, 145 million alone migrated from rural to urban centres in China (Hu, 2012)
98 Rural unemployment is responsible for the migration in China as stated by Lyu et al. (2019)
99 Explained in Section 2.3.4
relationship between an individual and the environment. The process of becoming active cybercriminal agrees with foremost proponents of SLT. For example, Jensen and Brownfield (1986) state that individuals will imitate a behaviour after being closely exposed to it for some time.

On the other hand, SLT in cybercrime should be discussed within the multidimensional nature of the process. Some established nuances have further introduced the uniqueness of technology in the discussion. Firstly, peers must not be in close physical proximity or contact to learn or become indoctrinated in their crimes. The presence of various social platforms and groups online for learning made peers span multiple geographical boundaries\(^{100}\). For example, Nigerians residing outside of the country continue to relate with those within the country, resulting in extensive skill acquisition\(^{101}\). Technology has made the entire world a global village with multiple ways of learning.

Secondly, learning can be individual and does not need any peer pressure or groups because the resources are readily accessible. The distributed nature of the web and the vast amount of learning materials imply that learning can be individual. The internet has become a social environment for learning towards becoming a cybercriminal.

This research provides another insight concerning the impact of formal training on technological knowledge. Services such as Andela and other computer institutes (such as Aptech, HIIT and NIIT)\(^{102}\) provide formal avenues to develop technical skills. The acquired knowledge becomes a source of informal education for those within their social group or who could not afford the training. Cybercrime in Nigeria is also highly prevalent in Universities and other higher education institutions (HEIs), suggesting the deployment of formal knowledge in these crimes. Thus, the discussion of SLT within the cybercrime implementation should acknowledge the role of formal education in the expansion of informal learning.

Furthermore, the application of SLT in the cybercrime context is subjective to technology penetration. The nature of technology access influences the social paradigm behind its usage. In Nigeria, the advent of cybercafés created the foundation and oiled the overall process of

---

\(^{100}\) Within cybercrime in Nigerian, those that have travelled continually exchange knowledge and information with colleagues in the country. This exchange is key and ensure increasing skills among cybercriminals.

\(^{101}\) Law enforcement agents that participated in this research established that local perpetrators often learn from their counterparts outside the country. The convicted participants established that online forums are used for this type of learning.

\(^{102}\) The increased formal technology institutes and incubation centres is fundamental within the technology penetration and increased competency in Nigeria.
development. Collective learning and sharing of information are rampant among cybercriminals as individuals continue to develop their skills. However, the growth of broadband and mobile internet access has individualised internet access, thereby transforming the social learning process. Learning has become individualised and based on interpersonal relations rather than technology-induced social relationships that initiated the industry.

One area in which this theory cannot be relevant is state sponsored cybercrime. It is a knowledge gap area whose approach to the learning process is not informal but regimented and focused-based. It might be classified as formal, but the secrecy of such programmes meant that the intricacy within the criminological discussion could not be effectively determined. The cognitive development of cybercriminals might involve scientific methods and complex to explain using only a sociological insight emphasised by this theory.

6.4 Rational Choice Theory

The findings from this research provide insight into the application of RCT to cybercrime. Firstly, every choice of an individual to be part of cybercrime reflects the socio-cultural and economic realities of society. As discussed in Strain Theory (Section 6.2), the unique nature of each society impact costs, thereby affecting the perception of potential cybercriminals. Clarke and Cornish (1985) explained that delinquent behaviour relies on rational decision-making, where both benefits and costs are weighted. In a society where corruption and deterrence are weak, the cost is highly diluted, thereby making the benefits stronger. Thus, the position of society in terms of justice directly affects the application of RCT to cybercrime.

Secondly, deterrence is not usually commensurate with the impact of cybercrime on victims. Offenders were deemed to engage in delinquent behaviour intentionally based on the awareness of rewards and costs. The consequence of cybercrime perpetration has usually been questionable and a source of criticism in Nigeria. Despite the enactment of the Cybercrime Law 2015, its use for criminal prosecution has been limited.

103 The empirical findings established that recruitment and involvement in the industry are based on personal interaction with peers, environment, and family members.
104 Some countries continue to run a dedicated cyber programme to attack other countries (see Section 2.6.4 for details)
105 The findings from the empirical research showed that corruption in the justice system is rampant. The deterrence for committing the crimes is poor thereby affecting the views of perpetrators.
106 One of the police participants established that nepotism and corruption influence numerous cybercrime cases thereby resulting in non-conviction.
107 As at the time of concluding this research. It might have changed ever since.
Furthermore, the lack of technical competency and ability within the criminal justice system directly affects the consequences of the crimes. The empirical research established that low skill exists among law enforcement agencies and the judiciary. It can affect the entire criminal justice process in terms of efficiency. Convicted criminals were confident that cybercrime could not be stopped based on the limited deterrence and evidence of growth beyond the capacity of regulation and law enforcement.

Even in a society where the judicial system seeks punitive measure for cybercrimes, the punishment remains short of what the victims expected. In the situation where conviction is secured, proceeds of the crime were not retrieved, thereby reducing deterrence. Unlike what is obtainable in the United Kingdom through the Proceeds of Crime Act 2002 enables civil recovery and confiscation of proceeds from crime, the Nigerian version has not been effective. Convictions often result in negligible consequence, thereby enhancing recidivism among cybercriminals. Overall, RCT becomes applicable, considering that global deterrence does not reflect the weight of impact or sufficient severity to deter cybercriminals.

