Special Issue
Journal of General Studies ESUT ISSN: 1115-6767, E-ISSN: 2971-6241 **Vol. 7 No. 2, 2025**

CYBERSECURITY AND CRIME-FIGHTING STRATEGIES IN NIGERIA

Young Ozogwu[1], John Anda[2], Gilbert Aimufua[3], Steven Bassey[4], Victor Kulugh[5]
[1,2,3,4] Centre for Cyber Security Studies, Nasarawa State University, Keffi, Nigeria
[5]Department of Cybersecurity, Bingham University, Karu, Nigeria. young.ozogwu@gmail.com

Abstract

Cybercrime is today gaining momentum in Nigeria; making national security and economic stability to rely heavily on cybersecurity. Law enforcement agencies and policymakers face substantial challenges from Nigeria's rising cyber-related offenses which include financial fraud, identity theft, hacking and cyber terrorism. This study analyses Nigeria's cybersecurity environment by assessing how legal structures, law enforcement methods, technical solutions and public awareness programs work together to fight cyber threats. It examines key documents, including the Cybercrime Prohibition and Prevention Act (Amended 2024) and the National Cybersecurity Policy and Strategy (NCPS, 2021), alongside scholarly literature and agency reports. Using thematic analysis, the study identifies strengths, weaknesses, and gaps in Nigeria's approach. The legal and policy documents exemplify Nigeria's current measures to address cybercrime through new legislation, upgraded enforcement capabilities and technological advancements. Cybercrime prosecution rates stay troublingly low between 2015 and 2023 averaging 14% while reported cases continue to increase. The Economic and Financial Crimes Commission (EFCC) along with the Nigerian Police Force (NPF) face challenges in forensic investigations and collaboration while operating with outdated crime-fighting methods. Nigeria's annual cybersecurity budget of $13 million remains far below the levels seen in developed countries which constrains its capacity to implement new technologies like artificial intelligence (AI), machine learning (ML) and blockchain security defenses. This study applies a qualitative research approach to combine literature from government reports, scholarly articles and cybersecurity legal and policy assessments in order to evaluate Nigeria's cyber defense capabilities. This paper finds that Nigeria can heighten its defense against cyber threats through strengthened cybersecurity policies, investments in advanced forensic technologies, improved public cybersecurity education and strengthened international collaborations. The study recommends innovative solutions, such as AI-driven fraud detection and a Nigeria-specific cybersecurity app, to strengthen defenses. It also suggests legal reforms, enhanced training, and international cooperation to protect Nigeria's digital economy.

Keywords: Cybersecurity, Cybercrime, Digital forensics, Artificial intelligence, Nigeria, Law enforcements.

Introduction

The rise of cybercrime poses serious risks to Nigeria's economy and national security. Financial losses run into hundreds of millions of dollars each year (Interpol, 2022). Trust in online systems is weakened, slowing digital transformation. Investors may hesitate to engage with a market they see as unsafe. Cybersecurity is the shield against these threats. It involves protecting networks, systems and data from unauthorized access, disruption, or destruction (NCPS, 2021). In Nigeria, this means a mix of laws, law enforcement strategies, public awareness programs and advanced technologies.

This study examines how cybercrime has evolved in Nigeria and how cybersecurity measures have developed in response. It reviews laws like the Cybercrime Prohibition and Prevention Act (Amended 2024) and the National Cybersecurity Policy and Strategy (2021). It also considers how agencies such as the Economic and Financial Crimes Commission (EFCC) and Nigerian Police Force (NPF) are responding. The objectives of this study include:

1. To explain the growth and changing nature of cybercrime in Nigeria.
2. To analyse Nigeria's legal and policy response to these threats.
3. To recommend practical, workable solutions that improve prevention and enforcement.

The Emergence and Development of Cybercrime and Cybersecurity in Nigeria

Cybercrime in Nigeria has a history that is going to thirty years. In the early 1990s, the internet was still new in the country. Yet, criminals quickly found ways to exploit it. One of the earliest and most notorious forms was the "advance-fee fraud," commonly called the 419 scam, named after the section of the Nigerian Criminal Code dealing with fraud. Offenders would send letters or later emails, promising large rewards in exchange for small "processing" fees. Many victims around the world lost thousands of dollars to these scams (Olayemi, 2014).

