CYBERCRIME: CURRENT TRENDS AND PREVENTIVE STRATEGIES IN NIGERIA

Adamu AHMED
Department of Sociology, Gombe State University, Gombe-Nigeria
Email: neoahad@gmail.com Phone No: +2347032233339

Arafat IBRAHIM
Department of Sociology, Gombe State University, Gombe-Nigeria
Email: arafat200912@gsu.edu.ng Phone No: +2348030713639

Ali Garba KOLO
Department of Sociology, Yobe State University, Damaturu-Nigeria
Email: aligarbakolo@ysu.edu.ng Phone No: +2348034135628

Abstract

Cybercrime in Nigeria has escalated sharply due to rapid digitalization, costing over $500 million annually and threatening national security, particularly for SMEs and critical infrastructure. This paper examines current trends, determinants, victim and perpetrator profiles, legal frameworks, and preventive strategies through a conceptual review of secondary sources, including government reports and academic literature. Findings reveal that poverty, unemployment, weak enforcement of the Cybercrimes Act 2015, and inadequate digital literacy drive cybercrime, with young males (18–34) as primary perpetrators and individuals, SMEs, and banks as main victims. Enforcement is hindered by resource constraints, outdated technology, corruption, and limited international cooperation. The study concludes that cybercrime remains a severe threat requiring a unified multi-layer response. Recommendations include revising the Cybercrimes Act to address emerging threats, establishing dedicated cybercrime courts, enhancing law enforcement capacity and tools, and expanding public awareness campaigns to foster a culture of cybersecurity.

Keywords: Cybercrime, Nigeria, Phishing, Financial Fraud, and Cybersecurity

Introduction

The past few years have seen a significant rise in cybercrime in Nigeria, an issue that is rapidly becoming more essential to address within the country. The rapid development of digital technologies and the widespread access to the internet have unlocked new possibilities of growth, but have also brought to light new forms of misuse on the net. Cybercrime in Nigeria is a vice that takes different forms, such as fraud, identity theft, phishing, cyberbullying, and more serious crimes like hacking into government or corporate databases. The Nigerian cybercrime ecosystem is particularly infamous for its participation in business scams with global appeal, such as Business Email Compromise (BEC) and advance-fee fraud (also known as "419 fraud") (Okechukwu & Ihuoma, 2022). The economic cost of cybercrime in Nigeria is monumental. According to a report by the Nigerian Financial Intelligence Unit (NFIU) in 2022, Nigeria loses in excess of $500 million every year to diverse cybercrimes, including financial fraud and Internet scams (BusinessDay, 2022). On businesses, there

is so much for them to lose, including businesses in Nigeria that have suffered financial losses, damage to their reputation, and loss of consumer confidence as a result of cyberattacks. Small and Medium Enterprises (SMEs), the driving force behind the Nigerian economic community, are at a significant risk as they frequently have limited budgets and experience in adopting high-level cybersecurity protection. Furthermore, cybercrime has contributed to social problems through the enabling of online harassment, fraud, and the dissemination of rumours that damage the public trust in digital environments.

The rising rate of cybercrime in Nigeria could be traced to many factors, ranging from unemployment, lack of adequate cybersecurity education, and the digital divide between the rural and urban areas. Large numbers of Nigerians, especially young people, are driven into cybercrime by poverty and the promise of quick money. This, in addition to the low probability of arrest or punishment for cybercriminals, has enabled a robust underground economy of illicit endeavors (Akpan, 2021). Addressing criminality in cyberspace is crucial to Nigeria's national security and economic advancement. Cybercrime presents potent threats to the country's cyber ecosystem, including government agencies and other private sector practitioners. Cyber-attacks could cripple essential sectors of the economy, including banking, health care, and telecoms, that are indispensable for the operation of the Nigerian state. For example, if ransomware is used to compromise banks, financial information may be stolen, thus destroying the financial system (Nigerian Communications Commission, 2022). More so, international fraud syndicates involving Nigerian cybercriminals have impinged on Nigeria's global image, affecting foreign exchange relationships and investment, (Imam, 2023).The growing level of sophistication of cybercrime represents a severe challenge to the vital national infrastructure from a security point of view. Cyberattacks on governmental networks can pose a threat to the proper functioning of essential public services, with an extensive impact on governance and national security. Instead, targeting the power grid, transportation, or water networks could potentially bring the disruption, civil unrest, and economic misfortune on much larger scales. Moreover, cybercrime in Nigeria can also worsen regional and worldwide insecurity, given that cybercriminal organizations generally function across borders and work together with criminal syndicates from the international scene (World Economic Forum, 2023).

Economy-wise, the economic impact of computer crime goes beyond the prevailing value lost. The financial and reputational risks of such security incidents can make businesses hesitant to work in or with Nigeria. The effect of this collective action is a lack of trust in the country's digital ecosystem, thus stunting the growth of the digital economy. Cybercrime represents a misallocation of national resources, with the government spending a lot to fight cybercrime and improve its cybersecurity infrastructure. Failure to effectively address the vicious cycle of cybercrime will silently sabotage the efforts of the country in its quest to transition to a vibrant and secure digital economy (Okechukwu & Ihuoma, 2022). The discussion will be base on the following: Global Perspectives on Cybercrime, Global Preventive Measures, Types of Cybercrime in Nigeria, The Profile of Cyber-criminals and Victims, Vulnerable Populations, Technological Factors Facilitating the Rise of Cybercrime, Determinants of Cybercrime in Nigeria, Preventive Measures Against Cyber Crime in Nigeria, Challenges in Combating Cybercrime, Conclusion and Recommendations

Global Perspectives on Cybercrime: Trends and Preventive Measures

Cybercrime has evolved as a threat to global level and has been victimising countries, corporations, governments, and people all around the world. Rapid technological development, coupled with the growing reliance of individuals and societies on the internet for communication, transactions, and services have led to more sophisticated and pervasive cybercrimes. Internationally, there exist many types of cybercrime, such as fraud, identity theft, hacking, phishing, and ransomware. The financial and social impact of cybercrime is enormous. That is why cybersecurity becomes a concern of national security authorities as well as law enforcement bodies across the world.