Thirdly, the influence of cybercriminals further affects the application of this theory. The economic power and influence of cybercrime proceeds to perpetrators makes the rational choice logical. Arrests do not usually result in conviction. Also, the borderless nature and the remote perpetuation of the crime provides significant geographical advantage that makes prosecution challenging. Also, the absence of a globally acceptable regulation and law often gives rise to crime perpetration. The weakness of organisations like Interpol reduces the perception of deterrence among cybercriminals. Thus, RCT relevance becomes enhanced by the difficulty in the prosecution of cybercriminals.

6.5 Technique of Neutralisation

Two fundamental insights provides a further extension of the application of the technique of neutralisation to cybercrime. The Nigerian case study provided another dimension to the concept of neutralisation. The first area is the influence of social acceptance in attaching legitimacy to action by cybercriminals. As discussed in Section 6.2, the socio-cultural and economic realities of Nigeria affect the entire perception of criminological behaviour. The affluence and wealth demonstrated by cybercriminals, coupled with dire economic situation,

---

108 This was evident among scholar and agrees with the findings by Button et al. (2015)
109 As a result of law enforcement agents been financially induced to doctor the entire case.
have stimulated society’s acceptance. This acceptance has given rise to altruism motivation\textsuperscript{110} among cybercriminals. The use of crime proceeds or criminal conduct\textsuperscript{111} for the common good receive general acceptance, therefore affording perpetrators to erase the sense of guilt.

The second implication is the role subculture plays in the viability of this technique. The Yahoo-Yahoo subculture\textsuperscript{112} normalises the act and behaviour of cybercriminals in Nigeria. Perpetrators have formed a loosely coordinated peer group that supports the demonstration of excessive wealth and creating a class of affluent young Nigerians. Membership of this subculture continues to gain acceptance among the public, thereby reinforcing the sense of innocence among cybercriminals. Thus, the theory of neutralisation has been affected by the overall social organisation of cybercriminals.

\textsuperscript{110} Cybercriminals have engaged in philanthropy towards neutralising their sense of guilt.
\textsuperscript{111} Some cybercriminals use their skills for personal belief of retribution, revenge or common good (see Section 5.3)
\textsuperscript{112} It is an extracted social organisation of young cybercriminals that have dedicated codes and socialise in a pre-defined manner. (see Section 3.1.1)
Chapter 7: Conclusion

This research has broadened the body of knowledge of cybercrime by investigating the factors that characterise its recent development. In particular, it looked at the recent impact of factors such as the economy, culture, regulation and demographics. These factors have rarely been adequately explored in previous research. This research is also one of the few studies that combine the different perspectives of cybercrime (e.g. law enforcement, Judiciary, academic research and legislature) to understand its motivation, mode of operation and emerging trends.

This research used Nigeria as an exemplar for examining how cybercrime is currently developing (Chapter 1.3). Many of the findings can be applied to other countries. Firstly, this chapter explains the five core contributions of this study to cybercrime research. This is followed by discussing emerging cybercrime trends and recommendations for future regulation and control of cybercrime. The following section considers the implications for criminological theories within the context of cybercrime. Finally, a section reflects on the limitations of this research, followed by recommendations for future research and concluding thoughts.

7.1 Research Contribution

This study makes important new contributions to the knowledge of cybercrime. Most previous research was conducted involving only one stakeholder group. This research uses findings from hard-to-reach sources in Nigeria, such as convicted criminals, topmost levels of the Judiciary, and cybersecurity management. Involving cybercriminals in this research provided more insight into the evolution of the crimes from an insider point of view. This research also looked at the entire cybercrime landscape - in contrast to most previous research that tended to look at individual types of cybercrime only.

In Chapter 1, three objectives were introduced in achieving the three key research aims: to investigate i) changing motivations; ii) modes of operations; and iii) emerging trends of cybercrime, using Nigeria as a case study. This section discusses how this research has contributed to the changing motivation and mode of operations.

Firstly, this research provided more insight into the changes recorded in the area of motivation. Findings and analysis discovered new motivations among cybercriminals: e.g. creativity, altruism, revenge, and national politics. These had developed from the original motivation for financial gain. The findings also included a reduced impact on cybercriminals of factors highlighted in Section 1.3: poor economic condition, high inequality, and failure of basic
industries. These new motivations for cybercriminals are likely to be also found in countries such as Mexico, India, Cameroon, Poland, Ukraine, and Belarus, which have similar characteristics to Nigeria.

Secondly, the research findings highlighted that the modus operandi of cybercrime is becoming much less predictable. The changes in motivation, together with the failure of government response, have increased the boldness of cybercriminals, who are confident of having more technical competence than the regulators. Internet characteristics such as its borderless nature, anonymity and remote access further enhance their sense of invisibility. The boldness and high technology penetration imply that any individual, often working within a group, can produce any type of cybercrime. It becomes difficult to predict the source, nature, and type of cybercrimes.

