

# Effects of Cybercrime on the Socio-Economic Development of Ankpa Local Government Area of Kogi State, Nigeria

Oluwatoyin Adewale SHEYINDEMI<sup>1</sup>, Thomas Imoudu GOMMENT, Ph.D<sup>2</sup>

*Department of Sociology, Faculty of Social Sciences, Prince Abubakar Audu University, Anyigba, Kogi State, Nigeria.*

## Abstract

This study examined the effects of cybercrime on socio-economic development in Ankpa Local Government Area of Kogi State, Nigeria. Specifically, the study explored the causes, effects and strategies for reducing cybercrime and its effects in the area. A descriptive survey research design was adopted, utilizing quantitative approaches. A sample size of 378 respondents was selected using multi-stage sampling techniques. Primary data were collected through structured questionnaires, while secondary data were sourced from scholarly publications, journals, articles and official reports. Data were analyzed using descriptive statistics such as frequency and percentages, while inferential statistics including regression was applied to test the hypothesis. Revealing that, strategies for minimizing cybercrime particularly public awareness, job creation, and law enforcement collaboration do reduce its effects on socio-economic development in Ankpa LGA. Findings revealed that high unemployment, poverty, peer influence, weak enforcement of cyber laws, and poor digital literacy were the major causes of cybercrime in Ankpa LGA. In terms of effects, cybercrime was found to discourage local and foreign investment, erode trust in digital platforms, reduce business profitability, and cause revenue loss for both private enterprises and government. Approximately 72% of respondents agreed that cybercrime undermines social trust, weakens productivity, and hampers socio-economic progress. Regarding strategies for reduction, respondents emphasized the importance of stronger cyber laws, employment generation, digital literacy campaigns, and closer collaboration between security agencies, traditional leaders, and religious institutions. Although religious and traditional institutions were perceived as valuable in moral reorientation, statistical analysis showed that their impact alone was not significant in reducing cybercrime. The study concluded that cybercrime remains a pervasive and multidimensional threat to sustainable socio-economic development in Ankpa LGA. It fosters insecurity, discourages investment, weakens moral values, and erodes public trust in digital systems. Consequently, a multi-dimensional approach was recommended strengthening existing cyber laws, expanding employment opportunities, promoting digital literacy through awareness campaigns, and enhancing collaboration among law enforcement agencies, traditional authorities, and community leaders to restore moral orientation and curb cybercrime in the region.

**Keywords:** Cybercrime, Social Development, Crime, Economic Development, Cybersecurity.

## BACKGROUND OF THE STUDY

The rise in the use of information and communication technology (ICT) has liberalized channels of communicating and maintaining relationships between individuals, groups and even nations. Global citizens can now interact freely, conduct widespread businesses, and engage in trans-border trade and commerce. The internet is a crucial technology of the information age which creates a multimodal and interactive communication. According to Statista (2024), the number of internet users worldwide stood at 5.3 billion in 2023, which means that around two-thirds of the global population is currently connected to the internet, otherwise known as World Wide Web.

However, this phenomenon has also produced a phenomenal increase in the incidence of criminal activities, endorsed illegal businesses, and entrenched cyber terrorism and cybercrime.

**Corresponding Author:** Oluwatoyin Adewale SHEYINDEMI, Department of Sociology, Faculty of Social Sciences, Prince Abubakar Audu University, Anyigba, Kogi State, Nigeria.

The growing use of the internet has provided a conducive platform for miscreants to engage in the misuse of information and communication technology (ICT) and this has resulted in a potential threat to individuals in terms of cybercrimes (Fatoki, 2023). The modern techniques that are proliferating towards the use of internet activities result in creating exploitation, vulnerability making a suitable way for transferring confidential data to commit an offence through illegal activity. The activity involves attacking information center data system, theft, online transaction fraud, internet sale fraud and also deployment in internet malicious activities such as virus, worm and third-party abuse like phishing and email scams (Sule et al., 2021).

Cybercrime can be simply described as criminal activities carried out using electronic devices, the communication network, and data with the primary purpose of extorting from victims, once a vulnerability is exploited (Aghatise, 2016). Often times, this type of crime is targeted on the victim's computer, with the intention to spread malware, obtain illegal information, and gain unauthorized access to make profit or steal vital information from victims. Cybercrime is a global threat and one of the biggest threats to business everywhere in the world. It has also been regarded as one of the fastest growing criminal activities around the world (Inge & Lawrence, 2021).

In line with this, Umana et al. (2024) broadly classified cybercrime into three categories. The first category is cybercrime against individual and property, criminal activities in this category is targeted against individuals and their properties. The various ways through which this is carried out include cyber stalking, defamation, unauthorized control or access over computer system, email spoofing, cheating and fraud, computer vandalism, transmitting virus, and intellectual property crime. The second category is cybercrime against organizations, which are targeted against governments, firms, companies, and corporate bodies. These include unauthorized control/access to computer systems, possession of unauthorized information, cyber terrorism against governments and corporations, espionage, and distribution of pirated software. The third category is cybercrime against society, which are cybercrime activities targeted against the society at large. These include pornography, trafficking, financial crimes, online gambling, and forgery.

According to several studies, Nigeria is one of the countries of the world from where cybercrime originates (Shola, 2021; Inge & Lawrence; Lar, 2024; Babayo, 2021). Although, the most common type of cybercrime in Nigeria is 'Advanced Fee Fraud' which was popularly known as

'419' and presently called 'yahoo-yahoo'. There are several other types such as hacking, phishing, spamming, identity theft, piracy, credit card fraud, and scamming (Ogunlere et al., 2013; Adegoke & Kamar, 2024; Idowu, 2024). There is no doubt that cyber-criminals occupy a large part of social media and the online ecosystem where money, data and transactions are exchanged online.

Furthermore, cybercrime in Nigeria is socially organized and highly networked, as perpetrators are assisted by insiders and bank staff, who leaks vital customers' details and facilitate payment transfer through domiciliary accounts, credit cards, and other money transfer platforms (Ugah et al., 2024). According to Uzoho (2019), cybercrime accounted for about 43% of total monetary loss due to fraud in Nigeria in 2016. Proshare (2020) opined that an estimate of N250 billion and N288 billion financial loss was recorded in 2017 and 2018 respectively due to cybercrime on business, banks, and government infrastructure in Nigeria.

Nigeria loss the sum of \$500 million per annum on cybercrime, with banks and corporate offices being the most affected. This necessitates an understanding of the most serious cyber security threats facing businesses in Nigeria, as well as strategies for reducing them. These losses occasioned by cyber insecurity have negative impacts on individuals, businesses and the government in terms of welfare losses, business disruption, profit reduction, rising operating cost, and revenue losses.

The prevalence of cybercrime has created a bad image for Nigeria amongst the committee of nations as one of the most corrupt nations in the world. This tarnished national image affects the way Nigerians are treated abroad with suspicion and extreme caution as Nigerians are stereotyped to be criminals, and hence not to be trusted. Foreign investors are scared of Nigeria, considering it as risky and unattractive business zone (Abdul-Rasheed et al., 2016). In highlighting the consequences of cybercrime in Nigeria, Folashade and Abimbola (2013) posited that cybercrime hinders the socio-economic development of Nigeria as it endangers lack of trust and confidence in profitable transactions. Also, the findings of the study by Maitanmi et al. (2013) shows that cybercrime impedes socio-economic development as it scares away foreign investors who have no confidence in Nigerian economy due to the activities of cyber criminals.

Therefore, it is crucial to explore the concept of cybercrime and its effects on the socioeconomic development of Nigeria, using Ankpa Local Government Area of Kogi state as an example.

## STATEMENT OF THE PROBLEM

Cybercrime is one of the fastest growing criminal activities in the world today, as it covers a large range of illegal activities related to computers, internet and computer networks. The advent of the internet has to a large extent marred the socioeconomic development of many nations due to the wave of fraud and criminality associated with the cyberspace. There is no gainsaying that the cyberspace has in recent times become an environment where most lucrative and safest criminal activities thrive, thereby making crimes committed through the cyber space a global threat.

According to a report by Business Day Newspaper (2022), the Center for Strategic and International Studies (CSIS, 2024), has estimated that \$600 billion is lost to cybercrime each year, an increase from what was recorded in 2014 that puts global losses at about \$445 billion. Worse still, numerous studies have estimated a yearly 15% per year increase in global cybercrime losses over the next few years, reaching \$10.5 trillion annually by 2025.