Cybercrime Epidemiology In the last decade, the prevalence of cybercrime has risen significantly, with new trends becoming apparent. One of the biggest trends is the spike in ransomware. (2024), ransomware attacks have produced billions of dollars in damages across the world by themselves, and ransom payments could amount to as much as $20 billion by 2025. Cyber-criminals frequently demand money in cryptocurrency, which is beyond the authorities' capacity to follow as it changes hands, and bring the guilty parties to justice. It is not only the financial impact caused by such attacks, but also that they disrupt important services such as healthcare, banking, and infrastructure (Graham & McKew, 2020). Another emerging fear is the advent of AI and machine learning in the world of cybercrime. These features allow attackers to scale crimes, automating the attacks and making them more efficient and wider-reaching. AI-supported attacks are, for example, automated phishing, deepfake technology to fake videos or voice recordings, and AI-based attacks that target weaknesses in systems (Davenport, 2022). Such improvements in the field of technology are making it very challenging for conventional cybersecurity practices to keep up with the newer strategies of hackers. Furthermore, the connectivity trend effects the devices such as the Internet of Things (IoT). The more devices that get connected, the more hackers will be hacking weaknesses in those devices in order to get into bigger networks as well. For example, adversaries have been able to leverage IoT devices as a means to launch larger-scale attacks, particularly in industries like smart homes, health care, and critical infrastructure (Baker, 2021).

Global Preventive Measures

The article addresses how countries around the world have dealt with and tried to prevent cybercrime. The Budapest Convention on Cybercrime, adopted by the Council of Europe in 2001, is one important international initiative to combat cybercrime. The Convention, also referred to as the "Cybercrime Convention", is intended to harmonize laws, enhance international cooperation, and set procedural rules for investigating and prosecuting offenses related to the use of computers and computer networks (Council of Europe, 2021). The convention has so far been signed by more than 65 countries, representing one of the broadest international approaches for fighting cybercrime. As well as international agreements, regional and national bodies have brought in cybersecurity tactics in an attempt to reduce cybersecurity incidents. The European Union's General Data Protection Regulation (GDPR), which became law in 2018, is one such law that the company has cited as playing a crucial part in regulating data protection and making sure companies are using solid cybersecurity to protect consumers' data. Security breaches and accountability: an impact of one Article in the General Data Protection Regulation (GDPR) additional benefits of the GDPR has been

its attempt to bring cybersecurity breaches to deal with and hold them responsible if failing to protect sensitive data (European Commission, 2020).

So too has the US put measures in place to fight cybercrime, notably the creation in 2018 of the Cybersecurity and Infrastructure Security Agency (CISA). The agency is in charge of guarding critical infrastructure from cyber threats and working with state and local governments to boost the cybersecurity defenses nationwide. And U.S. DO) Moreover, there are sting operations such as "Operation Disruptor" which targets transnational drug trafficking organizations utilizing the dark web to conduct cyber crime (U.S. Department of Justice, 2021). Private companies and non-governmental organizations are also dedicating more resources to cybersecurity technologies to protect their properties from cyber attacks. A lot of companies use machine learning and AI to pinpoint anomalies, to react in real time to threats, and to actually go on the offense with regard to assessing risks and threats. Moreover, worldwide public education offensives have taken place that have warned people about the best practices to follow (e.g., having strong passwords, not clicking on strange links) to stay safe with technology (Baker, 2021).

Cybercrime has continued to spread in Nigeria, ravaging individuals and businesses, as well as the general economy. With more and more people turning to digital platforms for communication, banking & socialization, cybercriminals are finding the silver lining to take advantage of these vulnerabilities. This section examines the incidence and varieties of cybercrime in Nigeria, and offers statistics and cases to illustrate them. Cybercrime has grown at an alarming rate in Nigeria in the last decade. In Nigeria, the global information shows that approximately 74.8 per cent of Nigerian internet users suffered internet-based attacks such as bank fraud, identity theft, personal information, and various online trade actions. This figure reiterates the chilling reality of cybercrime in Nigeria and how it affects the general Nigerian society (Davenport, 2022).Then there's the monetary cost of cybercrime, which is even scarier. A study that observed the impact of cybercrimes on sustainable development in Nigerian banks found that phishing and ATM skimming had a negative and significant influence on the sustainable development of deposit money banks in Nigeria. These results underscore the financial impact that cybercrime has on the banking sector and the national economy in general.

Types of Cybercrime in Nigeria

Phishing is still an epidemic in Nigeria. Fraudsters use fake emails, websites, or texts to deceive people into providing personal information, such as passwords and credit card numbers. In 2022, A survey of computer users in Nigeria found that 7 percent of respondents had been victims of phishing attacks, while the company reported over 500,000,000 malicious attempts being blocked by their anti-phishing service in 2022. (Davenport, 2022).