Thirdly, the study further provided an insight into the nature of organisation. The organisation of cybercrime is decentralised as an "organised disorganised" crime without any control. Anybody can participate in cybercriminal activities by setting up without any assistance, supervision, limitation, or association to any group. There is no rigid code of conduct and structured organisation for cybercriminals. Cybercrime has become a globalised criminal activity with interconnected cells and branches worldwide whose organisation cannot be predicted.

Fourthly, this research provided an insight into the role that migration plays in the mode of operations adopted by cybercriminals. It was discovered that rural-urban migration contributes to the complexity and number of cybercriminals in developing countries. The economic condition in rural settlement is forcing the migration of young people to urban areas. Because their skills do not match what is required in urban centres, they become unemployable. Cybercrime is now used to replace legitimate employment by these migrants. Most migrants use cybercrime to improve their economic condition, tackle inequality, and experience social mobility. This finding can be replicated in countries with high rural-urban migration and high cybercrime levels, such as China, Mexico, Russia, and Brazil. These countries have urban ghettos that accommodate criminals. These settlements are sources of complex technology-dependent crimes with unpredictable nature, characteristics, and intensity.

Lastly, this research provided policy implications for different countries from the regulatory point of view. It improved the understanding of the performance recorded by the current regulation in the area of cybercrime. The findings and analysis showed that using the
technological approach has failed to mitigate or prevent crimes (further explained in Section 7.3.2). Leading countries such as the USA and the U.K. have regulations, personnel, and technology to monitor and control cybercrime. There are also countries such as Saudi Arabia, North Korea, and China, which have very high censorship of internet use. However, neither model of regulation has shielded such countries from cybercrime attacks. The sole reliance on technology is not sufficient for regulating crimes on the internet. Because the implication is not limited to developing countries, every entity on the internet, irrespective of their country, is exposed to the risk of multi-dimensional, organised, and highly technical cybercrime.

7.2 Emerging Trends

The findings from this research have broader implications that are reflected in emerging trends. This research discovered different dimensions of growth in cybercrime conduct. The changes in motivation and mode of operation have implications on the social, economy and organisation of cybercrime. The implications will characterise the future conduct of these crimes. There are four specific emerging trends:

Firstly, cybercrime in some developing countries can dominate the world. This research highlighted the potency of developing countries. These countries (including Nigeria but also countries such as Poland, Romania, Russia, and Argentina) have high technology penetration and competence with limited regulation. They have become viable sources of highly complex tools, techniques, and criminal services. On the other hand, regulation in advanced countries has affected the activities of cybercriminals. The activities of regulators continue to challenge cybercrime growth in countries like the US, Canada, the U.K. and Australia (see: Section 1.3, 3.5.1). These countries are becoming less attractive because of the increase in law enforcement and prosecution. For example, Pirate Bay (a file-sharing website) was shut down by the Swedish Police, preventing illegal movie distribution.

Secondly, the relationship between cybercriminals from different countries is stimulating the development of a transnational economy. For example, there is an established relationship between Russian and Brazilian cybercriminals that has resulted in sophisticated attacks. These cybercriminals communicate and exchange tools, methods, information, and proceeds of crime on platforms such as the Deep web and the Dark web. Communication has created a cybercrime ecosystem that spans different countries. Participants in this transnational economy are not limited to developing countries but involve residents of developed countries. Every country has become part of a structured and coordinated cybercrime industry. The degree of potency
will depend on the effect of cybersecurity and regulation. Cybercrime in countries with weak regulation will continue to grow towards domination, while those in countries with strong cybersecurity will struggle. This relationship will continually shape the future of cybercrime worldwide.

One implication of this emerging trend is the professionalisation of cybercrime. The transnational economy is fuelled by the exchange of values among various cybercriminals. Individuals render services to willing clients without any control. These services are not strictly technical, but others that are complementary to the crimes. Example of services includes hacking, malware and botnet development, money laundering, language, and logistics management. The prominence of professionalism has resulted in the cybercrime-as-a-service model.

Thirdly, cybercrime-as-a-service implies that individuals acquire professionals and off-the-shelf tools without advanced technical knowledge. The model has created a cybercrime market with different specialised segments. When a specific resource is required, the cybercriminals are aware of the country or group to consult. The abundance of technical knowledge and limited positive opportunity make countries like China, Poland, Belarus, and others become a hub of technical professionals for hire. Individuals are paying for tools that will be deployed for criminal purposes. Also, there is a potential for criminals to engage professionals that will implement technically complex crimes (e.g. hacking, website defacement, SQL injection, and website defacement).

The implication is that an individual, business or government can coordinate a multinational cyber army with specialised skills to launch a cyberattack. Interested investors can adapt the available skills and tools for desired crime. These crimes will take a corporate venture, where investors with limited cyber capability become significant players. The head (team leader or boss) of a cybercrime syndicate recruits others for a specific criminal operation. Overall, cybercrimes can become a project in which a temporary multinational team is formed and coordinated remotely.

Lastly, cybercrime is becoming accepted as a way of life in some countries. The benefits derived from the crime and inherent national problems (See Section 1.3) have made society normalise the conduct. For example, Eastern European countries are witnessing general acceptance of cybercrime due to poor economic conditions and rising resistance to constituted government.
Countries like Mexico, Colombia, the U.K., and China are struggling with the increasing normalisation of online abuse of different kinds.