As internet use expanded in the 2000s, cybercrime became more sophisticated. Criminals moved from simple email scams to more technical attacks like ATM card cloning, phishing websites and hacking into company databases (Nwankwo & Ukaoha, 2019). This period also saw the rise of the so-called "Yahoo Boys." These were mostly young people using social engineering and online romance scams to trick victims, often from overseas. Between 2010 and 2015, the scope widened again. Identity theft, ransomware and large-scale data breaches became more common. Criminals began to target not only individuals but also banks, telecom companies and government databases (Interpol, 2022).

With the spread of smartphones, mobile banking and cryptocurrency, new opportunities for fraud appeared. Criminals also started using artificial intelligence, deepfake videos and complicated money-laundering schemes to hide from investigators (Daniels, 2023). The techniques became faster, more automated and harder to trace. Nigeria is now among the top 10 countries most affected by cybercrime. According to Interpol's 2022 report, the country loses over $500 million each year from both local and international cases (Interpol, 2022).

Table 1: Evolution of Cybercrime in Nigeria (1990s –To date)

Era	Common Cybercrime	Methods Used	Impact
1990s - 2000s	Advance-fee fraud (419 scams)	Fake business emails, fake lottery scams	Massive financial losses in the millions
2010 – 2015	ATM fraud, hacking	Card cloning, phishing attacks	Banks and financial institutions targeted
2016 – 2020	Identity theft, ransomware	Social engineering, malware	Data breaches, increased online banking fraud
2021 – Present	AI-driven cybercrime, deepfake fraud	Artificial intelligence, machine learning	Fake identities, manipulated videos, sophisticated phishing attacks

Sources: (Olayemi, 2014; Makeri, 2017; Nwankwo & Ukaoha, 2019; Daniels, 2023)

The development of cybersecurity in Nigeria to these threats was gradual and slow. Before 2010, efforts were mostly informal and reactive. Companies relied on basic antivirus software and firewalls, while government action was minimal. A major progress was achieved in 2015 with the introduction of Cybercrime Prohibition and Prevention Act**.** This was Nigeria's first comprehensive cybercrime law. It criminalized a wide range of offenses including hacking, identity theft, cyberstalking and online fraud (Nwankwo & Ukaoha, 2019). It also created a legal basis for digital evidence collection and cooperation with international agencies.

Between 2016 and 2020, security agencies like the EFCC, Nigerian Police Force (NPF) and Department of State Services (DSS) created special units to handle cybercrime. Public awareness campaigns also started, but they reached only a small part of the population (Makeri, 2017). Another milestone came with the launch of the National Cybersecurity Policy and Strategy (NCPS) in 2021.It introduced structured governance for cybersecurity, encouraged public-private partnerships and promoted the use of AI and big data in threat detection. However, funding and skilled manpower were still not enough (Osho & Onoja, 2015). In 2024, the Cybercrime Act was amended. The changes brought tougher penalties for offenders, it covered new threats like cryptocurrency fraud and improved coordination among agencies. The law also recognized AI-driven attacks as a serious national security risk (NCPS, 2021; Daniels, 2023).

Table 2: Evolution of Cybersecurity in Nigeria (1990s – Present)

Period	Key Developments	Challenges
1990s–2000s	Basic antivirus and firewalls in private sector; limited awareness in public	No national policy; minimal enforcement capacity
2010–2014	Early digital forensics units in EFCC and NPF; ad-hoc public awareness campaigns	Few trained personnel; low budgets; weak laws
2015	Cybercrime Prohibition and Prevention Act enacted	Initial implementation slow; lack of public understanding
2016–2020	Establishment of dedicated cybercrime units; sector-specific security policies	Poor inter-agency coordination; limited adoption of advanced technology
2021	National Cybersecurity Policy and Strategy launched	Funding gaps; shortage of skilled professionals
2024	Cybercrime Act amended; recognition of AI-driven threats; stronger penalties	Technology adoption still slow; global cooperation remains limited

Theoretical Framework

This study is guided by three main theories that help explain how and why cybercrime happens and how cybersecurity can respond to it.

a. Routine Activity Theory

Routine Activity Theory (Cohen & Felson, 1979) says that a crime happens when three things meet:

i. A motivated offender
ii. A suitable target
iii. The absence of a capable guardian

In Nigeria, all three conditions often exist. Many young people face high unemployment, making them more likely to be tempted by illegal online income. Targets are everywhere, from individuals using weak passwords to banks without strong online fraud detection. Capable guardians are missing because cybersecurity systems are weak, law enforcement lacks tools and agencies do not coordinate well (Osho & Onoja, 2015).

b. Space Transition Theory

Space Transition Theory (Jaishankar, 2008) explains how people behave differently online than they do in person. In the physical world, committing fraud is risky and often face-to-face. Online, criminals can hide behind screens, fake identities and foreign IP addresses.