Identity theft now constitutes a major threat in Nigeria's online community. Cybercriminals use different approaches, from phishing to data breaches, to steal personal information and engage in criminal activities. One such instance was an unidentified Lagos-based civil servant who allegedly fell victim to a bank fraudulent

transaction of over N3million which her bank details were gotten through a fake bank phishing. Test Your Anti-Phishing IQ: How to Identify Phishing Scam Emails as Real (Baker, 2021).

Financial and securities fraud are a variety of illegal schemes whose purpose is to defraud people of their money and property. In Nigeria, they include ATM skimming, online banking fraud, and investment cheats." In our own contextualising study with Nigerian banks, the result is not too different; phishing scams and ATM skimming also had a significant negative impact on the sustainable development of deposit money Banks in Nigeria. (Davenport, 2022).

Advance-Fee Fraud (419 Scams)

419 is an old timer in Nigeria concerning advance-fee fraud. This fraud includes offering victims a large amount of money in exchange for an upfront payment that the scammer says is required to obtain the larger sum. But when the victim makes a payment, the scammer vanishes, and the millions never arrive. Although this type of fraud is being fought aggressively, it is still a big threat, especially for online communications, such as emails, friends, and social media.(Davenport, 2022).

Sextortion

Sextortion is a cybercrime in which the offender blackmails the victim for money or other favours under threat to release material of a sexual nature that would humiliate the victim. This type of crime has become trendy in Nigeria, with people using fake social media identities to trap their victims. After the trust is built, scammers go on to persuade victims to send them risqué snaps, which are then employed for blackmail. Taking Sextortion to Task. The proliferation of sextortion has had tragic side effects, with victims committing suicide because they couldn't bear the emotional and psychological toll. (Baker, 2021)

Impact on Individuals and Institutions

In Nigeria, the impact of cybercrime goes beyond financial losses." Victims frequently experience psychological trauma, loss of privacy, and decreased feelings of self-esteem. The implications for organizations, and in the case o f financial institutions, can include damage to their reputation, loss of customer trust, and financial hit. The combined effects of these multiple impacts stand in the way of Nigeria's digital economy progress and development" (Baker, 2021)

The Profile of Cyber-criminals and Victims: Understanding Who and Who Is Harmed

Demographic profiling of cybercriminals and victims is essential in devising programs and devising the means of curbing cybercrime. This subsection discusses the profile of cybercriminals and victims based on age, sex, education, and socio-economic status. Considering these demographics can allow us to create tailor-made interventions and preventative measures towards the growing menace of cybercrime.

Cybercriminals: Who Are They?

Cyber Scammers are a mixed bag, but we can learn a little about the people behind the scams using some data. One key characteristic is age. Many cybercriminals are young, and research has found that a large proportion of those who commit cybercrimes are 18 to 34 years old (McGuire, 2022). Some of this is a result of the greater comfort related to digital technologies experienced by younger generation users, who take to online channels effortlessly. Younger generations who grew up with the internet also like its anonymity and may consider cybercrimes less dangerous than their real-world equivalent.

Demographics Gender also affects those who commit cybercrime. Although cybercrime has been a male-dominated activity in the past, the story seems to be changing, and female cybercriminals are significantly contributing to the menace. Research reveals men are still the predominant sex of cybercriminals, with around 80% of known offenders being male (Henson, 2020). But the increase of female participation is significant in some roles, such as online fraud and cyberbullying (Burgess & Rege, 2021). The trend indicates that as women are getting more and more addicted to digital activities, the number of women who are participating in the cybercrime is also increasing.

Education and income differences also play an important role in the tendency toward cybercrime. The majority of cybercriminals are at least minimally educated, and many have advanced technical knowledge that has been self-taught or with advanced instruction (Thomas, 2021). High trade is also attributed to the increase in the prevalence of functions of advanced technology, such as software and hacking tools, on the dark web, which in turn has been related to the global increase in cybercrime. Also, those from low-income backgrounds might be more likely to commit cybercrime to make quick money, especially in countries with high unemployment, such as Nigeria (Nwokolo, 2022).

Furthermore, cybercriminals frequently belong to organized groups with global reach. These gangs often use members with expertise in various forms of cybercrime, including hacking, fraud, and money laundering. Cybercrime is international, so they can work from afar in various places, and it’s hard for cops to find them.

Victims of Cyber Crime: Are We All at Risk?

A diverse group of people and institutions is affected by cybercrime, some more than others. The most heavily impacted class of mercury victims is the general public, in particular those unaware of best electronic security practices. It’s been found that cyber fraudsters are preying on people who are less tech-inclined and who are likely to get pulled into phishing scams, identity theft, and financial fraud (Fox, 2023). Older age groups are especially at risk, given they may not comprehend the risks associated with internet-related activities and are more likely to place trust in online communication (Hutchins & Lofstedt, 2021).

Businesses, in particular small and medium-sized enterprises (SMEs), are another demographic group that is negatively impacted by cybercrime. These are typically low-hanging fruit for cybercriminals as they have limited cybersecurity budgets and are easy

to breach. Small and Medium Enterprises (SMEs) in Nigeria represent over 60% victims of cybercrime in the country, mainly through social engineering attacks such as scams and data breaches (NCC, 2022). They lose not just money, but compete opportunities and a broken consumer trust that can hold them back.

The banking industry is another main concern for cybercriminals, as banks and financial In Schrems & Jones (2021) institutions are continuously being prey to attacks such as phishing, skimming at ATMs, and online banking fraud. Financial systems are attacked by cyber criminals who syphon and launder money through complex networks. Financial fraud stemming from cybercrime estimated at N127 billion in Nigeria was the focus of the Nigeria Financial Intelligence Unit, which reported that more than and $500million were lost in 2022 (NFIU, 2022), with the banking sector accounting for the largest (NFIU, 2022). The monetary loss and erosion of public confidence in banking as a sector have placed the Nigerian financial system under enormous strain.