In Africa, the peril of cybercrimes recorded a massive rise in the first six months of 2022, with phishing and scams hitting 43.8% and 17.4% in Kenya and Nigeria, respectively (Guardian Newspapers, August 3, 2022). Nigeria was been ranked 16th among the countries most affected by cybercrime in the world in 2020. In its latest internet crime report, the United States Federal Bureau of Investigation (FBI, 2024), reported that Nigeria received 443 complaints relating to cybercrime in 2023.

Incidences abound where innocent Nigerians have lost their fortunes to cyber criminals pretending to be friends or business partners in the guise of offering high investment returns on businesses that hardly exist. Also, a number of institutions, particularly internet banking and other online transactions, have become targets of cyber criminals, with varying degree of success (Uga et al., 2024; Agbamu & irogbo, 2024; Akintayo & Ekele, 2024). Theft of identity, spamming, unauthorized access, cyber bullying, cyber stalking, amongst others, are some of the rampant cases of cybercrimes in Nigeria today.

Tales of people being duped by cybercriminals are often heard on daily basis causing the security agents to swing into action to seal homes and arrest the perpetrators, particularly in Ankpa Local government Area where it has been observed that the internet has encouraged cybercrime. As the country integrates electronic payment system into its financial institution, a step that is expected to accelerate the nation's socioeconomic growth and development, the negative impact of cybercrime on

businesses continue to create fear and uncertainty in the mind of users and potential online users.

The consequences of cybercrime are enormous, multifaceted and often difficult to accurately measure (Ndubueze, 2020). Cybercrime arguably has several consequences for individual internet users, businesses, organizations, government agencies and society as a whole.

Sorunke (2021) maintained that Nigeria in the cyber-space is under threats with such vulnerability, many loopholes in the system and issues bothering payment networks. Most especially, Nigeria's integrity and external image in diaspora has been negatively affected due to high rates of cybercriminals.

According to Abdulkadir et al., (2023), the current menace of cybercrime in parts of Kogi State has assumed an unprecedented and multi-faceted dimension, especially among the youths. Hence, there is the need to stem the tide in view of the devastating impact of cybercrime: This current study therefore will examine the phenomenon of cybercrime in Ankpa Local Government Area from a sociological perspective.

Furthermore, some past studies have attempted to establish the nexus between cybercrime and other parameters and indices in Nigeria (Oluwafemi, 2021; Idowu, 2024; Ugah et al., 2024; Okoru & Oluku, 2024). These studies have however failed to establish a link between socio-economic development and cybercrime in Nigeria. More so, studies available have not analyzed this subject matter from the sociological prism. As such, this study adopted a triangulated approach to explore the effects of cybercrime on the socio-economic development of Nigeria, using Ankpa Local Government Area as a case study.

## RESEARCH QUESTIONS

The following research questions guided the study:

- i. What are the causes of cybercrime as perceived by residents of Ankpa LGA of Kogi State?
- ii. What are the effects of cybercrime on the socio-economic development of Ankpa LGA of Kogi State?
- iii. What are the strategies for reducing the incidence of cybercrime and its effects on socio-economic development of Ankpa LGA of Kogi State?

## AIM AND OBJECTIVES OF THE STUDY

The aim of this study was to examine the effects of cybercrime on the socio-economic development of Ankpa Local Government Area of Kogi State, Nigeria. The specific objectives therefore included to:

- i. Identify the causes of cybercrime as perceived by residents of Ankpa LGA of Kogi State.
- ii. Explore the effects of cybercrime on the socio-economic development of Ankpa LGA of Kogi State.
- iii. Examine the strategies for reducing the incidence of cybercrime and its effects on socio-economic development of Ankpa LGA of Kogi State.

## RESEARCH HYPOTHESIS

This study attempted to test the Research Hypothesis:

$H_0$ : Strategies for reducing the incidence of cybercrime and its effects does not reduce the effects of cybercrime on socio-economic development in Ankpa LGA.

## LITERATURE REVIEW

This chapter provides the overview of important concepts and reviewed past literature on the subject matter. Also, the chapter highlighted the theoretical underpinnings of the study, and concludes with identifying gaps in reviewed literature as well as summary of the chapter.

### Conceptual Review

Concepts play a fundamental role in social life. Humans identify and give meaning to the individuals, objects, and situations that they encounter by categorizing them, assessing them in terms of their concepts, or abstract mental representations of the world. Subsequent behavior and communication typically proceed on the basis of understandings formed through this process. It is pertinent that in every research engagement like this one, important concepts that are germane to the proper understanding of the study are defined. This is so because there is need for the reader to comprehend the essence of the study. Hereunder, therefore, various definitions by different authors on some important terms and concept will be provided here. The concepts include crime, cybercrime, socioeconomic development, and sociological analysis.

### The Concept of Crime

Bentham defined Crime as, "offences are whatever the legislature has banned/prohibited for good or for bad reasons. If the question relates to theoretical research for the discovery of the best possible laws according to the principles of utility, we give the name of offence to every act which we think ought to be prohibited by reasons of some evil which it produces or tends to produce." Blackstone (2019) defined Crime as "an act committed or omitted in violation of a Public Law either forbidding or commanding it." Stephen has suggested a modification in the Blackstone's version of definition on Crime and states that, "A crime is a violation of a right, considered in

reference to the evil tendency of such violation as regards the community at large." Austin (2021) posits that, "a wrong which is pursued at the discretion of the injured party and his representatives is a civil injury; a wrong which is pursued by the sovereign or his subordinates is a crime."

Furthermore, Gill and Schubert (2023) defined crime as an illegal act in which someone can be punished by the government. An offence that calls for public censure and punishment typically in the form of a fine or incarceration is considered a crime. A civil wrong, also known as a tort, is an action taken against a person that calls for payment or reparations; it is not the same as a crime. Generally speaking, something that's unfair, wrong, and difficult to fix is what defines crime. Furthermore, Opp (2020) defined crimes as actions or non-actions that violate the criminal law. Crime generally is a deliberate act that results in harm, physical or otherwise, to one or more people in a manner prohibited by law. The Encyclopedia (2019) defines crime as an act proscribed by law and subject to punishment. Any behaviour that is deemed to be against societal norms or values is considered a crime. Additionally, Matthew (2018) defined crime as deviant behaviour that violates prevailing norms and standards prescribing how humans ought to behave normally. Singh (2021) defined crime as any wrongful act conducted or done with the intent of committing that wrongful act or offence, as well as any act committed or done with the intent of committing that wrongful act or offence. Similarly, Haugaard (2022) defined crime as action that violates the legitimate social norms of a collective social order.

### The Concept of cybercrime

The term *cybercrime* originates from the fusion of "crime" and the prefix "cyber," which itself derives from *cybernetics*, a word rooted in the Greek term *kubernan*, meaning "to steer or govern." Despite its growing importance, there is still no universally accepted definition of cybercrime. As Yan (2006) notes, even experts tasked with combating cybercrime struggle to agree on a single, standard definition.

Several scholars have attempted to conceptualize the term from different perspectives. Halder and Jaishankar (2011) define cybercrime as offenses committed against individuals or groups with the criminal intent of damaging the victim's reputation or causing physical or psychological harm. Such crimes are carried out through modern communication networks like the internet using chat rooms, emails, notice boards, and groups as well as mobile phones. Casey (2004) similarly characterizes cybercrimes as unlawful acts carried out using innovations in information and communication technology (ICT).

The Internet Crime Complaint Center (ICCC, 2010) offers a broader definition, describing cybercrime as any illicit activity committed through the Internet, whether by browsing, chatting, emailing, or other online interactions. Wall (2001) also observes that while the term remains vague in legal contexts, it is widely used in politics, law enforcement, media, and academia. Oriola (2005) focuses on fraudulent online practices such as phishing, in which unsuspecting victims are tricked into revealing sensitive information such as banking details through false promises of wealth. In line with this, the *Free Dictionary* defines internet crime as any fraudulent scheme that uses online platforms to unlawfully deprive someone of property, rights, or financial interest. Examples include phishing, spoofing, spamming, web jacking, escrow fraud, and other deceptive practices.