Nigerian cybercriminals often use:

- Virtual Private Networks (VPNs) to hide their location
- Encryption to block investigators from reading stolen files
- Decentralized networks to store and transfer illegal content

These methods make tracking them extremely difficult (Aminu, 2024). For example, a scammer in Lagos might appear online as a user in Canada, making it hard for Nigerian law enforcement to trace them.

c. Cyber Resilience Framework

The Cyber Resilience Framework looks at how institutions prepare for, endure and recover from cyberattacks. The focus of this framework is how quickly a system can get return back to normal after an attack, thereby emphasizing that no system is 100% safe. In Nigeria, cyber resilience is still underdeveloped. Many government and private organizations have no tested recovery plans. If a ministry's website is hacked, it may stay offline for weeks. The absence of backup systems, skilled IT teams and clear procedures increases damage from attacks.

These theories show that cybercrime in Nigeria is not just about technology, it is also about human behaviour, social conditions and institutional capacity. They show why crimes happen, why they are hard to stop and how Nigeria can build stronger defenses.

Cybersecurity Policies and Legal Frameworks

Nigeria has created several laws and policies on cybersecurity. These laws set the rules for prevention, investigation and punishment**.**

The Cybercrime Prohibition and Prevention Act

This act was Nigeria's first comprehensive cybercrime law. It criminalized activities such as hacking, identity theft, cyberstalking, phishing and online fraud (Nwankwo & Ukaoha, 2019). It also allowed law enforcement to collect digital evidence and cooperate with international agencies. This Act marked the start of Nigeria's formal legal response to cybercrime. Before this law, most cyber offenses were handled under general criminal laws, which did not cover digital evidence or online-specific crimes. In 2024, the Act was updated to tackle newer and more complex threats. The main changes were:

- Tougher penalties for offenders
- Inclusion of crimes such as cryptocurrency fraud, AI-driven attacks and deepfake scams
- Improved coordination between agencies like the EFCC, DSS, NPF and the Nigerian Communications Commission (NCC)

The amendment brings Nigerian law closer to global best practices (NCPS, 2021). It also accepts that technology changes quickly, so laws must keep adapting to stay useful (Daniels, 2023).

The National Cybersecurity Policy and Strategy

This policy provides a roadmap for protecting Nigeria's digital space. Its major objectives are:

- Protecting critical national infrastructure like banks, telecoms and power grids
- Supporting cybersecurity cooperation between public institutions and private entities
- Raising public awareness about online safety
- Building the skills of law enforcement through training and better technology

The NCPS (2021) connects legal frameworks with practical action. However, it lacks some elements found in other countries, such as a military cyber-defense strategy and a comprehensive national digital identity system (Osho & Onoja, 2015).

Gaps and Challenges

We observed that even with these laws and policies, enforcement is still weak. Most agencies often work alone, which causes duplication and missed chances for cooperation (Ezeji, 2024). Many members of staff of security agencies do not have the specialized training needed in digital forensics. Inadequate funding as another major challenge. Nigeria spends about $13 million a year on cybersecurity, this is far below what developed countries invest in fighting cybercrime (Interpol, 2022). Then, there is the sluggishness in updating Nigeria's legal frameworks to be in tandem with current realities.

Role of Technology in Cybercrime Prevention

One of the most powerful ways to fight cybercrime is through technology. These days, cybersecurity now depends on AI, ML and big data to spot and stop threats quickly. In Nigeria, these advanced tools are not widely used yet. Many agencies still depend on old systems for investigations and monitoring (Daniels, 2023). Criminals take advantage of these gaps to do damage.