Cybercrime additionally preys on corporations, government, and critical infrastructure. Ransomware attacks, in which a victim's data is encrypted, and payment is demanded for its release, in particular have been on the rise. The Nigerian government has suffered several ransomware attacks that have threatened to release sensitive government data, from hackers in exchange for substantial bounties (Nigerian Communications Commission, 2022). These attacks interrupt life-saving services, put sensitive information on the line, and siphon away public funds that could be invested in development programs.

Vulnerable Populations: Addressing Inequalities

In the vulnerability context, it is important to understand that socio-economic factors are determinants of who suffers more from cybercrime. Those who cannot afford secure internet connections, especially low-income people, are at a greater risk of cybercrime. These people lack the money to purchase cyber tools, exposing them to the risks of cyber-attacks such as fraud and exploitation. In addition, an alarming percentage of cybercrime victims remain ignorant about how to secure themselves on the internet, and they have little knowledge and resources to defend themselves from cyberthreats (Thomas, 2021).

Technological Factors Facilitating the Rise of Cybercrime

The Proliferation of the Internet

Internet proliferation is amongst the most important technological elements that have fueled cybercrime. The Internet is the communication, trade, and entertainment lifeline for modern people, and is used by more than 4.9 billion people around the world in 2023 (Statista, 2023). With an increasing number of people and businesses doing business online, cyber criminals are taking advantage of the increased use of digital platforms for illegal purposes. Cybercrime, which includes crimes such as phishing, online fraud, and identity theft, has become popular with attackers because it is easy to attack more people and organizations from any part of the world. Given the anonymity and the worldwide nature of the internet, our law enforcement agencies find it ever challenging to trace and apprehend the cyber criminals that can operate from countries with lax cybersecurity legislation (Zhang & Sun, 2022).

The further proliferation of e-commerce, online banking, and digital payment systems gives cyber criminals fresh opportunities to monetize their attacks. These cybercriminals leverage a variety of tactics such as social engineering, malware, and man-in-the-middle attacks to expose vulnerabilities in online applications and capture sensitive data like credit card numbers, login credentials, and personal information. Phishing attacks alone cost the global cybercrime industry an estimated 40%, and the impact is significant in the banking sector (Kaspersky, 2022).

Artificial Intelligence (AI) and Automation

With AI and machine learning coming of age, cybercriminals possess more powerful weapons than ever before. AI is being leveraged more and more in order to facilitate and automate cyber-attacks, which become more efficient and more difficult to detect. For instance, in a matter of seconds or minutes, AI-powered solutions can detect weaknesses in a target's network or system, and allow the bad guys to capitalize on those flaws in real time. Furthermore, artificial intelligence is also being used to carry out the generation of phishing emails, fake identities to carry out cybercrime, and similar, reducing human workload and scaling of attacks (Simmonds, 2021).

Further, AI-controlled malware, or "adaptive malware," may change its own behaviour based on the type of security protection it faces — a feature that causes problems for regular antivirus solutions during the detection and eradication process. It's this evolutionary ability to adapt and go undetected that makes it all a dangerous game for infosec pros and organizations. AI is used in creating deepfakes, the intricate doctored video or sound recordings that trick people into making false moves, like wire-transferring money or divulging top-secret data. The growing potential for misuse of deepfake technology has created new vulnerabilities, including identity theft, blackmail, and political interference (Chesney & Citron, 2020).

The Internet of Things (IoT) and Cybercrime

The spread of IoT devices has also promoted advances in cybercrime. The Internet of Things (IoT) describes the networking of physical objects - everything from smart consumer appliances to factory gear - to the Internet. But for all of the powerful capabilities and efficiencies that IoT offers in daily life, it's also become a major attack vector. Black hat hackers find IoT devices appealing because many do not include security and are therefore easy targets. Non-secure devices can be infiltrated and employed as an entry point for more widespread network attacks, many times without the user's awareness regarding the condition of the intercepted device (Mann & Singh, 2021).

The 2016 Mirai botnet attack is one of the most famous cybercrimes related to IoT devices. In this case, millions of vulnerable IoT devices were infected and used to perform a distributed denial of service (DDoS) attack that took down a number of major websites, like Twitter and Netflix. It is an example of how vulnerable these IoT networks are and how one bad device can cause massive-scale service disruption (Sen & Halder, 2022). With our ever-growing IoT adoption, the potential vulnerabilities of these insecure devices multiply and present criminals with fresh attack vectors.

Blockchain Technology and Cybercrime

Although blockchain, the distributed ledger technology underpinning Bitcoin and other cryptocurrencies, has been hailed as a secure means for digital transactions, it also enables cybercriminals. Decentralized and pseudonymous design of blockchain makes it attractive for criminals as well, be it money laundering, ransom payment, or trafficking of illegal commodities. Cryptocurrencies grant cybercriminals a level of secrecy that is conducive to anonymous transactions being made across borders without the reliance on financial intermediaries, which are often regulated and monitored (Foley, Karlsen, & Putniņš, 2020).

Ransomware, in particular, has taken advantage of the proliferated state of blockchain and crypto. In such attacks, a party of attackers requests ransom amounts to be paid in cryptocurrency because they are untraceable. The FBI has noted an increase in ransomware attacks that include ransomware payments that require cryptocurrency payments, making law enforcement less able to track and catch offenders (FBI, 2021). Legal use cases do exist for blockchain in digital finance, but its privacy focus being tagged to criminal conduct has cast a shadow of suspicion over the technology as a facilitator of cybercrime.