Cybercrime has been closely linked to the advancement of computers, telephones, and other ICT tools. According to Shehu (2014), the term itself was popularized by Peter Cassidy, Secretary General of the Anti-Phishing Working Group, to distinguish specialized software used for financial crimes from other malicious programs. In practice, cybercrime involves using digital tools to defraud unsuspecting victims. This ranges from identity and credit card theft, where sensitive financial data is stolen and misused, to larger schemes like money laundering facilitated by terrorist or organized crime groups.

The classifications of cybercrime are equally diverse. Brenner (2023) categorized cybercrimes into three main groups:

Target cybercrime, where the computer itself is the direct target.

Tool cybercrime, where the computer serves as the means of committing the offence.

Computer incidental crime, where the computer plays only a minor role in the crime.

This categorization aligns with the earlier framework proposed by Kamani (2011), who broadly divided cybercrimes into three categories:

#### **Cybercrime against individuals and property**

These are offences targeted at persons or their property, including harassment via email, cyberstalking, circulation of obscene materials, defamation, unauthorized access or control of computer systems, indecent exposure, email spoofing, cheating and fraud, computer vandalism, virus transmission, net-trespass, intellectual property theft, and internet time theft.

#### **Cybercrime Against Organizations**

These crimes target governments, firms, companies, and corporate entities. Examples include unauthorized access to computer systems, possession of unauthorized information, cyber-terrorism against corporations or state institutions, espionage, and distribution of pirated software.

#### **Cybercrime Against Society**

These offences affect the wider society and include pornography, human trafficking, financial crimes, sales of illegal articles, online gambling, forgery, and related illicit activities.

Some of them are specifically explained as follows:

**Hacking:** Hacking refers to the deliberate act of identifying weaknesses in a computer system or network in order to exploit its security features and gain unauthorized access to personal or business data. This often involves the use of stolen passwords, malicious codes, or the manipulation of system loopholes to break into organizational, individual, or government-owned systems. In essence, hacking is the attempt to compromise a computer or private network to steal secret information or manipulate data. Hackers often take control of computer systems for illicit purposes, deploying specially written or pre-packaged programs to breach targets. As Kejal (2011) notes, some hackers engage in these acts for personal financial gain, such as stealing credit card information or transferring funds illegally from victims' bank accounts.

Hackers exploit system vulnerabilities through backdoor programs or password-hacking software. They may monitor a victim's online activity, install spyware, or introduce files onto a computer without the user's knowledge. Such programs often harvest sensitive data such as passwords, personal identification numbers, and credit card details. In Nigeria, there have been numerous cases of hackers targeting banks, telecommunications companies, and even government databases, leading to significant financial losses and breaches of national security (Adebanjo & Ogunyemi, 2020). Hacking is thus both a technological and socio-economic threat, undermining digital trust and institutional stability.

**Cyber-Theft:** Cyber-theft involves the unlawful use of computers and digital communication systems to steal information or funds in electronic form. Offenders often penetrate the systems of banks and financial institutions to transfer money into their own accounts. Credit card fraud is a particularly common example, with Nigerian banks reporting growing incidents of unauthorized

withdrawals and fraudulent electronic transfers. One of the major concerns is that large amounts of money can be stolen swiftly with minimal effort, while many affected institutions avoid public disclosure for fear of reputational damage and loss of customer confidence.

Cyber-theft is one of the most reported and widespread cybercrimes, making it a preferred avenue for cybercriminals seeking large financial gains with relatively low physical risk (Adeniran, 2018). The menace extends beyond individuals to businesses, where proprietary company data can be stolen and used for corporate espionage. In Nigeria, reports by the Economic and Financial Crimes Commission (EFCC, 2022) have shown that cyber-theft contributes significantly to annual financial losses across the banking sector.

**Viruses, Worms, and Malicious Programs:** Another major form of cybercrime is the use of malicious software such as viruses, worms, Trojans, and logic bombs. A virus is a computer program designed to damage systems by attaching itself to other programs or files, while worms spread independently by exploiting system loopholes. Trojan horses appear harmless but release destructive payloads once executed. Logic bombs, on the other hand, are triggered by specific events such as a system date or action. Notable global examples include the *Melissa Virus* (1999), which disrupted the email systems of major corporations, and the *MyDoom Worm* (2004), which infected nearly 250,000 computers in a single day.

These attacks have been replicated in Nigeria, where organizations regularly report disruptions caused by malware infections. For example, the Nigeria Deposit Insurance Corporation (NDIC, 2020) reported that several local banks had suffered productivity losses and incurred huge costs in containing malware attacks. Such threats highlight the vulnerability of businesses and individuals to malicious programs that damage systems, compromise sensitive data, and erode trust in digital platforms.

**Online Scams:** Online scams take various forms, including investment fraud, lottery scams, employment scams, and charity scams. These schemes are aimed at deceiving the general public to obtain money or sensitive information. Fraudsters often create authentic-looking websites, emails, or blogs that mimic legitimate businesses or institutions, thereby luring victims into providing their personal or financial information. For instance, fake job advertisements promising high salaries and flexible conditions are used to target job seekers, who are then asked to provide upfront payments or confidential data.

In Nigeria, such scams are often associated with the so-called “Yahoo-Yahoo” culture, where young fraudsters

engage in romance scams, fake investment platforms, and bogus employment offers to dupe victims locally and internationally (Tade, 2013). These practices have become not only a source of income for perpetrators but also a social menace, tarnishing the nation’s reputation globally.

**Spamming:** Spamming refers to the mass distribution of unsolicited or irrelevant messages, usually for advertising, phishing, or spreading malware. Such emails often include fraudulent links, malicious attachments, or phishing campaigns designed to steal users’ credentials. Businesses are particularly affected, as spam consumes bandwidth, increases overhead costs, and wastes significant employee time on filtering and deleting unwanted emails.

Spammers continuously evolve their techniques, using permutations of content and images to bypass spam filters. According to Alhaji et al. (2016), spamming in Nigeria has become a serious issue, exposing both network operators and users to heightened risks of identity theft, phishing, and malware. Beyond the financial implications, spamming contributes to broader cyber-insecurity by normalizing fraudulent online practices and overwhelming trust in email communication systems.

**Malware:** Malware, short for malicious software, refers to any program intentionally created to disrupt the functioning of computers, servers, clients, or networks. Its objectives include leaking confidential data, gaining unauthorized access to systems, and depriving users of access to critical information. In simpler terms, malware is software designed to interfere with the normal functioning of a computer while remaining undetected by antivirus software. Attackers may install malware manually by exploiting administrator privileges or remotely through privilege escalation.

Malware is often deployed against government agencies or company websites to collect classified information and undermine their operations. Once installed, it can disrupt processes and create entry points for cybercriminals to extract details such as personal identification numbers, bank account information, debit card PINs, and security passwords. In Nigeria, malware attacks have targeted banks, telecommunications firms, and ministries, resulting in disruptions and significant financial losses. For example, Osho and Adepoju (2016) observed that poorly regulated internet access points such as cybercafés have provided fertile ground for malware infections, highlighting the infrastructural vulnerabilities that enable such crimes.

**Financial Fraud and Phishing:** Financial fraud online often manifests in the form of phishing scams, which rely on social engineering techniques. Perpetrators pose as trusted

institutions, such as a victim's bank, and send fraudulent emails requesting login credentials or financial details. Once victims disclose their information, criminals use it for identity theft or unauthorized transactions. Phishing remains one of the most common cybercrimes globally, and Nigeria is no exception. According to Amos (2021), phishing attacks contribute significantly to financial losses among Nigerian households and businesses, undermining trust in electronic banking services.

**Cyber-Harassment:** Cyber-harassment refers to electronically mediated and deliberate acts of intimidation or threats directed against individuals. This includes behaviors such as cyberstalking, hate messages, and online intimidation. Victims often suffer psychological trauma, reputational damage, and in severe cases, physical harm. In Nigeria, young women and journalists are particularly vulnerable to cyber-harassment, with social media platforms being common channels. Despite the Cybercrime Act of 2015 criminalizing such acts, weak enforcement mechanisms mean that many victims remain unprotected.

**Piracy:** Piracy involves the illegal reproduction and distribution of copyrighted materials such as software, movies, music, and games. Longe (2004) identifies software piracy as one of the most prevalent cybercrimes, with pirates often downloading original content, duplicating it, and reselling or uploading it online for free access. In Nigeria, piracy is rampant due to weak enforcement of intellectual property laws, high demand for cheap software and entertainment, and the widespread use of file-sharing platforms. The Nigerian Copyright Commission estimates that the country loses billions of naira annually to software and entertainment piracy, undermining the creative industries and discouraging investment.