Another dimension of this trend is the legitimisation of these crimes through the increasing support of governments for cyberwarfare. Taking part in cyberwarfare is seen as a patriotic endeavour and not perceived to be criminal. Members of the Chinese cyber hacker army, U.S. Army Cyber Command, Israel Defence Forces (IDF) Cyber Defence Unit, and Russian GRU are engaged in attacks without any sense of guilt. Members of civil society justify and support criminal activities perceived to be in the national interest.

The implication is that different types of cybercrime will increasingly become acceptable and legitimate in the eyes of the public. Even crimes such as AFF might be seen as a way of enriching the country, thereby feeding into the economic aspect of cyberwarfare. Authorisation and permission from state agents to conduct these crimes will continue to grow and eliminate any guilt. The crimes will be embraced and continually become attractive in a way that will be uncontrollable.

7.3 Recommendations

These matters are essential for both policymakers and researchers in understanding cybercrime and developing an effective cybersecurity policy. Two recommendations emerged from these findings.

7.3.1 Integration of regulation worldwide

Cybersecurity regulation around the world is not uniform. While some countries have high cybersecurity implementation and technology infrastructure, the experience in other countries is weak and inefficient. Most countries have domestic problems that are pressing and taking focus away from cybercrime. These different worries meant that the interest of the various governments is not uniform nor the same worldwide.

Considering that cybercrime is a global problem, the absence of a uniform global strategy, organisation and agreement is a significant flaw in regulation. While cybercriminals are creating a global industry, there is no standard provision for intelligence sharing, risk analysis, or criminal databases. Countries are engaged in bilateral agreements and relationship in the area of cybersecurity. It is usually conducted for joint investigations of cybercrime cases. The approach is reactive and does not promote the prevention of crimes.
Considering the scale and impact of cybercrime, a risk-based approach should be a strategic requirement to prevent cybercrime. As discussed in 3.5.1, the political interference of INTERPOL and lack of required collaboration has eroded the effectiveness of its cybercrime effort. Also, the voluntary nature of the Budapest Treaty and its failure to acknowledge other vital stakeholders remain a significant weakness. Thus, a new global framework that incorporates all law enforcement agencies, private companies and other stakeholders should emerge. The framework below is suggested as a result of the findings from this research.

**Global Cybercrime Regulation Body**

- **Continental Cybercrime Regulation Body**
- **Specialist Organisation**
- **National Law Enforcement**
- **National Judiciary**
- **Private Organisations**
- **Researchers**

![Figure 6: Proposed Framework for Global Regulation](image)

As presented in Figure 1, a three-layered approach will be suitable for integrating the entire global regulation. In this framework, a dedicated body should be instituted where countries can become members. Every member state should agree to the general standards and principle of this body. It will allow information exchange and borderless analysis of trends that can be effective for cybercrime prevention. For better oversight, every continent will have dedicated branches that directly interact with the law enforcement and Judiciary of each constituent country.

Also, the specialist organisation directly interacts with private organisations and researchers. The role of this organisation is to provide more insight and enrich knowledge concerning emerging trends and new risks. They will inform the global organisation about new threats and ways of enhancing national security. This framework incorporates digital analysis and financial intelligence in a global framework, enabling real-time exchange of ideas and information.
7.3.2 Sociotechnical Approach to Regulation

Cybercrime is not primarily technological. It is a tool that humans deploy to achieve criminal intentions and purposes. The crimes are driven by social, cultural, and economic intentions (see: Section 2.6). To some extent, cyberwarfare can be regarded as national duty in which individuals involved see it as part of their social responsibility. Approaching this crime from only the technological aspect contributes to failure in understanding and regulation.

Governments worldwide have adopted the dual approach of using technology or law enforcement approach to combat cybercrime. However, this research shows that such an approach continues to be less effective. Technological and criminal justice intervention is mostly reactionary after the crime has been perpetrated. The risk element of the crimes has not been reduced with every entity on the Internet exposed to the threat.

The research shows that social intervention should be part of the regulatory process. Social components will ensure an inclusive and efficient means of preventing cybercrimes. Social intervention in terms of social services, family support or educational support for young people can become highly impactful in preventing the perpetration of the crime. For example, strain elements are one of the major causes of the economic motivation of this crime. Thus, a social intervention program that will directly target the influencing strains can curtail the growth of financial crimes such as AFF.

Social intervention is imperative and provides an avenue to limit factors that influence cybercriminals. Countries should focus on different factors that stimulate delinquent behaviour on the internet. The sociocultural elements that can lead individuals into crime can be controlled towards achieving positive behaviour. Governments should ensure economic development and provide better opportunities that will stimulate the positive use of skills.

7.4 Theoretical Implication of Findings

Current criminology theories are individually inadequate for exploring the topic of cybercrime. Three main aspects characterise this inadequacy:

Firstly, the characteristics of each theory do not fully align with the nature of cybercrimes. The theories were developed long before cybercrime existed and did not allow for its unique characteristics: e.g. irrelevance of distance, rapidity of perpetration, virtualisation of transaction, variation in motivation, and distributed perpetration. The theories mainly cater to
the social, economic, and cultural characteristics of crime. However, technology is fundamental to cybercrime and needs to be allowed within criminological theory.