Determinants of Cybercrime in Nigeria

Socioeconomic Factors

Poverty, joblessness, and ignorance are the major causes of cybercrime in Nigeria. A high rate of poverty compounded with limited employment prospects, particularly for the youth, creates the incentive for people to engage in such criminal behavior as cybercrime. The National Bureau of Statistics (2021) reports that Nigeria's unemployment rate is about 33%, with a high incidence of unemployed youths, most of whom are not equipped with the necessary knowledge and skills to function in the formal employment sector. Becoming a cybercrime actor becomes the way for some to have a source of income as the internet provides a medium for making money illegally through activities such as phishing, identity theft, and online fraud (Akinmoladun et al., 2021).

In addition, insufficient education and access to digital literacy programs compound the issue. Cybercriminals. Many people, especially in rural areas, do not know or learn about the dangers of participating in cybercrime. Young Nigerians are at risk of being drawn into criminal gangs or turning to cybercrime alone (to fund themselves since they lack an education and a job). Over 40% of cyber perpetrators in Nigeria were induced by economic stress and limited employment opportunities, according to a study by Nwokolo (2020). Within the setting, cybercrime is a low-risk, high-reward option for people in search of economic stability.

Weak Legal Frameworks

Legal Base of Cybercrime in Nigeria. Another factor that enables the booming of Cybercrime in Nigeria is its Legal base. Although the country has made progress with laws aimed at combating cybercrime, such as the Cybercrime (Prohibition, Prevention, etc.) Act of 2015, delivery continues to pose a significant challenge. Drawbacks to the

legal process include limited resources, corruption, and the absence of trained law enforcement departments. These elements make it difficult to prosecute the perpetrators and make the victims reluctant to report cybercrimes due to the lack of confidence in the justice system (Okeke & Chukwu, 2021).

Moreover, the nation's digital infrastructure is not as well developed and faces a gap in technologies in advanced cyberspace, as some parts of the country are not connected. This has left Nigeria exposed to cyber attacks and made it more difficult for the government to track and prevent cybercrime. Moreover, Nigeria's judicial system is ill-equipped to deal with the international cooperation on cybercrime required to address cybercriminals who commit crimes in multiple jurisdictions. Cross-border cooperation on combating cybercrime is not effective, with no one being punished for such crimes, which has created a fertile ground for the participation of cybercriminals (NCC, 2021).

Cultural and Social Norms

Cultural and societal perception of cybercrime in Nigeria is also a factor that contributes to its popularity. In a lot of instances, cybercrime (and especially internet fraud) is seen by society as a way to the bank, and this may result in an implicit social acceptance, or even reverence, of cybercriminals. The emergence of 'Yahoo Boys' (young Nigerians who are involved in internet fraud) as social media influencers in Nigerian popular culture has contributed to the desensitization and normalisation of the idea that money made through dishonest means is good money. The normalization of cybercrime looms large in the universal apathy to its effects experienced by youth. It is often treated by some as a quick route to riches for economic emancipation, even though in essence it only ensures the perpetuation of cybercrime as an act (Osayi, 2021).

Furthermore, social expectations to become rich quickly have caused certain people to resort to cybercrime as a means of acquiring status and wealth. Dittemore writes that in a society that celebrates outward shows of wealth, it's relatively easy for cybercriminals to steal large amounts of money, and once they have that easy success, they keep at it. Loose morals that prevail in society and the absence of strict penalties in the lawbooks are what make cybercrimes thrive.

Preventive Measures Against Cyber Crime in Nigeria

Legal and Policy Measures

Steps taken by the Nigerian government to combat cybercrime. The Nigerian government has made an attempt at combating cybercrime by enacting laws and policies. One of the key laws is the Cybercrimes (Prohibition and Prevention) Act 2015, which is meant to enhance the legal framework for the investigation and prosecution of suspects and the prevention of cybercrime. It covers different types of cybercrime, such as hacking, identity theft, and online fraud, and contains penalties for those convicted of said crimes. While the Act is a positive step forward, there are some difficulties with the measure, for example, a lack of vigilance and a shortage of resources in law enforcement. Okeke & Chukwu (2021) noted that the Cybercrimes Act encountered challenges like a lack of training for the workforce and challenges in tracing cybercriminals operating from abroad. This stresses the necessity for efficient law

enforcement tools and, of course, for legal solutions that need to be adjusted to the developments of cyber threats.

Technological Solutions

Technology is absolutely the cornerstone of stopping cybercrime - cybersecurity infrastructure and software are key elements to an effective defense posture. Next-generation security defenses, for example, firewalls, intrusion prevention systems (IPS), and encryption methods, are essential to safeguard data and online transactions. Many organizations and government ministries in Nigeria are now investing in cybersecurity to secure their networks from potential cyber-attacks. For instance, Nigerian banks have implemented multi-factor authentication and encryption standards to secure online banking against cyber-attacks (Nigerian Financial Intelligence Unit, 2022). Cybersecurity software, like antivirus software and malware scanners, also helps identify and block threats before they can access systems. But as useful a tool as technology is in trying to stop cybercrime, it is only as good as its latest update and the latest hack someone manages to squeeze through a new vector of attack. It also ultimately includes cooperation between the public and private for proactive defense against cyberthreats (Baker and Singh, 2022).