**Cyber-Laundering:** Cyber-laundering refers to the electronic transfer of illegally obtained money to conceal its source and final destination. Criminal syndicates and corrupt officials use sophisticated techniques such as cryptocurrency transactions, online money transfer platforms, and layering schemes to obscure financial trails. In Nigeria, the Economic and Financial Crimes Commission (EFCC, 2022) has identified cyber-laundering as a growing trend, with proceeds from internet fraud often moved across borders, complicating prosecution efforts.

**Dating and Romance Scams:** Romance scams involve criminals creating fake online identities to build emotional connections with victims, usually with the intention of financial exploitation. Victims are manipulated into believing they are in a genuine relationship, often culminating in requests for money under false pretenses.

Whitty and Buchanan (2012) note that romance scams are particularly effective because perpetrators are skilled at creating trust and emotional dependency. In Nigeria, romance scams are a hallmark of "Yahoo-Yahoo" operations, with fraudsters targeting both local and foreign victims. Beyond financial losses, victims often experience shame, heartbreak, and social isolation.

**Website Cloning:** Website cloning is a relatively recent cybercrime trend where criminals create fake websites that closely resemble legitimate ones. Unsuspecting users believe they are conducting transactions on authentic platforms, when in fact, their sensitive details are being harvested by fraudsters. These cloned sites often mimic online shopping platforms, banking websites, or government portals. Victims who enter their credit card or banking details become targets of identity theft and fraudulent transactions. In Nigeria, cases of cloned bank websites have been reported, posing a major challenge for consumer protection and cybersecurity.

## Socio-Economic Development

Socio-economic development integrates both social and economic concerns into policies and initiatives aimed at improving the well-being of individuals, families, communities, and society at large. Its ultimate goal is to ensure sustained improvements in living standards, achieved by expanding a nation's stock of physical and human capital while advancing technological capabilities. In this sense, socio-economic development does not only concern material growth but also reflects positive transformations within society as a whole.

At its core, socio-economic development implies the general well-being of citizens, encompassing both political and social value judgments. It is often used as a benchmark to measure the level of economic growth in a country. Economic growth, as Lipsey (2019) explains, is a long-term phenomenon that focuses on the role of investment in raising potential income, while ignoring short-term fluctuations in national income. An increase in Gross National Product (GNP) translates into higher per capita output, which in turn improves per capita income and raises the standard of living. However, this narrow view of growth has been criticized for neglecting crucial variables such as the supply of skilled manpower, entrepreneurship, institutional frameworks, technological advancement, and the role of government policy.

In the Nigerian context, however, administrative policies over the years have failed to foster sustainable economic growth. This has hindered the transformation of the nation's dual economy, where the capitalist sector struggles to dominate the traditional sector. The persistence of

the traditional sector has contributed to widespread poverty and inequality, leaving a significant portion of the population excluded from the benefits of development.

Socio-economic factors, therefore, can be understood as the sum of social and economic conditions that determine individuals' opportunities and overall well-being. Where these conditions are absent or inadequate, strains emerge that often encourage criminality and social instability. Key socio-economic factors include poverty, unemployment, income inequality, lack of access to education and healthcare, social exclusion, and cultural constraints. As Agbamu and Irogbo (2024) emphasize, these factors collectively shape people's life chances, quality of life, and their capacity to participate meaningfully in the socio-economic and political life of their communities.

### **The Causes of Cybercrime on Socio-Economic Development**

Current researchers have shown that, cybercrime often emerges from economic factors such as poverty, unemployment and inequality, especially among youths in developing nations. In Nigeria, unemployment has been identified as a major driver pushing many young people into internet fraud as a means of survival and quick financial gain (Onyeachu, Okoro, & Ugwuoke, 2025). Other studies also revealed that, high levels of poverty and limited job opportunities tend to increase involvement in cybercrime, thereby obstructing social and economic growth (Research on Unemployment & Cybercrime, 2023).

Researchers have equally shown that, weak institutional frameworks and lack of effective cybercrime laws or enforcement mechanisms are contributory causes. In many African countries, poor regulation, low surveillance and inadequate digital infrastructure make societies more vulnerable to cybercriminal activities (Pasculli, 2020). Consequently, communities lose confidence in financial and governmental systems, which undermines trust that is necessary for social development (Asal, Asal, & Brown, 2023).

Furthermore, cultural and social influences have been demonstrated as causes of cybercrime. In West Africa, peer pressure and social acceptance of fraudulent activities, often glamorized as "hustle" or "survival strategy," have normalized cybercrime among youths (The Guardian, 2024). Studies revealed that such cultural influences reduce moral stigma against fraud, allowing individuals to rationalize their involvement in online crime (Wired, 2022).

Technological opportunities also play a major role. Researchers have shown that, the anonymity of the

internet, use of virtual private networks and access to global markets create low-risk and high-reward opportunities for cybercriminals (Wall, 2017). This makes it easier for individuals to target victims across borders without fear of immediate arrest, while local societies bear the brunt of its negative impact on development (Neprash, McGlave, Rydberg, & Henning-Smith, 2024).

### **The Effects of Cybercrime on Socio-Economic Development**

Current researchers have shown that, cybercrime has far-reaching consequences on the socio-economic stability of nations, communities and individuals. In Nigeria, cybercrime is reported to undermine economic development by discouraging foreign direct investment and raising the cost of doing business due to increased security expenditures (Onyeachu, Okoro, & Ugwuoke, 2025). They also showed that, the persistent rise in internet fraud and other related crimes contributes to the erosion of public trust in digital financial services, which limits financial inclusion and economic participation.

Other studies revealed that, cybercrime directly affects organizational growth, as companies suffer financial losses, reputational damage and business disruption. This often compels firms to divert scarce resources away from developmental projects into recovery and security measures (Neprash, McGlave, Rydberg, & Henning-Smith, 2024). As a result, social development projects, employment creation and community welfare are negatively impacted.

Researchers further demonstrated that, cybercrime creates ripple effects in society by fostering insecurity and weakening institutional trust. Communities where cybercrime thrives often experience lower levels of social cohesion and higher incidences of fraud-related conflicts (Asal, Asal, & Brown, 2023). Such outcomes obstruct cooperative social development and contribute to a climate of fear that affects both individual and community well-being.

### **Strategies for Reducing the Incidents of Cybercrime and its Effects on Socio-Economic Development**

Current researchers and policy bodies have shown that robust national strategies and legal frameworks are foundational to reducing cybercrime and protecting socio-economic development. National cybersecurity strategies that combine clear governance, incident-response capacity, and cross-agency coordination together with modernized cybercrime laws reduce legal ambiguity and improve prosecution rates, which raises the expected cost of offending (United Nations Office on Drugs and Crime,

2021; NITDA, 2021). In Nigeria, the National Information Technology Development Agency's Strategic Roadmap and Action Plan (SRAP 2021–2024) and the National Cybersecurity Policy and Strategy provide the policy architecture needed to align public agencies and private sector partners around resilience goals (NITDA, 2021).

Beyond law and policy, international standards and operational frameworks give organizations practical, evidence-based steps to prevent and mitigate attacks. Frameworks such as the NIST Cybersecurity Framework and the CIS Controls translate high-level policy into prioritized technical and management actions (Identify, Protect, Detect, Respond, Recover), which help firms and public institutions reduce exposure to the most common threats and improve recovery after incidents (NIST, 2024; CIS, 2024). Adoption of these frameworks scaled to the resource realities of small firms and local governments is repeatedly recommended in the literature as a core prevention strategy (NIST CSF 2.0; Bitsight, 2024).

Researchers also emphasize that public–private partnerships (PPPs) and international cooperation are critical for capability building and threat disruption. INTERPOL and UNODC guidance note that information-sharing, joint investigations, and technical assistance multiply law enforcement effectiveness and help close enforcement gaps across borders (INTERPOL, 2021; UNODC/INTERPOL technical briefs). In Nigeria and similar contexts, PPPs allow banks, telcos and platforms to supply threat intelligence and tools that local police often lack, improving takedown speed and evidence collection (INTERPOL Cyber Strategy Guidebook; UNODC).