Table 3: Cybersecurity Awareness Levels in Nigeria (Survey Data, 2023)

Awareness Level	Percentage (%)	Description
Low Awareness	50%	Individuals unaware of cybersecurity best practices
Moderate Awareness	30%	Basic understanding but poor security habits
High Awareness	20%	IT professionals and trained individuals

Sources: (Tijjani, 2023); Makeri, 2017); Aleke et al., 2023)

a. AI and Machine Learning in Cybersecurity

AI and ML analyze large datasets in real time. They detect patterns that are unusual that signal hacking, phishing, or fraud. In2022 in France for example**,** Darktrace Antigena stopped a ransomware attack at a hospital group known as Dordogne GHT. It autonomously blocked the Ryuk ransomware, protecting critical medical devices (Darktrace, 2022). In South Africa, Standard Bank uses an ML-based fraud detection system. It monitors millions of transactions daily, significantly reducing financial fraud (Standard Bank, 2023). These tools flag suspicious activities, like unusual login attempts, for immediate investigation. In Nigeria, adopting similar systems could address the shortage of trained investigators. For instance, AI could monitor banking apps to catch fraud faster than manual reviews.

b. Personal and Corporate Security Tools

Simple tools like anti-malware software can be used by individuals and companies to blocks viruses and spyware. Multi-factor authentication (MFA) makes accounts very difficult to hack, while the use of encryption tools can also keep sensitive data keeps secure. In the United Kingdom, Barclays Bank requires MFA for all online banking users. This cut phishing-related losses by 30% in 2022 (Barclays, 2022). Nigeria's banks could adopt similar measures to protect customers. Regular software updates also strengthen defenses (Aleke et al., 2023).

Cybersecurity Awareness

Fighting cybersecurity through technology alone is not enough. Many cyberattacks succeed because people are unaware of basic safety practices. According to a survey by Tijjani (2023), it indicates that:

- 50% of Nigerians have low awareness of cybersecurity best practices.
- 30% have moderate awareness but still make risky choices.
- Only 20% have high awareness**,** mostly IT professionals (Tijjani, 2023).

For example, even with advanced security systems, if an employee clicks a phishing link, hackers can still gain access to a company's network.

Capacity Building for Law Enforcement

It is important to train police, EFCC officers and other security agencies in digital forensics. Without providing them with the necessary skills, even the best technology cannot be used effectively. Well-trained officers can trace cyberattacks faster, preserve digital evidence correctly and prosecute offenders successfully (Ebenezer, 2019).

The Technology Awareness Connection

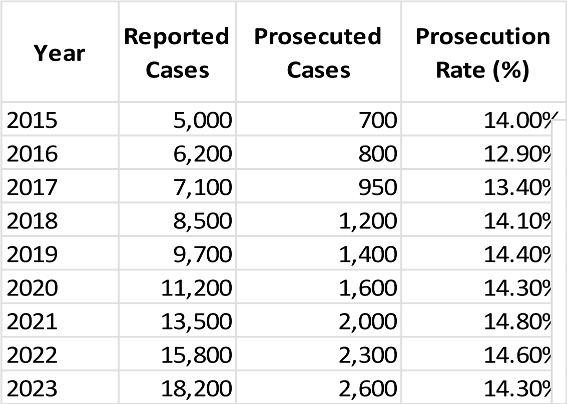
Strong cybersecurity requires both technology and public education. AI tools and advanced software protect systems, while awareness campaigns and training protect people. Without one, the other is less effective.

Findings and Discussion

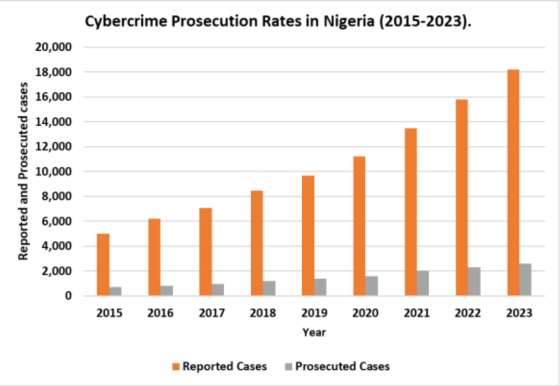
i. Weak Enforcement of Cybersecurity Laws

The Cybercrime Prohibition and Prevention Act (Amended 2024) and the NCPS of 2021 are strong on paper. However, their impact is limited by weak enforcement. Many law enforcement officers lack specialized training in digital forensics. Investigations often rely on outdated methods like manual data reviews and poor inter-agency coordination creates duplication of effort and delays. For example, if EFCC and NPF investigate the same cyber fraud case separately without sharing information, suspects may escape through legal gaps.