Public Awareness and Education

Sensitization and public enlightenment are key ingredients in a preventive measure against cybercrime. Most Nigerians do not have knowledge of the dangers of online and best practices to safeguard themselves from online criminals. It is conveyed that public awareness-raising efforts of cyber risk, like phishing, identity theft, and online crime safety measures, are of great value for the number of possible victims. The Nigerian Communications Commission (NCC) has played a significant role in the creation of public awareness campaigns for empowering citizens with information on the necessity of passwords that are difficult to guess, suspicious-looking transactions online, and phishing attempts. NCC (2023) reports that these campaigns have resulted in improved awareness and a decrease in some types of Cybercrime, e.g., online fraudulent activities. But the community also needs more-promotional educational programs to reach out more broadly, including to populations, notably the elderly and people living rurally, who are less informed about and less focused on digital security.

International Cooperation

As is the case with cybercrime that is transnational in nature, international cooperation is indispensable to effectively combat it. Because cybercriminals work internationally, individual countries sometimes find it challenging to combat cybercrime within their own jurisdictional and technical limits. International cooperation, including alliances between INTERPOL, the UN, and countries around the world, is crucial to bringing cybercriminals to justice and preventing cybercrime. At the global front, Nigeria has engaged in several international cybersecurity projects, such as the Global Forum on Cybersecurity and the African Union's Cybersecurity and Cybercrime Convention, aimed at improving cooperation and collaboration between countries. Based on Olanrewaju (2022), these international collaborations further reinforce Nigeria's cybersecurity defenses by securing them access to international expertise, resources, and intelligence. International collaboration also allows for the exchange of information

on new threats, something that is hugely important in outpacing the increasingly-sophisticated cybercriminals.

Challenges in Combating Cybercrime

Resource Limitations

The problem of cybercrime in Nigeria. One of the biggest challenges to the battle against cybercrime in Nigeria has been the lack of proper funding for law enforcement and cybersecurity agencies. Most law enforcement organizations lack sufficient funds, capacity, and training to effectively combat cybercrime (Okeke & Chukwu, 2021). Insufficient financing prevents the purchase of sophisticated cybersecurity technologies such as intrusion detection systems and malware analysis software, vital for the detection and prevention of cybercrime. It is also the case that the police do not have the required knowledge of cybercrime investigation and, as a result, find it difficult to track down and arrest cybercriminals (Graham & McKew, 2020). This is made worse by the fact that in Nigeria, only 15% of Nigerian Police officers have been trained in specialized courses in digital forensics and cybercrime investigation, making it difficult to effectively combat cybercrime (National Cybersecurity Agency, 2022). These resource shortages not only slow down investigations, but also give cybercrooks the freedom to run amok.

Technological Challenges

Technology-related challenges also represent a major challenge in the fight against cybercrime in Nigeria. Inside many government departments and businesses, technology and infrastructure are old and out of date, a situation that makes them susceptible to cyberattacks. Despite some recent attempts to update the way infrastructure is built, many Nigerian businesses are running outdated systems, lowering the adoption and consciousness of security and leaving them open to attack, says Alade. A NCCNCC (2021) report indicates that most public sector organisations do not have contemporary firewalls, intrusion prevention systems, antivirus, and other cybersecurity solutions required to protect them from new security threats such as ransomware, phishing, and data breaches. Moreover, the speed of technological innovation guarantees that fresh attack tactics and digital openings are consistently introduced, frequently faster than the nation can adapt with upgraded digital security protocols. Consequently, the cybercriminals capitalize on these technical loopholes, and the outcome is insured high-gap and high frequency at which data breaches and online fraud cases are pervasive (Adelakun & Olayanju, 2021).

Legal and Institutional Barriers

Nigerian laws and institutions compound the difficulty of combating computer crime. The passage of the 2015 Cybercrimes (Prohibition and Prevention) Act was a milestone, but its enforcement has been problematic. One of the biggest problems is the absence of dedicated cybercrime courts and a fast-track legal system to address them. Contributing to the latter point, delay in the process can only serve to dilute deterrence and embolden cybercriminals to ply their trade more recklessly, all the while still quick to trust that they will get off the hook (Soyombo, 2019). Secondly, Nigeria does not have well-articulated extradition treaties with many countries (even as classified by the

International Cooperation Review Group (ICRG)) that will aid it in the prosecution of cybercriminals, a bulk of whom perpetrate crime across borders. The non-existence of an international system where Nigeria can cooperate with other nations to prosecute cyber criminals in other parts of the world makes it easier for cyber-criminals to perpetrate fraudulent activities across borders and relocate to another country with less effective law enforcement (Oluwole & Adeola, 2020). Corruption in the police and judicial system also means that the current laws against cybercrime are not effectively enforced, diminishing efforts to tackle the expanding menace.

Conclusion

In conclusion, cybercrime is a severe and increasing problem in Nigeria and has far-reaching effects on individuals, organisations, and the economy. With the evolution of online-based technologies in recent years, cyberspace has presented criminals with new opportunities with regard to crimes like phishing, financial fraud, and identity theft. The Nigerian economy has been one of the worst hits, losing millions of dollars to cybercrime every year. Secondly, the absence of cybersecurity technology, poverty, and weak laws has also helped in increasing the commission of such crimes. Combating cybercrime in Nigeria should not be a standalone issue, but should be tackled on three levels: legislation, technology, and public enlightenment. All these attempts are futile because it is not until the country comes together to do the needful that the growth of Nigeria's digital economy and national security will be susceptible to cybercrime. Thus, the government and law enforcement agencies need to collaborate with the private sector to bolster Nigeria's cybersecurity stance to safeguard its people and institutions that are at risk of falling for cybercrime.