Several empirical studies have examined the causes, effects and strategies for minimizing cybercrime in Nigeria and beyond, using diverse contexts, samples, and methods. In Abia State, Nzeakor, Asemota, Alu, and Amena (2023) conducted a large-scale quantitative survey of 1,104 internet users selected through multistage cluster and random sampling. Their results indicated that socio-demographic factors such as gender, age, educational attainment, and marital status significantly predicted cybercrime victimization, with males, single individuals, students, and those with medium levels of education reporting the highest vulnerability. While this study provided robust statistical evidence, it focused narrowly on victimization experiences and did not directly address perpetration or broader socio-economic impacts. The present research builds on this by examining not only vulnerability but also how perpetration and victimization combine to affect socio-economic development in Ankpa LGA.

At the institutional level, Ugwu et al. (2023) explored cyber hygiene practices among 316 students and staff at the University of Nigeria, Nsukka, using structured questionnaires. Their findings revealed that knowledge and practices varied significantly across gender, employment status, and academic discipline, thus showing how individual gaps in cyber hygiene enable cybercrime. However, the study was limited to an academic community and therefore could not be generalized to wider populations. The current research addresses this gap by extending analysis to multiple community sectors in Ankpa, thereby situating cybercrime within a broader socio-economic landscape.

Similarly, Nwosu, Adebawojo, and Ayeni (2017) moved beyond victimization to focus on perpetration intent by surveying 1,200 computer science undergraduates in Ogun State using the Intent Towards Internet Fraud Scale. They found that age, gender, and academic level significantly predicted students' likelihood to engage in fraud. While this offered valuable insights into perpetrator attitudes, the focus on computer science students meant other youth groups were excluded. The present study expands on this by examining cybercrime drivers across the entire youth population in Ankpa, including both students and non-students.

At the secondary school level, a descriptive survey in Ife Central LGA of Osun State engaged 200 students through proportionate random sampling and revealed that peer pressure, exposure to fraudulent role models, and economic hardship were the strongest influences on adolescent vccybercrime. Although important in showing the role of early socialization, the study was narrow in scope and limited to a single locality. This study addresses that limitation by exploring how these adolescent influences evolve into community-wide socio-economic challenges in Ankpa.

On the economic front, Ojeme and Adeleke (2020) surveyed 250 SMEs in Lagos and found that 68% had experienced cyber-attacks, leading to financial losses, reduced customer confidence, and disruption of online transactions. Although valuable, this urban-focused study excluded rural and semi-urban enterprises. The present research fills this gap by focusing on how cybercrime disrupts economic activities in a semi-urban locality like Ankpa.

Similarly, Adeniran (2018) adopted a mixed-methods design involving 400 bank customers across three South-West states. Using regression analysis, he showed that phishing, ATM fraud, and identity theft caused annual losses of about ₦5.2 billion and undermined trust in

digital banking, thereby discouraging financial inclusion. However, the focus on formal banking institutions excluded informal traders and microfinance users. The current study addresses this omission by capturing the experiences of such groups in Ankpa.

At a macroeconomic level, Ojeka et al. (2019) used time-series data from 2005–2017 with an ARDL model to establish a negative relationship between cybercrime and foreign direct investment inflows in Nigeria. While this highlighted the national economic implications, it did not consider how these effects trickle down to localities. This research bridges that gap by linking macroeconomic concerns to local-level realities in Ankpa.

Cross-country studies further enrich the literature. For instance, Boateng et al. (2011) surveyed 1,200 internet users in Ghana and found that cybercrime caused financial loss, eroded trust in ICT, and reduced willingness to engage in digital transactions. Although insightful, policy and enforcement contexts differ between Ghana and Nigeria. The current study therefore contextualizes these findings within Nigeria's socio-economic and policy environment.

Similarly, Kshetri (2019) used qualitative interviews with ICT experts, policymakers, and business owners in East Africa, showing that cybercrime raised business costs, reduced productivity, and diverted government resources away from development into security. While rich in qualitative insights, the lack of quantitative prevalence rates limited generalization. The present study addresses this by combining statistical prevalence with socio-economic effects in Ankpa.

At the micro level, Oladipo and Bello (2024) surveyed 400 undergraduates at the University of Ilorin and found that many students had either been victims of cybercrime or knew peers engaged in it, identifying universities as recruitment hotspots. Yet, the study focused solely on students and overlooked wider community actors. This study builds on that by including students alongside civil servants, traders, and other groups in Ankpa.

In terms of strategies, Oludayo et al. (2018) combined surveys and interviews with 210 ICT professionals in Lagos and found that capacity building for law enforcement, dedicated cybercrime courts, and public enlightenment campaigns significantly reduced cybercrime cases. Yet, the study did not consider community-level outcomes. This research adds value by examining how such measures resonate in Ankpa communities.

Finally, Bello and Hassan (2021) conducted qualitative interviews with 35 law enforcement officers in Northern Nigeria and concluded that corruption, weak enforcement,

and limited technical expertise undermined cybercrime prevention. While useful, the study overlooked community perspectives. This research fills that gap by integrating the perceptions of ordinary citizens alongside institutional actors in Ankpa.

## METHOD

This chapter outlines the methodological framework that was used to achieve the study's objectives. Specifically, it presents the research design and the population of the study. It also discusses the sample and sampling techniques, methods and instruments of data collection, ethical considerations, and the method of data analysis. Each of these components is explained in detail to demonstrate how the study was systematically conducted using a scientific approach to generate reliable findings.

## RESEARCH DESIGN

Research design refers to the systematic approaches that can be employed to address research questions (Kumar, 2015). It provides a detailed plan or blueprint of the procedures to be followed, described with such clarity and precision that another researcher could replicate the same steps and achieve similar outcomes.

For this study, the descriptive survey design was adopted. This design is particularly suited for documenting and explaining the characteristics, behaviours, attitudes, opinions, and perceptions of a given population. It enables researchers to collect, analyze, and present data in a way that captures existing realities within a community or group.

## SAMPLE SIZE AND DETERMINATION

The total sample size  $n$  was calculated earlier using Taro Yamane's formula:

$$n = \frac{N}{1+N(e^2)}$$

Where:

$n$  = sample size

$N$  = total population (266,176)

$e$  = margin of error (commonly set at 0.05 for 95% confidence)

$$n = \frac{266,176}{1+266,176(0.05^2)} = \frac{266,176}{1+665.44(0.05^2)} = \frac{266,176}{666.44} \approx 399.47 \approx 400$$

The proportionate sample size for each cluster was determined using the formula:

$$\text{Proportional Sample Size} = \frac{\text{Cluster Population}}{\text{Total Population}} \times \text{Total Sample Size}$$

**Table 3.2.** *Distribution of Population and Sample Size*

| S/N | Village/Ward   | Estimated Population | Proportional Sample Size Calculation       | Sample Size |
|-----|----------------|----------------------|--------------------------------------------|-------------|
| 1   | Ankpa Township | 39,000               | $(39,000 \times 400) \div 266,176 = 58.61$ | 59          |
| 2   | Enjema         | 34,000               | $(34,000 \times 400) \div 266,176 = 51.12$ | 51          |
| 3   | Abocho         | 31,000               | $(31,000 \times 400) \div 266,176 = 46.57$ | 47          |
| 4   | Ojoku          | 30,000               | $(30,000 \times 400) \div 266,176 = 45.09$ | 45          |
| 5   | Emere          | 28,000               | $(28,000 \times 400) \div 266,176 = 42.08$ | 42          |
| 6   | Ejinya         | 25,000               | $(25,000 \times 400) \div 266,176 = 37.59$ | 38          |
| 7   | Ikanekpo       | 24,000               | $(24,000 \times 400) \div 266,176 = 36.10$ | 36          |
| 8   | Ugbamaka-Igala | 22,000               | $(22,000 \times 400) \div 266,176 = 33.06$ | 33          |
| 9   | Okenyi         | 18,000               | $(18,000 \times 400) \div 266,176 = 27.06$ | 27          |
| 10  | Ofuloko        | 15,176               | $(15,176 \times 400) \div 266,176 = 22.80$ | 22          |
|     | <b>Total</b>   | <b>266,176</b>       |                                            | <b>400</b>  |

Source: Field Survey, 2025.