Table 4: Cybercrime Prosecution Rates in Nigeria **Chart 1.1: EFCC Annual Cybercrime Reports (2015-2023)**



Year	Reported Cases	Prosecuted Cases	Prosecution Rate (%)
2015	5,000	700	14.00%
2016	6,200	800	12.90%
2017	7,100	950	13.40%
2018	8,500	1,200	14.10%
2019	9,700	1,400	14.40%
2020	11,200	1,600	14.30%
2021	13,500	2,000	14.80%
2022	15,800	2,300	14.60%
2023	18,200	2,600	14.30%



Source: (EFCC Annual Cybercrime Reports (2015-2023))

ii. Outdated Law Enforcement Strategies

Nigeria's law enforcement agencies rarely use advanced tools like AI-based fraud detection and real-time network monitoring to fight cybercrime. Instead, agencies depend on reactive approaches, making them to act only after damage has been done. This gives criminals time to move money, delete evidence, or hide their identity.

iii. Low Public Trust in Law Enforcement

Findings show that victims often avoid reporting cybercrime because they doubt the ability of the police or EFCC to act quickly and effectively. This underreporting weakens national threat intelligence.

iv. Technology Gaps

Nigeria invests very little in cybersecurity infrastructure, when compared to what other developed countries spend. There is no nationwide network of Security Operations Centers (SOCs) to coordinate real-time threat responses. Many agencies still store digital evidence on unsecured drives, increasing the risk of tampering or loss.

v. Public Awareness and Education Deficits

Half of Nigerians have little to no knowledge of basic cybersecurity practices. This increases the “attack surface” for cybercriminals. No system is foolproof as far as its technical defenses can be bypassed if its users fall for phishing scams or use weak passwords.

vi. Limited International Cooperation

Cybercrime is often global in scope. Many Nigerian cyberattacks target victims abroad or involve infrastructure hosted overseas. While Nigeria works with Interpol and other partners, real-time cooperation is rare. The absence of fast legal frameworks for extradition and cross-border evidence sharing slows prosecutions.

Recommendations

To make Nigeria’s fight against cybercrime stronger, this study suggests practical steps that fit the country’s needs. Using AI, building strong partnerships between government and private entities and raise public awareness is the main focus.

a. **Adopt AI-Driven Fraud Detection Tools:**
The idea here is to use AI for the detection of frauds. For example, a platform like FraudSense AI can scan banking transactions in real time and flag suspicious activities within seconds. If Nigeria’s Central Bank insists that this must be a feature in all mobile banking apps, users will be better protected. A pilot initiative of this idea can start in Lagos and Abuja, where cybercrime is most common.

b. **Develop a Nigeria-Specific Cybersecurity App:**
This involves the development of a cybersecurity app for Nigeria, called CyberSafe Naija. The purpose of the app is to teach people simple safety tips, like how to spot phishing emails, create strong passwords and use two-factor authentication. It could also send alerts about new local scams, such as updated 419 tricks. NITDA can help in this area by working with local developers to launch the app by 2026, targeting to reach 10 million downloads within two years.

c. **Establish Public-Private Cybersecurity Alliance:**
Nigeria can set up the Nigeria CyberShield Alliance, bringing together government agencies like EFCC, NPF and NCC, alongside tech companies such as MTN and Globacom and universities like the Enugu State University of Science and Technology, ESUT. The goal is to share real-time threat data, fund local AI research and train about 5,000 cybersecurity experts each year. For example, MTN could provide network data to track malware, while universities design AI tools to fight scams common in Nigeria. This alliance could begin by mid-2026 with $5 million in private funding.

d. **Set up Community Cybersecurity Hubs:**
Build Cyber Hubs in each of Nigeria's six geopolitical zones. These hubs will serve as local centers for digital forensics training, public awareness workshops and real-time threat monitoring. Each hub can use Darktrace Antigena, an AI tool that autonomously responds to network intrusions. The hubs can train 1,000 police officers yearly and educate 50,000 citizens through community programs. Fund this with a $10 million budget reallocation by 2027.