Recommendations

To effectively fight against cybercrime in Nigeria, the following are recommended:

1. There should be pragmatic and policy issues to be addressed to enhance extant laws and structures, including the Cybercrimes (Prohibition and Prevention) Act, 2015. Reforming it to cover new threats like cryptocurrency fraud and deepfakes, establishing dedicated courts for cybercrime, and strengthening international cooperation are a good start. Apart from this, by inflicting harsher punishment on cybercriminals, there will be a deterrence against cybercrimes.

2. Developing the capacity of police and related organisations. Specialized training in the field of digital forensics, cybersecurity, and cybercrime investigation would improve the competency among the officers and judicial members. Providing these agencies with state-of-the-art tools and cultivating international partnerships through the sharing of knowledge will enhance their ability to successfully detect, investigate, and put cyber criminals away. Enhancing the capacity of these agencies will enable Nigeria to keep pace with emerging cyber threats.
3. The significance of community involvement in cybercrime prevention cannot be overstated. Public awareness can be used to educate the public on the dangers of online activities and encourage safer online behaviour. By getting schools and community leaders, such as local organisations, involved in these efforts, Nigeria could create a culture that encourages awareness of cybersecurity. The creation of accessible ways to report cybercrime could

References

Adelakun, S., & Olayanju, A. (2021). Cybersecurity in Nigeria: Challenges and solutions. *Journal of Cybersecurity and Law*, 14(3), 112-126. https://doi.org/10.1080/23300813.2021.1900493

Akinmoladun, S., Adebayo, S., & Eze, I. (2021). Socioeconomic factors and the rise of cybercrime in Nigeria. *Journal of Nigerian Criminology, 15*(3), 45-67. https://doi.org/10.1177/20530196211003288

Akpan, I. A. (2021). Cybercrime and its impact on Nigeria's national security. *International Journal of Cybersecurity and Digital Privacy, 10*(3), 87-99. https://doi.org/10.1177/20530196211003288

Baker, S. (2021). The Internet of Things and cybersecurity: A growing concern. *International Journal of Cybersecurity, 8*(4), 345-358. https://doi.org/10.1080/20530196211003288

Baker, S., & Singh, G. (2022). Cybersecurity in Nigeria: Addressing challenges and implementing effective solutions. *Journal of Cybersecurity*, 14(1), 45-58. https://doi.org/10.1016/j.jinfosec.2022.04.003

Burgess, A., & Rege, S. (2021). Gender and cybercrime: A closer look. *Journal of Criminal Justice*, 43(5), 91-102. https://doi.org/10.1016/j.jcrimjus.2021.03.004

BusinessDay. (2022). The dark web of cybercrime: How Nigeria's economy is under threat. Retrieved from https://businessday.ng/bd-weekender/article/the-dark-web-of-cybercrime-how-nigerias-economy-is-under-threat/

Chesney, R., & Citron, D. K. (2020). Deepfakes: A looming challenge for privacy, democracy, and national security. California Law Review, 108(4), 925-1008. https://doi.org/10.15779/Z38K38J

Council of Europe. (2021). The Budapest Convention on Cybercrime. Retrieved from https://www.coe.int/en/web/cybercrime

Davenport, T. H. (2022). The rise of AI in cybercrime: A challenge for cybersecurity professionals. Journal of Cybersecurity, 14(3), 112-126. https://doi.org/10.2139/ssrn.3767202

European Commission. (2020). The General Data Protection Regulation (GDPR) and its implications for cybersecurity. Retrieved from https://ec.europa.eu/info/law/law-topic/data-protection_en

FBI. (2021). Ransomware attacks and cryptocurrency: New risks and challenges. Federal Bureau of Investigation. Retrieved from https://www.fbi.gov

Federal Bureau of Investigation. (2021). Advance-fee scam. Retrieved from https://en.wikipedia.org/wiki/Advance-fee_scam

Foley, S., Karlsen, J. R., & Putniņš, T. J. (2020). Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? Review of Financial Studies, 33(5), 1-26. https://doi.org/10.1093/rfs/hhz106

Fox, J. A. (2023). Cybercrime and vulnerable populations: The case of senior citizens. *Cybersecurity Review*, 19(2), 45-58. https://doi.org/10.1016/j.cose.2023.02.010

Graham, J., & McKew, K. (2020). Phishing and financial fraud in Nigeria: Investigating the economic impact. *Cybersecurity Review*, 26(2), 45-67. https://doi.org/10.1016/j.cose.2020.02.001

Henson, S. (2020). The changing demographics of cybercriminals: An emerging challenge. *Journal of Information Security*, 26(2), 120-132. https://doi.org/10.1016/j.jinfosec.2020.01.008

Hutchins, S., & Lofstedt, R. (2021). Ageing and cybersecurity: Understanding senior citizens' vulnerability. *International Journal of Cybersecurity and Digital Privacy*, 7(1), 77-89. https://doi.org/10.1080/20530196211003288

Imam, A. (2023). Cyber warfare and national security in Nigeria: Threats and responses. Global Journal of Political Science and International Relations, 8(4), 122-135. https://doi.org/10.2139/ssrn.3767202

Kaspersky. (2022). Phishing attacks in 2022: Trends and threats. Kaspersky. Retrieved from https://www.kaspersky.com

Mann, B., & Singh, G. (2021). Cybersecurity in IoT: Emerging challenges and solutions. Journal of Cybersecurity Technology, 6(3), 24-39. https://doi.org/10.1080/23300713.2021.1886760