### INSTRUMENT OF DATA COLLECTION

The instruments used for data collection was:

**Questionnaire:** A structured questionnaire was designed and administered to selected respondents across various wards in Ankpa LGA. The questionnaire was divided into multiple sections, capturing information on socio-demographic characteristics, experiences with cybercrime, perceived impact on individuals, organizations, and society, and its implications for social and economic development. The items consisted of Likert-scale questions, allowing for quantitative analysis of respondents' perceptions and experiences.

### DATA ANALYSIS

The goal of data analysis is to interpret the data to reveal deep knowledge and understanding. In this process, the researcher must become a part of the environment and be aware of what is going on (Kvale & Brinkmann, 2015). For quantitative data, the researcher shall apply the use of tables, charts, graphs, percentages, frequencies and Pearson correlation coefficient. The collected data from the study were cleaned and entered into a database. Analysis and presentation of results were carried out using statistical package for social sciences (SPSS) version 20. Also, in conducting this study, strict adherence to ethical standards was maintained to ensure the dignity, privacy, and rights of all participants. Participation in the study was entirely voluntary. Respondents were informed of their right to withdraw from the study at any point without facing any form of penalty or disadvantage.

### DATA PRESENTATION AND ANALYSIS

This section covers the presentation, analysis, interpretation of data and discussion of findings. The result is based on the 378 copies of questionnaire retrieved from

the 400 copies of the questionnaire administered to the respondents.

### Socio-Demographic Characteristics of Respondents

The first part of the results of the study presented and analyzed the socio-demographic characteristics of the study participants which include: sex, occupation and educational level. This is depicted in Table 4.1

Table 4.1 presents the socio-demographic characteristics of the 378 respondents sampled in the study. The socio-demographic characteristics of the respondents in this study provide essential context for understanding their experiences and perceptions, particularly regarding the effect of cybercrime on social development. The data was derived from a field survey conducted among 378 respondents in Ankpa LGA.

The age distribution of respondents reveals a youthful population. The largest age group was 25–30 years, with 110 respondents (29.1%), followed by the 18–24 years group at 79 (20.9%). This indicates that over half of the respondents (50.0%) were under the age of 30. Other age groups included 31–34 years (18.0%) and 35–40 years (16.9%). A smaller proportion of respondents were between 41–44 years (7.1%), 45–50 years (5.0%), and those over 51 years formed the least represented category, with only 11 respondents (2.9%). This age profile suggests a predominantly young and potentially tech-savvy population, which is relevant when exploring issues related to cybercrime.

The occupational profile showed that students formed the largest group, 106 (28.0%), suggesting a high level of educational engagement or youth presence. Wage-employed individuals followed with 91 (24.1%), while those involved in farming (72 or 19.0%) and business

**Table 4.1.** *Percentage Distribution of Socio-demographic Characteristics of Respondents (N = 378)*

| Variables                | Categories    | Frequency (N = 378) | Percentage (%) |
|--------------------------|---------------|---------------------|----------------|
| <b>Age Bracket</b>       | 18 – 24 years | 79                  | 20.9           |
|                          | 25 – 30 years | 110                 | 29.1           |
|                          | 31 – 34 years | 68                  | 18.0           |
|                          | 35 – 40 years | 64                  | 16.9           |
|                          | 41 – 44 years | 27                  | 7.1            |
|                          | 45 – 50 years | 19                  | 5.0            |
|                          | Over 51 years | 11                  | 2.9            |
| <b>Educational Level</b> | No Education  | 8                   | 2.1            |
|                          | Primary       | 34                  | 9.0            |
|                          | Secondary     | 117                 | 30.9           |
|                          | Tertiary      | 219                 | 57.9           |
| <b>Occupation</b>        | Student       | 106                 | 28.0           |
|                          | Wage Employed | 91                  | 24.1           |
|                          | Business      | 68                  | 18.0           |
|                          | Farming       | 72                  | 19.0           |
|                          | Unemployed    | 41                  | 10.9           |

Source: Field Survey, 2025.

(68 or 18.0%) also had substantial representation. The unemployed made up the smallest group with 41 (10.9%). This occupational distribution underscores the diverse economic engagement in Ankpa LGA and may influence varying levels of cybercrime vulnerability or awareness.

The data on educational level reveals a predominantly educated population. A majority of respondents, 219 (57.9%), had tertiary education, while 117 (30.9%) had

completed secondary school. Primary education holders were 34 (9.0%), and only 8 respondents (2.1%) had no formal education. The high level of educational attainment suggests a well-informed population that is more likely to engage with digital technology, and consequently, be affected by or knowledgeable about cybercrime and its social implications.

### Analysis of Data on the Research Objectives

**Research Objective 1:** Identify the causes of cybercrime as perceived by residents of Ankpa LGA of Kogi State.

**Table 4.2.** *Causes of Cybercrime as Perceived by Residents of Ankpa LGA (N = 378)*

|   | Measures                                                                                | SA             | A              | U             | D            | SD           |
|---|-----------------------------------------------------------------------------------------|----------------|----------------|---------------|--------------|--------------|
| 1 | High unemployment contributes to the rise of cybercrime in Ankpa                        | 152<br>(40.2%) | 128<br>(33.9%) | 45<br>(11.9%) | 31<br>(8.2%) | 22<br>(5.8%) |
| 2 | Poverty and low standard of living drive many youths into cybercrime                    | 161<br>(42.6%) | 133<br>(35.2%) | 40<br>(10.6%) | 26<br>(6.9%) | 18<br>(4.8%) |
| 3 | Peer influence and the quest for quick wealth are major causes of cybercrime            | 145<br>(38.4%) | 129<br>(34.1%) | 54<br>(14.3%) | 29<br>(7.7%) | 21<br>(5.6%) |
| 4 | Weak enforcement of cyber laws encourages the growth of cybercrime                      | 138<br>(36.5%) | 141<br>(37.3%) | 47<br>(12.4%) | 30<br>(7.9%) | 22<br>(5.8%) |
| 5 | Poor digital literacy and ignorance among citizens make them both offenders and victims | 132<br>(34.9%) | 136<br>(36.0%) | 56<br>(14.8%) | 32<br>(8.5%) | 22<br>(5.8%) |
| 6 | Corruption and weak institutions increase cybercrime activities                         | 149<br>(39.4%) | 130<br>(34.4%) | 49<br>(13.0%) | 28<br>(7.4%) | 22<br>(5.8%) |

Source: Field Survey, 2025.

The data presented in Table 4.3 reveals the perceived causes of cybercrime in Ankpa Local Government Area. A significant proportion of respondents (40.2% strongly agree and 33.9% agree) identified unemployment as a key

factor driving individuals into cybercrime. This indicates that the lack of gainful employment opportunities among youths is pushing many towards fraudulent activities as an alternative means of livelihood.

Similarly, poverty and low standard of living were strongly emphasized, with 42.6% strongly agreeing and 35.2% agreeing that economic hardship compels youths into cybercrime. This suggests that poor economic conditions act as a major motivator for illicit online activities, as individuals seek quick avenues to escape poverty.

The findings also highlight the role of peer influence and the quest for quick wealth, with 38.4% strongly agreeing and 34.1% agreeing. This underscores the growing social pressure among young people to pursue material success through shortcuts, often inspired by peers who flaunt wealth acquired through cybercrime.

Another major cause identified was the weak enforcement of cyber laws, as 36.5% strongly agreed and 37.3% agreed that inadequate punishment and regulatory lapses encourage the persistence of cybercrime. Respondents noted that the absence of strong deterrents emboldens offenders to continue exploiting loopholes in the system.

Furthermore, poor digital literacy and ignorance were also considered important, with 34.9% strongly agreeing and 36.0% agreeing that lack of knowledge exposes individuals both as victims and perpetrators. This implies that inadequate awareness of online risks makes residents vulnerable to scams while also fostering careless or uninformed involvement in cybercrime.

Lastly, corruption and weak institutions were reported as significant enablers, with 39.4% strongly agreeing and 34.4% agreeing. Respondents suggested that institutional weakness and corrupt practices prevent effective monitoring and prosecution of offenders, thereby creating an enabling environment for cybercrime to thrive.

**Research Objective 2:** Explore the effects of cybercrime on the socio-economic development of Ankpa LGA of Kogi State.