Secondly, Criminologists are trying to fit the theories to the crime rather than focusing on the emergence of new theories from the characteristics of the crimes. Up to now, researchers have been unable to situate cybercrime wholly within any of the theories. Criminologists have not yet created a robust and specialised theoretical background for cybercrime using its features or characteristics. Thus, the limitation in the knowledge and understanding of these crimes.

Thirdly, the future of cybercrime further provides significant concern for the theories. The advancements in technology imply increased levels of cybercrime and an increase in the modes of committing cybercrime. For example, cybercriminals might adopt automation by considering the introduction of technologies such as 5G, Artificial Intelligence, Big Data, and Quantum Computing. These changes will further stretch the inadequacy of the theories by introducing contexts that were not considered earlier.

7.5 Research Limitation

This research provides meaningful insights concerning the motivations, modes of operation and emerging trends of cybercrime. However, there are some recognised limitations. Firstly, this research could not reach more people in other stakeholder groups. Different stakeholder groups that could not be included are cybercrime victims, Internet Service Providers, financial service providers and other private sector stakeholders. Even within the active stakeholder group, the research was limited in the number of participants. In future research, all these stakeholders will be included, and emphasis will be placed on cybercriminals to enrich the insight into the crimes and evolution.

Secondly, the time for the data collection was limited. This limitation emanates from the extended timescales and bottlenecks associated with participant recruitment. For example, the process of securing approval to interview convicted criminals was too long due to bureaucracy and organisational bottlenecks. For future research, the application process will be initiated earlier to enable more time for data collection.

7.6 Future Research

The conduct of this research was based on Nigeria as an exemplar. However, the realities in other countries differ based on the unique sociocultural, economic, regulatory, and technological reality. It will be suitable to conduct this kind of research in different countries.
Replicating this research in other countries will further highlight both similarities and differences in the evolution of cybercrime worldwide.

Also, other topics were identified to extend the knowledge derived from this research:

**Investigate the best ways of combating cybercrime in developing countries.**

This research should focus on gaining in-depth ideas on these crimes and preventing or reducing their impact from the perspective of cybercriminals. Empirical research that combines the views of different cybercriminals would illuminate the process of regulation. The findings from this research will further steer the effectiveness of cybersecurity strategies.

**Investigate reasons for the failure of cybersecurity strategy in countries.**

Cybersecurity strategies worldwide have failed to achieve the desired result, as seen from continued cybercrime growth. There has been limited focus on the reason for the ineffectiveness of its implementation. Though this research identified some factors that affect regulation, others could be derived from research into this particular area. Such research should focus on stakeholder perspectives concerning the factors that inhibit the current cybercrime strategies.

**Investigate the role of cyberwarfare in cybercrime normalisation**

As identified in the emerging trends, cyber warfare might contribute to the normalisation of cybercrime. Focused research in this topic area is required. It will deepen the knowledge about members of the various cyber army members concerning their involvement in these schemes. This understanding will provide more knowledge of the discovered emerging trend from this research.

**7.7 Conclusion**

Cybercrime in Nigeria continues to grow, thereby making the country an exemplar for conducting the research. Various factors such as technology penetration, weak regulation, failure of basic industries, and high level of inequalities contribute to the initiation and growth of these crimes. It has become a means to climb from the lowest level of the economy to affluence. It is attractive to young people, expanding fast both in its prevalence and in crime typology.

However, new motivations such as altruism, revenge, creativity, financial gain, and nationalistic ideology are responsible for cybercrime complexity. The motivation and mode of
operation of these crimes are reflected in countries worldwide. The new crimes are changing rapidly, demonstrating unpredictability and the advancement of cybercriminals. The future of cybercrime is unpredictable as a reflection of emerging motivation. These new motivations are responsible for highly technical crimes.

Access to the internet comes with both benefits and problems. Global and local brands are expanding technology adoption with the increasing digitisation of services. The penetration of technology results in the growth of the risk experienced by internet users. The crimes are decentralised, thereby enhancing the scalability of the emerging transnational market.

This research has established the need for adjustments in regulation and theoretical research. Technological solutions should incorporate social interventions to reduce the negative impulses of criminals. Global integration of regulation will enhance oversight and governance. Also, researchers should embrace inductive approaches to research where new theoretical foundations of cybercrime will emerge.

In conclusion, the Nigerian experience has wider implications and mirrors experiences in other countries. The findings have demonstrated sociocultural and economic tendencies that stimulate these crimes. Thus, it is a local problem with international impact. Also, the experience in Nigeria further deepens the knowledge of what is obtainable in similar countries.
References


Adepegba, A. (November 19, 2019). Fraudster masterminds $100m scam from Kirikiri correctional facility. Https://punchng.com/fraudster-masterminds-100m-scam-from-kirikiri-correctional-facility/


Idris, I. (2016). Youth unemployment and violence: Rapid literature review. [http://hdl.handle.net/10625/55887](http://hdl.handle.net/10625/55887)


Nalla, M., & Seung-yeop, P. (2016). Police perceptions of cybercrime in South Korea: Implications for combating cyberterrorism and cooperation with private security. Journal of