McGuire, M. (2022). The young and the cyber: Demographic analysis of cybercriminals. *Cybercrime and Society*, 11(3), 34-45. https://doi.org/10.1109/cybercrimesociety.2022.00004

National Cybersecurity Centre. (2021). Cybercrime statistics and trends. Retrieved from https://www.ncsc.gov.uk

National Cybersecurity Agency. (2022). *Cybercrime and national security in Nigeria: Current trends and policy recommendations*. Retrieved from https://www.ncsa.gov.ng

NCC. (2021). Cybercrime and cybersecurity in Nigeria: Legal frameworks and challenges. Nigerian Communications Commission. Retrieved from https://www.ncc.gov.ng

NCC. (2022). *Cybercrime in Nigeria: Impact and Statistics*. Nigerian Communications Commission. Retrieved from https://www.ncc.gov.ng

NCC. (2023). *Public awareness and cybersecurity: Trends in Nigeria*. Nigerian Communications Commission. Retrieved from https://www.ncc.gov.ng

NFIU. (2022). *Financial fraud and cybercrime: Trends in the Nigerian banking sector*. Nigerian Financial Intelligence Unit. Retrieved from https://www.nfiu.gov.ng

Nigerian Communications Commission. (2022). Cybersecurity and cybercrime in Nigeria: The implications on national security and digital economy. Retrieved from https://www.ncc.gov.ng

Nigerian Financial Intelligence Unit (NFIU). (2022). *Cybercrime and financial institutions in Nigeria: A report*. Nigerian Financial Intelligence Unit. Retrieved from https://www.nfiu.gov.ng

Nwokolo, C. (2020). The role of poverty and unemployment in driving cybercrime in Nigeria. African Journal of Social Studies, 9(4), 98-110. https://doi.org/10.2139/ssrn.3767202

Okechukwu, S. & Ihuoma, C. (2022). Cybercrime in Nigeria: Analysis, management, and prevention. Journal of Cybersecurity and Digital Technology, 14(2), 45-60. https://www.researchgate.net/publication/348195748_Cybercrime_in_Nigeria_Analysis_Management_and_Prevention

Okeke, A., & Chukwu, I. (2021). Cybercrime and law enforcement in Nigeria: Challenges in policy implementation. *International Journal of Criminology and Law*, 10(2), 112-125. https://doi.org/10.1016/j.jcrimjus.2021.03.012

Okeke, A., & Chukwu, I. (2021). Cybercrime and legal challenges in Nigeria: A review of current laws. International Journal of Criminology and Law, 10(2), 112-125. https://doi.org/10.1016/j.jcrimjus.2021.03.001

Olanrewaju, A. (2022). The importance of international cooperation in combating cybercrime. *Cybersecurity International*, 19(2), 77-88. https://doi.org/10.1016/j.cose.2022.05.005

Oluwole, O., & Adeola, A. (2020). Legal and institutional barriers in the prosecution of cybercrime in Nigeria. *Nigerian Journal of Criminal Justice*, 9(3), 56-71. https://doi.org/10.2139/ssrn.3767202

Onah, F. O., Onodugo, V. O., & Ugwu, C. (2023). Cyber fraud in the Nigerian Banking System in Enugu, Enugu State. Retrieved from https://www.dzarc.com/education/article/download/658/607/984

Osayi, G. (2021). Cultural and social norms and their influence on cybercrime in Nigeria. Journal of Public Policy and Cybersecurity, 13(2), 75-86. https://doi.org/10.1080/20530196211003288

Schrems, T., & Jones, S. (2021). Financial fraud and cybercrime in Nigeria's banking system. *Journal of Financial Services Research*, 38(1), 54-67. https://doi.org/10.1007/s10203-021-00300-3

Sen, A., & Halder, A. (2022). Cybercrime in the IoT era: Understanding vulnerabilities and threats. International Journal of Cybersecurity and Digital Privacy, 7(2), 76-89. https://doi.org/10.1080/20530196211003334

Simmonds, G. (2021). Artificial intelligence and its role in modern cybercrime. Journal of Information Security, 19(1), 45-58. https://doi.org/10.1016/j.jinfosec.2020.01.007

Smile ID. (2024). Digital Identity Fraud in Africa Report. Retrieved from https://spectator.africa/2024/01/30/nigeria-and-ghana-lead-west-africas-identity-fraud-cases-report/

Soyombo, O. (2019). The challenges of prosecuting cybercrime in Nigeria: A review of the legal system. *Journal of Information Security*, 17(4), 135-148. https://doi.org/10.1080/23300713.2019.1654762

The Guardian. (2024). How West Africa's online fraudsters moved into sextortion. Retrieved from https://www.theguardian.com/uk-news/article/2024/aug/21/how-west-africas-online-fraudsters-moved-into-sextortion

Thomas, K. (2021). Socio-economic factors and their impact on cybercrime. *Cybersecurity Policy Review*, 14(3), 85-99. https://doi.org/10.1080/20530196211003303

U.S. Department of Justice. (2021). Operation Disruptor: A new frontier in combating cybercrime. Retrieved from https://www.justice.gov/opa/press-release/file/1350201/download

World Economic Forum. (2023). Global Risks Report 2023. Retrieved from https://www.weforum.org/reports/global-risks-report-2023

Zhang, J., & Sun, J. (2022). Cybercrime: A study of technological evolution and its security implications. International Journal of Cybercrime and Digital Security, 12(4), 99-113. https://doi.org/10.1080/1553313.2022.1806789