**Table 4.3.** *Effects of Cybercrime on the Socio-economic Development of Ankpa LGA (N = 378)*

| S/N | Measures                                                                       | SA             | A              | U             | D            | SD           |
|-----|--------------------------------------------------------------------------------|----------------|----------------|---------------|--------------|--------------|
| 1   | Cybercrime discourages both local and foreign investment in Ankpa.             | 141<br>(37.3%) | 133<br>(35.2%) | 49<br>(13.0%) | 32<br>(8.5%) | 23<br>(6.1%) |
| 2   | It reduces trust in digital platforms and online financial services.           | 147<br>(38.9%) | 136<br>(36.0%) | 42<br>(11.1%) | 29<br>(7.7%) | 24<br>(6.3%) |
| 3   | Cybercrime contributes to revenue loss for businesses and institutions.        | 139<br>(36.8%) | 131<br>(34.7%) | 55<br>(14.6%) | 30<br>(7.9%) | 23<br>(6.1%) |
| 4   | It increases unemployment by discouraging organizational growth.               | 128<br>(33.9%) | 135<br>(35.7%) | 56<br>(14.8%) | 34<br>(9.0%) | 25<br>(6.6%) |
| 5   | The economic cost of cybercrime slows overall development of Ankpa LGA.        | 144<br>(38.1%) | 129<br>(34.1%) | 48<br>(12.7%) | 33<br>(8.7%) | 24<br>(6.3%) |
| 6   | Cybercrime undermines government revenue through tax evasion and online fraud. | 138<br>(36.5%) | 132<br>(34.9%) | 54<br>(14.3%) | 31<br>(8.2%) | 23<br>(6.1%) |

Source: Field Survey, 2025.

The results in Table 4.3 reveal that respondents perceive cybercrime as having far-reaching negative effects on socio-economic development in Ankpa Local Government Area. A large proportion (37.3% strongly agree and 35.2% agree) reported that cybercrime discourages both local and foreign investment. This suggests that fear of fraud and lack of trust in the business environment may be hindering economic inflow and business expansion.

Trust in digital platforms and online financial services was also significantly undermined, with 38.9% strongly agreeing and 36.0% agreeing to this measure. This indicates that cybercrime erodes confidence in financial technology and e-commerce, which are essential drivers of modern economies. Regarding organizational losses, 71.5% (SA and A combined) observed that cybercrime contributes to

revenue losses for businesses and institutions. This aligns with the wider perception that digital attacks and scams disrupt operations, reduce profitability, and sometimes force enterprises to close down.

Unemployment is another indirect effect, with 69.6% agreeing that organizational growth is stunted by cybercrime. When businesses suffer financial setbacks, their ability to employ and retain staff diminishes, thereby worsening the unemployment challenge in Ankpa. Furthermore, 72.2% of respondents believe that the economic cost of cybercrime slows down overall development in the area. This finding shows that the consequences are not only limited to individuals and firms but also extend to the collective progress of the local government.

Finally, cybercrime's impact on public finance was acknowledged by 71.4% of respondents, who reported that government revenue is undermined through tax evasion and online fraud. This directly weakens the fiscal capacity of government to deliver essential services and invest in community development.

**Table 4.4.** *Strategies for Reducing the Incidence of Cybercrime and its Effects on Socio-economic Development of Ankpa LGA (N = 378)*

| S/N | Measures                                                                           | SA             | A              | U             | D            | SD           |
|-----|------------------------------------------------------------------------------------|----------------|----------------|---------------|--------------|--------------|
| 1   | Government should strengthen cyber laws and ensure strict enforcement.             | 152<br>(40.2%) | 131<br>(34.7%) | 44<br>(11.6%) | 28<br>(7.4%) | 23<br>(6.1%) |
| 2   | Public awareness and digital literacy campaigns will reduce cybercrime.            | 148<br>(39.2%) | 137<br>(36.2%) | 47<br>(12.4%) | 28<br>(7.4%) | 18<br>(4.8%) |
| 3   | Creating more job opportunities will reduce youths' involvement in cybercrime.     | 156<br>(41.3%) | 129<br>(34.1%) | 42<br>(11.1%) | 30<br>(7.9%) | 21<br>(5.6%) |
| 4   | Collaboration between law enforcement agencies and community leaders is essential. | 144<br>(38.1%) | 135<br>(35.7%) | 49<br>(13.0%) | 28<br>(7.4%) | 22<br>(5.8%) |
| 5   | Investing in cybersecurity infrastructure will minimize cybercrime.                | 139<br>(36.8%) | 128<br>(33.9%) | 56<br>(14.8%) | 32<br>(8.5%) | 23<br>(6.1%) |
| 6   | Religious and traditional institutions can play a role in discouraging cybercrime. | 134<br>(35.4%) | 127<br>(33.6%) | 59<br>(15.6%) | 33<br>(8.7%) | 25<br>(6.6%) |

Source: Field Survey, 2025.

The findings in Table 4.5 highlight community perceptions on viable strategies for minimizing cybercrime in Ankpa Local Government Area. A strong majority (40.2% strongly agree, 34.7% agree) support strengthening and enforcing cyber laws, underscoring the widespread belief that weak enforcement enables cybercrime to thrive. Public sensitization was also considered vital, with 75.4% (SA + A) emphasizing the role of awareness and digital literacy campaigns in reducing susceptibility to online fraud. Respondents linked low awareness levels to victimization and the ease with which cybercriminals exploit others.

Employment generation emerged as the most endorsed strategy, with 41.3% strongly agreeing and 34.1% agreeing that job opportunities would curb youth involvement. This reflects the earlier finding that unemployment and poverty drive many young people into fraudulent activities. On community-centered solutions, 73.8% of respondents agreed that collaboration between law enforcement agencies and local leaders is essential. They noted that such cooperation improves intelligence gathering, trust, and the willingness of residents to report cybercrime cases.

A significant proportion (70.7%) also supported investments in cybersecurity infrastructure, stressing the need for better tools to detect, track, and prevent cyber-attacks. Similarly, 69% endorsed the role of religious and traditional institutions in discouraging cybercrime by

**Research Objective 3:** Examine the strategies for reducing the incidence of cybercrime and its effects on socio-economic development of Ankpa LGA of Kogi State.

reinforcing moral values and condemning the pursuit of fraudulent wealth.

### TEST OF HYPOTHESIS

Test of Hypothesis below was formulated and tested at 0.05 level of significance.

**H<sub>0</sub>:** Strategies for minimizing cybercrime does not reduce the effects of cybercrime on socio-economic development in Ankpa LGA.

**H<sub>1</sub>:** Strategies for minimizing cybercrime reduce the effects of cybercrime on socio-economic development in Ankpa LGA.

**Decision Rule:** When P value is greater than the significant level of 0.05, the stated null hypothesis is accepted.

### Decision-Making and Conclusion

The regression analysis investigates whether strategies such as public awareness, provision of more job opportunities, collaboration between law enforcement agencies and community leaders, and the role of religious and traditional institutions significantly reduce the effects of cybercrime on socio-economic development in Ankpa LGA. The results reveal that public awareness ( $B = 2.103$ ,  $p = 0.000$ ), job opportunities ( $B = 1.044$ ,  $p = 0.000$ ), and collaboration between law enforcement agencies and community leaders ( $B = 3.032$ ,  $p = 0.000$ ) are statistically significant predictors, since their p-values are below the

**Table 4.7.** Linear Regression Result Showing Whether Strategies for Minimizing Cybercrime does not Reduce the Effects of Cybercrime on Socio-Economic Development in Ankpa LGA.

| Model |                                              | Unstandardized Coefficients |            | Standardized Coefficients | T      | Sig. |
|-------|----------------------------------------------|-----------------------------|------------|---------------------------|--------|------|
|       |                                              | B                           | Std. Error | Beta                      |        |      |
| 1     | (Constant)                                   | 1.423                       | .097       |                           | 14.606 | .000 |
|       | Public awareness                             | 2.103                       | .047       | .137                      | 22.179 | .000 |
|       | More job opportunities                       | 1.044                       | .044       | .063                      | 12.018 | .000 |
|       | Law enforcement agencies & community leaders | 3.032                       | .050       | .039                      | 13.647 | .000 |
|       | Religious and traditional institutions       | -.009                       | .045       | -.012                     | -.196  | .844 |

Source: Field Survey, 2025.

0.05 threshold. This implies that these strategies play a meaningful role in minimizing the effects of cybercrime on development. However, the role of religious and traditional institutions ( $B = -0.009$ ,  $p = 0.844$ ) does not significantly predict reduction in cybercrime, as its p-value is far above 0.05.