Punch Newspaper (June 8, 2018a). IG Idris and never-ending brutality of SARS. Https://punchng.com/ig-idris-and-never-ending-brutality-of-sars/


Tade, O., & Akinleye, B. (2012). 'We are Promoters not Pirates': A Qualitative Analysis of Artistes and Pirates on Music Piracy in Nigeria. *International Journal of Cyber Criminology, 6*(2), 1014-1029


Vecchiarelli, J. (February 8, 2018). Nigeria Comes Face to Face with a HUGE Literacy Crisis. https://www.proliteracy.org/Blogs/Article/311/Nigeria-Comes-Face-to-Face-with-a-HUGE-Literacy-Crisis


WeForest (June 10, 2019). Brazil as an agricultural powerhouse. Https://www.weforest.org/newsroom/brazil-agricultural-powerhouse


Appendix A: Consent Form

XXXX business address

of participating organisation

St Georges Building
141 High St
Portsmouth
PO1 2HY

T: 023 9284 3900

Pelumi.apantaku@port.ac.uk

11th April 2016

Form 01/cons

CONSENT FORM – Interview Participant

**Research:** Cybercrime in Nigeria: Perception and Reality

**Researcher:** Pelumi O Apantaku

**Interview Participant:** (..organization..): (..name..)

Please initial box

1. I have read and assimilate the invitation & information sheet (Form 02/inv) dated 11th April, 2016 about this study. I am satisfied after extensive understanding of the research through information consideration, inquiries and adequate explanation.

2. I admit of been aware that my participation is voluntary. I am satisfied that I can withdraw my participation and permission for data usage before usage at any time without any justification.

3. I am fully aware that some of the collected data will be included in the PhD thesis,
journal articles and academic presentations with proper maintenance of anonymity that will eliminate any sort of traceability. I totally support use of data in publications for general access coupled with the fact that only the researcher can access the original data. I also understand that the no other person will access the original data with destruction after completing the data.

4. I agree to interviews being recorded.

5. I do not wish interviews to be recorded, but I consent to notes being taken.

6. I agree to take part in the above study.

Name of participant: …………………………………………………………………………………………………………………………………………………

Participant’s signature on behalf of (.organisation.): …………………………………... Date: …………………………………………

Name of researcher: ………………………………………………………………………………... …………………………………………

Researcher’s signature: ………………………………………………………………… Date:

If you have any further queries, please contact me at the above address or by e-mail; alternatively you can contact my research supervisor, Dr Victoria Wang at the same postal address or at Victoria.Wang@port.ac.uk.
Cybercrime in Nigeria: Perception and Reality

Interview Invitation and Information Sheet

Dear YYYYYY,

Based on the recent telephone conversation, attached are further explanations about the research and the importance of your assistance. I am Pelumi Apantaku currently conducting a full time PhD in Criminology at the Institute of Criminal Justice Studies (ICJS) at the University of Portsmouth. The topic is “Cybercrime in Nigeria: Perception and Reality” which is very consequential but enjoys limited popularity in research.

Research method

I will be aiming to interview nearly 45 employees from various agencies including the Nigerian Police Force, the Nigeria Security and Civil Defence Corps, the Economic and Financial Crime Commission, the Judiciary and the Legislature together with convicted prisoners that were involved in cybercrime. The aim is to have in depth understanding of the changing trend of cybercrime in Nigeria in order to determine the perception in order to discover the current
reality based on the new trend in the Cybercrime in Nigeria industry. The interview is expected to be approximately 40 to 60 minutes in duration. The interview will be conducted at your preferable venue and period. The interview might be recorded or notes taken. The interview will take a discussion mode attracting prompts for further elaboration of suggestion.

Data management
Opinions and statements made during the interview might be referenced or quoted within the thesis or relevant academic journals. However, your identity will be safeguarded with the preservation of your anonymity and your organisation through the use of codes in quotes. I will be pleased to provide the research results or published journal articles if you desire.

As a standard, you should not provide any information that will amount to ethical challenges like infringing on the confidentiality of clients or accepting the prohibited by relevant regulators or the law. This research will fully comply with the Data Protection Act 1998 for all accepted data by preventing unauthorised data. The collected original data will be destroyed on the conclusion of the PhD program.

Consent
It must be stated that participation is voluntary and withdrawal at any time is at your discretion. Prior to the analysis or publishing of the collected data, you own the right to withdraw the permission. This can be done by contacting me via this email address pelumi.apantaku@port.ac.uk
Attached is a consent form (Form 01/cons) which should be filled as a confirmation of your voluntary wish to participate in the research. Please keep a copy of this letter and the consent form for your personal records.