e. **Introduce a National Cybercrime Hackathon:**
Host an annual Naija CyberHack, inviting young coders to develop solutions for local cyber threats, like cryptocurrency fraud or deepfake scams. Winners can receive funding to turn their ideas into startups. For instance, a team could create an AI tool to detect deepfake videos in Nigerian political campaigns. NITDA and private tech firms can sponsor this event, starting in 2026, to foster innovation.

f. **Strengthen Cross-Border Cybercrime Task Force:**
Create a West Africa Cyber Task Force with ECOWAS partners to tackle regional cybercrime. This task force will use IBM X-Force Exchange, a cloud-based platform for sharing threat intelligence across borders. It will speed up evidence sharing and extradition for cases like cross-border 419 scams. Nigeria can lead this initiative, launching it by 2027, with support from Interpol.

g. **Embed Cybersecurity in School Curricula:**
Add a CyberSmart Curriculum to primary and secondary schools. Teach students about safe internet use, password security and spotting scams. Use gamified lessons, like virtual "scam buster" challenges, to engage students. The Ministry of Education can roll this out by 2028, targeting 80% of schools nationwide.

h. **Incentivize Corporate Cybersecurity Compliance:**
Offer tax breaks to companies that adopt advanced cybersecurity tools, like CrowdStrike Falcon, which uses AI to prevent ransomware. Firms must certify their systems annually to qualify. This will encourage banks and telecoms to invest in security. The Federal Inland Revenue Service can implement this by 2026, aiming to secure 70% of major firms.

Table 5: Policy Recommendations & Responsible Agencies

Recommendation	Responsible Agency	Expected Impact
Deploy FraudSense AI for fraud detection	Central Bank, Banks & NCC	Faster detection of financial fraud
Launch CyberSafe Naija app	NITDA, Local Developers	Increased public cybersecurity awareness
Form Nigeria CyberShield Alliance	EFCC, NPF, NCC, Telcos & Universities	Improved threat data sharing and training
Establish Community Cyber Hubs	Ministry of Communications & NPF	Enhanced local training and threat response
Host Naija CyberHack annually	NITDA & Tech Firms	Innovative local cybersecurity solutions
Create West Africa Cyber Task Force	ECOWAS, Interpol& EFCC	Stronger regional cybercrime prosecution
Implement CyberSmart Curriculum	Ministry of Education	Educated youth to reduce cybercrime risks
Offer tax breaks for cybersecurity compliance	Federal Inland Revenue Service	Higher corporate investment in security

Conclusion

Cybercrime in Nigeria has grown from simple 419 scams to highly sophisticated attacks using artificial intelligence, deepfakes and cryptocurrency fraud. These crimes are a threat to national security, they also weaken the economy and damage public trust in digital systems. Nigeria has made progress with laws like the Cybercrime Prohibition and Prevention Act and policies such as the National Cybersecurity Policy and Strategy. However, weak enforcement, outdated technology, low public awareness and poor coordination between agencies continue to hold back results.

The findings show that fighting cybercrime is not only about technology, it is also about people, skills and cooperation. Laws must keep up with new threats, law enforcement must be well-trained and well-equipped and citizens must understand how to protect themselves online. If Nigeria increases its investment in cybersecurity, builds capacity across law enforcement, raises public awareness and works more closely with international partners, it can turn the tide against cybercrime. The cost of inaction is too high, both for the country's economy and for the safety of its citizens. The time to act is now.

References

Aleke, F. A., Edegbe, G. N., Omaji, S., & Olayinka, A. S. (2023). Combating cybercrime perpetrated via social media channels using individual resilience techniques. *Nigerian Journal of Cybersecurity Research, 5*(2), 45-60. Retrieved from https://journals.covenantuniversity.edu.ng/index.php/cjict/article/view/4065

Aminu, A. M. (2024). International Criminal Police Organisation and the challenges in the fight against cybercrime in Nigeria. *Journal of Security Studies, 12*(1), 89-104. Retrieved from https://journals.fukashere.edu.ng/index.php/kjpir/article/view/178

Barclays. (2022). Protect your computer. https://international.barclays.com/security/protect-your-computer/

Daniels, O. (2023). National cybersecurity policy and strategy of Nigeria: A case study. *African Journal of Policy and Governance, 9*(3), 112-130. Retrieved from https://www.proquest.com/openview/8b8c7572fd57093a27b57e808ec68aff/1?cbl=18750&diss=y&pq-origsite=gscholar