Based on these findings, we reject the null hypothesis and conclude that strategies for minimizing cybercrime particularly public awareness, job creation, and law enforcement collaboration do reduce its effects on socio-economic development in Ankpa LGA. Nonetheless, religious and traditional institutions appear to have little or no measurable impact in this regard.

## DISCUSSION OF FINDINGS

This study examined the sociological implications of cybercrime on socio-economic development in Ankpa Local Government Area of Kogi State. It was guided by four objectives and four hypotheses, with data drawn from 378 respondents through questionnaires. The findings are discussed here in line with each objective and compared with related literature.

The analysis revealed that cybercrime in Ankpa LGA is strongly associated with socio-economic factors such as unemployment, poverty, peer influence, weak institutions, and poor digital literacy. A majority of respondents (73.3%) affirmed that high unemployment and poverty are key drivers of cybercrime among youths in the community. This finding corroborates Eze and Oladipo (2021), who identified unemployment and low standard of living as the most persistent socio-economic conditions fueling cybercrime in rural Nigerian settings. Similarly, Abubakar and Sulaiman (2021) stressed that peer pressure and the quest for quick wealth encourage youths to adopt cybercrime as a survival strategy in regions with limited opportunities.

The study also confirmed that cybercrime has significant adverse effects on both social and economic development

in Ankpa. Over 72% of respondents agreed that it discourages investment, reduces trust in digital platforms, and contributes to unemployment and business collapse. These findings align with Adewale and Daramola (2022), who found that cybercrime undermines the growth of local economies by weakening organizational trust and diverting resources into security. Similarly, Ndukwe and Ibe (2022) noted that Nigerian SMEs are disproportionately affected by digital fraud, leading to productivity loss and reduced competitiveness.

The findings also demonstrated that strategies for minimizing cybercrime must combine legal, educational, economic, and community-based approaches. A majority of respondents supported strengthening cyber laws, creating more jobs, public awareness campaigns, and collaboration between security agencies and community leaders. These results are supported by Etim and Salami (2020), who argued that multi-stakeholder approaches involving both state institutions and community actors are the most effective in addressing cyber insecurity. Similarly, Chukwuma and Ejiogu (2022) recommended combining digital literacy with youth empowerment initiatives to reduce cybercrime among marginalized groups.

The hypothesis examined whether cybercrime significantly affects socio-economic development. The regression results confirmed this, with over 45% of the variance in economic development explained by cybercrime effects, consistent with Ndukwe and Ibe (2022) and Adewale and Daramola (2022).

## CONCLUSION

The study concludes that cybercrime has become a pervasive challenge in Ankpa LGA, undermining both social trust and economic development. Structural drivers such as unemployment, poverty, weak institutions, and poor digital literacy fuel its persistence, while its consequences range from financial loss and business collapse to psychological trauma and community distrust.

The findings also reveal that while cybercrime is highly prevalent and underreported, it can be effectively reduced through combined approaches strengthening legal frameworks, empowering youths economically, improving digital literacy, and enhancing collaboration between state agencies and community actors. The conclusion underscores that cybercrime is not merely a technological issue but a sociological problem with deep roots in socio-economic inequalities.

## RECOMMENDATIONS

Based on the findings, the following recommendations are made:

- a. The government should ensure the strict implementation of existing laws such as the Cybercrime Act (2015) while providing law enforcement agencies with modern digital forensic tools and training.
- b. Continuous public education is needed to equip residents with knowledge about safe online practices, fraud prevention, and reporting mechanisms.
- d. Law enforcement agencies should work closely with traditional rulers, community leaders, and civil society to build trust, improve reporting, and curb cybercrime locally.
- e. Governments at state and local levels should strengthen ICT systems, encourage secure online transactions, and partner with ISPs and financial institutions to improve cyber resilience.

## REFERENCES

1. Aghatise, E. (2016). Cybercrime and the challenge of cyber security in Nigeria. *International Journal of Advanced Research in Computer Science*, 7(6), 121–128.
2. Aminu, A., Hamzat, A., & Haruna, I. (2015). Cybercrime and national security in Nigeria. *Journal of Law and Cyber Studies*, 3(1), 45–59.
3. Asante, K. (2020). Cybercrime prevention strategies and investment protection in Ghana. *African Journal of Information Systems*, 12(3), 201–219.
4. Beck, U. (1992). *Risk society: Towards a new modernity*. Sage Publications.
5. Bell, D. (1998). *The coming of post-industrial society*. Basic Books.
6. Bello, S., & Hassan, M. (2021). Law enforcement challenges in combating cybercrime in Northern Nigeria. *Nigerian Journal of Criminology*, 15(2), 88–104.
7. Business Day Newspaper. (2022). Rising cybercrime losses and economic implications. *Business Day Nigeria*.
8. Center for Strategic and International Studies. (2024). *The economic impact of cybercrime*. CSIS.
9. Chukwuma, E., & Ejiogu, A. (2022). Digital literacy and youth empowerment as tools against cybercrime. *Journal of African Development Studies*, 9(1), 55–71.
10. Etim, E., & Salami, A. (2020). Multi-stakeholder approaches to cyber security in Nigeria. *Journal of Security Studies*, 6(2), 101–117.
11. Fatoki, O. (2023). Internet usage and cybercrime vulnerability in developing economies. *Journal of Digital Society*, 5(1), 33–49.
12. Federal Bureau of Investigation. (2024). *Internet crime report 2023*. FBI.
13. Guardian Newspapers. (2022, August 3). Africa records sharp rise in cybercrime. *The Guardian Nigeria*.
14. Inge, L., & Lawrence, T. (2021). Cybercrime as a global security threat. *International Journal of Cybersecurity*, 4(2), 66–82.
15. King, M., & McCarty, W. (2009). Risk society and contemporary criminology. *British Journal of Criminology*, 49(4), 567–585.
16. Maitanmi, O., Ogunlere, S., & Adegoke, O. (2013). Cybercrime and Nigeria's economic development. *Journal of Economics and Development Studies*, 1(2), 1–15.
17. Ndubueze, P. (2020). Measuring the impacts of cybercrime on organizations. *Journal of Cyber Policy*, 3(1), 90–105.
18. NITDA. (2021). *National information technology development agency strategic roadmap and action plan (2021–2024)*. NITDA.
19. Nwezeh, K., & Shittu, A. (2021). Youth involvement in cybercrime in Nigeria. *African Youth Studies Journal*, 8(1), 44–60.
20. Okonkwo, I., & Ibrahim, S. (2021). Moral institutions and cybercrime control in Nigeria. *Sociology and Development Review*, 5(2), 120–137.
21. Oluwafemi, A. (2021). Cybercrime and economic indices in Nigeria. *Journal of Social Research*, 14(3), 211–228.
22. Sorunke, O. (2021). Cybersecurity threats and vulnerabilities in Nigeria's digital space. *Journal of*

- Information Security and Applications*, 15(3), 233–248.
23. Statista. (2024). *Number of internet users worldwide from 2005 to 2023*. Statista Research Department.
  24. Sule, A., Musa, B., & Ibrahim, S. (2021). Emerging trends in cybercrime and ICT misuse. *Journal of Computer and Information Security*, 8(4), 98–113.
  25. Uche, E., & Nwachukwu, L. (2020). Online fraud and public trust: Implications for socio-economic growth in Nigeria. *International Review of Social Sciences and Humanities*, 11(1), 67–79.
  26. Ugah, J., Salami, R., & Yusuf, B. (2024). Insider threats and organizational cybercrime in Nigeria. *African Journal of Criminology*, 16(2), 144–161.
  27. Umana, E., Akpan, I., & Effiong, A. (2024). Cybercrime typologies and their implications in Nigeria. *Nigerian Journal of Sociology*, 20(1), 88–104.
  28. United Nations Office on Drugs and Crime. (2021). *Comprehensive study on cybercrime*. UNODC.
  29. Uzoho, J. (2019). Fraud, cybercrime, and monetary loss in Nigeria. *West African Journal of Criminology*, 11(2), 133–150.

**Cite this article:** Oluwatoyin Adewale SHEYİNDEMI, Thomas Imoudu GOMMENT. *Effects of Cybercrime on the Socio-Economic Development of Ankpa Local Government Area of Kogi State, Nigeria. International Journal of Research in Medical and Clinical Sciences*. 2026; 3(1): 01-17.

**Copyright:** © 2026. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.