Research governance
I am supervised by Dr Victoria Wang at University of Portsmouth. The research is governed by the ethics committee to make sure that strict adherence to research ethics is upheld. The methods to be used in this research has been reviewed and approved by the ICJS Ethics Committee
Please contact me or Dr Victoria Wang at the University in case of further inquiries concerning this research and participation. In case of any complaints, you should contact Professor Button at the address given provided above or the Complaints Officer at the address below;

University of Portsmouth
University House
Winston Churchill Avenue
Portsmouth
PO1 2UP
T: 023 9284 3900
Victoria.Wang@port.ac.uk

Yours sincerely

Pelumi O Apantaku
Pelumi.apantaku@port.ac.uk
Appendix C: Focus Group Invitation

Cybercrime in Nigeria: Perception and Reality
Focus Group Invitation and Information Sheet

Dear YYYYY,

Based on the recent telephone conversation, attached are further explanations about the research and the importance of your assistance. I am Pelumi Apantaku currently conducting a full time PhD in Criminology at the Institute of Criminal Justice Studies (ICJS) at the University of Portsmouth. The topic is “Cybercrime in Nigeria: Perception and Reality” which is very consequential but enjoys limited popularity in research.

Research method

I will be aiming to interview nearly 45 employees from various agencies including the Nigerian Police Force, the Nigeria Security and Civil Defence Corps, the Economic and Financial Crime Commission, the Judiciary and the Legislature together with convicted prisoners that were involved in cybercrime. The aim is to have in depth understanding of the changing trend of
cybercrime in Nigeria in order to determine the perception in order to discover the current reality based on the new trend in the Cybercrime in Nigeria industry. The focus group is expected to be approximately 75 to 90 minutes in duration. The focus group will be conducted with your colleagues from your organisation. The focus group might be recorded or notes taken. The focus group will take a discussion mode attracting prompts for further elaboration of suggestion. The focus group will be conducted at a suitable venue and time for every individuals involved.

Data management
Opinions and statements made during the focus group might be referenced or quoted within the thesis or relevant academic journals. However, your identity will be safeguarded with the preservation of your anonymity and your organisation through the use of codes in quotes. I will be pleased to provide the research results or published journal articles if you desire.

As a standard, you should not provide any information that will amount to ethical challenges like infringing on the confidentiality of clients or accepting the prohibited by relevant regulators or the law. This research will fully comply with the Data Protection Act 1998 for all accepted data by preventing unauthorised data. The collected original data will be destroyed on the conclusion of the PhD program.

Consent
It must be stated that participation is voluntary and withdrawal at any time is at your discretion. Prior to the analysis or publishing of the collected data, you own the right to withdraw the permission. This can be done by contacting me via this email address pelumi.apantaku@port.ac.uk

Attached is a consent form (Form 04/cons) which should be filled as a confirmation of your voluntary wish to participate in the research. Please keep a copy of this letter and the consent form for your personal records.

Research governance
I am supervised by Dr Victoria Wang at University of Portsmouth. The research is governed by the ethics committee to make sure that strict adherence to research ethics is upheld. The methods to be used in this research has been reviewed and approved by the ICJS Ethics Committee

Please contact me or Dr Victoria Wang at the University in case of further inquiries concerning this research and participation. In case of any complaints, you should contact Professor Button at the address given provided above or the Complaints Officer at the address below;
University of Portsmouth
University House
Winston Churchill Avenue
Portsmouth
PO1 2UP
T: 023 9284 3900
Victoria.Wang@port.ac.uk

Yours sincerely

Pelumi O Apantaku
Pelumi.apantaku@port.ac.uk
Appendix D: Ethical Approval

2nd December 2016

Dear Pelumi Apantaku

<table>
<thead>
<tr>
<th>Study Title:</th>
<th>Cybercrime in Nigeria: Perception and Reality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethic Committee</td>
<td>15/16-49</td>
</tr>
<tr>
<td>reference:</td>
<td></td>
</tr>
</tbody>
</table>

Thank you for submitting your documents for ethical review. The Ethics Committee was content to grant a favourable ethical opinion of the above research on the basis described in the application form, protocol and supporting documentation, revised in the light of any conditions set, subject to the general conditions set out in the attached document.

The Ethics Committee provides a favourable ethical opinion with the following requirements.

1. You state that interview participants can withdraw on the request until the final dissertation is published. The documentation should be amended to state “a participant may withdraw up to the point of data analysis”. It is not feasible for an interview participant to withdraw once analysis has started. Ensure that all documentation is amended to state this.
2. The documentation should be amended to state that focus group participants can withdraw either before or during the Focus Group, but not after, as it is not feasible to disentangle the dynamic of the focus group once the focus group has been completed. Ensure that all documentation is amended to state this.
3. A ‘Consent Form’ needs to be included in the heading of the ‘Focus Group – Interview Participant’ consent form.
4. All Consent forms must state that the data could be accessed by others in the University, such as the supervisor, the ethics committee or the viva examiners or the Board of Examiners and it should be stated that the data will be kept for 10 years and consent forms for 30.
5. The contact details for complaints should be amended to, Dr. Phil Clements (phil.clements@port.ac.uk), Head of Department, and Dr. Jane Winstone (jane.winstone@port.ac.uk), Chair, Faculty of Humanities and Social Sciences Research Ethics Committee. All documentation should be amended to state this.
6. The research will not contact participants. Contact with the participants will be made by the gatekeeper in all cases and provided with the researcher contact details. If the participants want to continue they will make contact with the researcher. All documentation should be amended to make this clear.
7. We asked for 'warnings' to be inserted into the information sheets for participants. (Please see the committee feedback on the previous submission). Although you indicate that these warnings have been included, none of the reviewers could identify them in the participant information sheet. These warnings must be included. These requirements must be completed before data collection commences and will be overseen by your supervisor, Dr. Victoria Wang, to ensure that they have been fulfilled.