Darktrace. (2022). Major French hospital group stops ransomware attack with Darktrace AI [Press release]. https://www.darktrace.com/news/major-french-hospital-group-stops-ransomware-attack-with-darktrace-ai

Ebenezer, A. E. (2019). Strategic assessment of cybercrime control through cybersecurity and resilience by cybersecurity centers: A case study of the Nigerian experience. *Journal of Information Security & Intelligence, 6*(4), 75-91. https://www.globalacademicstar.com/download/article/strategic-assessment-of-cyber-crimes-control-through-cyber-security-and-resilience-by-cyber-security-center-a-case-study-of-the-nigeria-experience.pdf

Ezeji, C. (2024). Challenges faced by the criminal justice system and role players in combating cybercrime in Nigeria. *African Law Journal, 11*(2), 45-58. Retrieved from https://ir.nilds.gov.ng/handle/123456789/157

Federal Republic of Nigeria. (2024). *Cybercrime (Prohibition, Prevention, etc.) Act, 2024*. *Government of Nigeria*. Retrieved from https://placng.org/i/wp-content/uploads/2024/05/Cybercrimes-Prohibition-Prevention-etc-Amendment-Act-2024.pdf

Federal Republic of Nigeria. (2021). *National Cybersecurity Policy and Strategy, 2021*. *Government of Nigeria*. Retrieved from https://cert.gov.ng/ngcert/resources/NATIONAL_CYBERSECURITY_POLICY_AND_STRATEGY_2021.pdf

Interpol. (2022). *Cybercrime trends in Africa: Annual report. International Criminal Police Organization*. Retrieved from https://www.interpol.int

Kshetri, N. (2019). *Cybercrime and cybersecurity in the global South: The case of Nigeria*. *Springer*. Retrieved from https://www.researchgate.net/publication/317847658_Cybercrime_and_Cybersecurity_in_the_Global_South

Makeri, Y. A. (2017). Cybersecurity issues in Nigeria and challenges. *International Journal of Cyber Law & Security, 5*(1), 33-49. Retrieved from https://kiu.ac.ug/assets/publications/196_cyber-security-issues-in-nigeria-and-challenges.pdf

Nwankwo, W., & Ukaoha, K. C. (2019). Socio-technical perspectives on cybersecurity: Nigeria's cybercrime legislation in review*. Nigerian Journal of Cyber Law, 7*(1), 98-120. Retrieved from https://www.academia.edu/40871832/Socio_Technical_Perspectives_On_Cybersecurity_Nigerias_Cybercrime_Legislation_In_Review

Olayemi, O. J. (2014). A socio-technological analysis of cybercrime and cybersecurity in Nigeria. *Journal of Information Technology & Society, 8*(3), 55-73. Retrieved from https://academicjournals.org/journal/IJSA/article-full-text-pdf/A79763043710

Osho, O., & Onoja, A. D. (2015). National cybersecurity policy and strategy of Nigeria: A qualitative analysis. *African Journal of Cyber Governance, 9*(1), 22-40. Retrieved from https://www.researchgate.net/publication/282026229_National_Policy_and_Strategy_of_Nigeria_A_Qualitative_Analysis

Standard Bank of South Africa. (2023). Standard Bank of South Africa annual integrated report 2023. https://www.standardbank.com/static_file/StandardBankGroup/filedownloads/RTS/2023/SBSA_AnnualReport.pdf

Taofeek, O. K., & Mande, S. (2023). The impact of cybersecurity strategy in combating cyber-crime and attacks in organizations: Study of Halogen Security Company Limited, Ikeja, Lagos. *Policy and Security Management Studies, 1*(2), 88-105. Retrieved from https://www.researchgate.net/publication/375770757_THE_IMPACT_OF_CYBER_SECURITY_STRATGEGY_AND_AWARENESS_IN_COMBATTING_CYBER_CRIME_IN_ECONOMY_AND_ORGANIZATIONS_STUDY_OF_HALOGEN_SECURITY_COMPANY_LIMITEDIKEJA_LAGOS

Tijjani, H. (2023). Police effective fight against cyber-crime in Nigeria: Assessment of the perceptions of the members of the public in Bauchi Metropolis. *Journal of Criminology and Policing, 14*(1), 65-79. Retrieved from https://fjcss.fuoye.edu.ng/index.php/fjcss/article/view/71/67