There is no need to submit any further evidence to the Ethics Committee; the favourable opinion has been granted with the assumption of compliance.

The favourable opinion of the EC does not grant permission or approval to undertake the research. Management permission or approval must be obtained from any host organisation, including University of Portsmouth, prior to the start of the study.

Documents reviewed

The documents reviewed by The Faculty of Humanities and Social Sciences Ethics Committee.

<table>
<thead>
<tr>
<th>Document</th>
<th>Version</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Form</td>
<td>3</td>
<td>15/11/16</td>
</tr>
<tr>
<td>Consent Form(s)</td>
<td>3</td>
<td>15/11/16</td>
</tr>
<tr>
<td>Invitation Letter</td>
<td>3</td>
<td>15/11/16</td>
</tr>
<tr>
<td>Interview Questions</td>
<td>3</td>
<td>15/11/16</td>
</tr>
<tr>
<td>Focus Group Questions</td>
<td>3</td>
<td>15/11/16</td>
</tr>
</tbody>
</table>

Statement of compliance

The Committee is constituted in accordance with the Governance Arrangements set out by the University of Portsmouth.
After ethical review

Reporting and other requirements

The enclosed document acts as a reminder that research should be conducted with integrity and gives detailed guidance on reporting requirements for studies with a favourable opinion, including:

- Notifying substantial amendments
- Notification of serious breaches of the protocol
- Progress reports
- Notifying the end of the study

Feedback

You are invited to give your view of the service that you have received from the Faculty Ethics Committee. If you wish to make your views known please contact the administrator ethics-fhss@port.ac.uk

Please quote this number on all correspondence – 15/16:49

Yours sincerely and wishing you every success in your research

**************

Chair
Dr Jane Winstone
Email: ethics-fhss@port.ac.uk

Enclosures: “After ethical review – guidance for researchers”
Appendix E: Research Questions

Generic Questions

- Can the life of crime be justified as based on the economic condition?
- Has economic condition stimulated cybercrime in Nigeria?
- Does the poor see cyber crime as a means of survival and increasing their chance in the society?
- Is the agricultural sector feeling the effect of cybercrime?
- How has cybercrime viewed with respect to economic empowerment in the various migrant settlements?

EFCC Officials

- Can you describe the new trend in the cybercrime industry in Nigeria?
- How can you describe the skill level of crimes being perpetrated in Nigeria online?
- In what ways has affordable internet influence the nature and dynamics of cybercrime in Nigeria?
- What role has internet affordability play in eliminating reliance on cybercafé in perpetrating cybercrime?
- What is your opinion concerning the impact of rapid internet penetration on increasing sophistication of cybercrime?
- How can you describe the future of the cybercrime industry in the short term (5 years) and long-term (10 years)

NSCDC Officials

- In what ways have rural-urban migration influence urban poverty in Nigeria?
- How has the rural-urban migration influenced the complexity and variation in the Cybercrime in Nigeria industry?
- Has cybercrime perpetration been decentralised as a result of the affordable internet?
- How has cybercrime viewed with respect to economic empowerment in the various migrant settlements?
• How has the migration contribute to the evolution of the cybercrime market in Nigeria?
• Is there any proof that cybercrime practice has increased the economic and social status of the rural migrants?
• How has the GSM introduction enhanced the internet penetration in Nigeria?

**The Nigerian Police**

• What are the changes in the targeted victims of cybercrime in Nigeria
• Has internet penetration influenced the volume of cybercrime in Nigeria?
• Is the affordable internet connection makes cybercrime more lucrative?
• Has internet affordability changed the nature of cybercrime in Nigeria?
• Can you explain the degree of technical competence within the Nigerian police force and its impact on combatting cybercrime in Nigeria?
• Please describe the changes in motivation in cybercrime perpetuation in nature?

**The Legislature**

• In what ways can you attach cybercrime impact on legislature both individually and collectively?
• Can you describe the level of importance attached to cyber crime in Nigeria?
• What are the challenges in making laws to combat cyber crime?
• How has cybercrime viewed with respect to economic empowerment in the Nigerian legislature?

**The Judiciary**

• Please explain the changes in the type of cyber crime being prosecuted in court?
• Can you detail the degree of efficacy of the current cybercrime bill in prosecuting cyber crime cases?
• From prosecuted cases;
  o What are the motivations of perpetrators
  o What are the nature of targeted victims
• Can you explain the degree of conviction of cyber crime cases
Convicted Criminal

- What is the motivation for taking into cyber crime
- Can you explain the nature of victims in terms of age range and location
- What are the changes in the industry currently
- What is your view concerning the organised nature of cybercrime in Nigeria?
- What role is technology penetration having on the cybercrime industry in Nigeria?

Focus Group Questions

- What are the new types of cybercrime being experienced in Nigeria?
- How has decentralisation enhanced the perpetration?
- What is your opinion concerning the collaboration of Cybercrime in Nigeria perpetrators and other international criminal rings
- Describe the impact of cyber crime in Nigeria on other countries in West Africa
- Why are local victims being targeted increasingly?