International Journal of Criminal Justice Reform

CYBERCRIME ECOSYSTEM: LAWS, LOOPHOLES, AND THE SEARCH FOR EFFECTIVE SOLUTIONS AGAINST THE PROPAGATION OF CYBERCRIME IN NIGERIA

[1]Emmanuel C. Ndubuisi, [2]Charles C. Umelue

[1]Segna Chambers (Legal Practitioners and Company Secretaries), Enugu State
Email: Ndubuisiemmac@gmail.com Tel: +234 706 212 6064

[2]Sir C. L. Ndukaihe & Co. (Legal Practitioners), Anambra State
Email: Charlygod221@gmail.com Tel: +234 707 314 6460

Corresponding Author: Emmanuel C. Ndubuisi; Segna Chambers (Legal Practitioners and Company Secretaries), Enugu State,
Email: Ndubuisiemmac@gmail.com Tel: +234 706 212 6064

DOI: HTTPS://DOI/10.5281/ZENODO.19191611

ABSTRACT

Nigeria's rapid digital transformation has come at a steep price: the country now ranks among the global epicenters of cybercrime, both as a major source of perpetrators and as one of the most heavily victimized populations. This paper dissects the entire cybercrime ecosystem. From neighborhood "Yahoo Boys" and organized fraud syndicates in Lagos, Benin City, and Port Harcourt to the international money-laundering networks that cash out their proceeds. This work analyses the current legal framework, anchored by the Cybercrimes (Prohibition and Prevention) Act 2015 as amended in 2024, in addition to other legislations, and exposes the wide gaps that remain in the ecosystem along with provisions that have not kept pace with an evolving landscape, chronic under-funding of digital forensics; sluggish international cooperation. the study documents the loopholes that allows criminal innovation to outrun regulatory response consistently. Existing countermeasures against cybercrime, such as public awareness drives, the National Cybersecurity Policy and Strategy, and scattered public-private initiatives among others are assessed for reach, impact, and sustainability, with most found severely wanting. The paper closes with a pragmatic,

IJCJR VOL. 2, ISSUE 1, PP 45– 67, 2026
DOI: HTTPS://DOI/10.5281/ZENODO.19191611
PUBLISHED 23-03-2026
WWW.EMSAJPUBLISHERS.ORG/IJCJR

sequenced reform package: precise legislative amendments to cover emerging threats, compulsory digital-literacy modules in secondary education, a fully resourced and independent national CERT, dedicated ring-fenced budgets for cyber units within the police and EFCC, and a binding ECOWAS-wide protocol for real-time evidence exchange and joint operations. In the same aegis, this study would highlight the challenges plaguing the application and enforcement of the Cybercrime Act, in line with streamlining Nigeria's ICT landscape with world-best standards. Unless Nigeria moves decisively to close both the statutory gaps and the enforcement deficit, Nigeria's digital economy will continue to grow in the shadow of an unchecked criminal underworld.

KEYWORDS: Cybercrime, Nigeria, International cooperation, Financial crimes, Enforcement, Cyberlaws.

INTRODUCTION.

DEFINITION OF TERMS:

WHAT IS CYBERCRIME?

According to Encyclopedia Britannica, Cybercrime is the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography, and intellectual property, stealing Identities, or violating privacy. On the other hand, the United States Immigration and Customs Enforcement defined Cybercrime as any illegal activity carried out using computers or the internet. Any criminal activity that involves a computer, either as an instrument, target, or a means for perpetuating further crimes, comes within the aegis of cybercrime. A generalized definition of cybercrime may be "unlawful acts wherein the computer is either a tool or target or both". (Chawki et al, p. 3) From the definition above, a necessary ingredient to qualify an illegal act as a cybercrime is the usage of a computer or internet either as a means, or a means to an end. These points in the direction that cybercrime is a side product of advancement in technology and information.

Essentially, the key elements obtainable for a balanced definition of Cybercrime are that it involves the performance of an illegal Act or Acts, by an individual and or by

an individual as an extension of an organization, usually a crime syndicate with the aid of a computer, or the internet.

It is relevant to note that there is no express definition of the term cybercrime under the Cybercrime Act of 2015 and the Cybercrime (Prohibitions and Preventions etc.) (Amendment) Act 2024. However, in the Cybercrime Act of 2015, some acts were outlined as constituting a cybercrime; these acts include cybersquatting, cyberstalking, child pornography, identity theft, cyber terrorism, and intellectual property theft, etc.

The authors will go ahead to define Cybercrime as any illegal activity that is facilitated by the use of computers, networks, or the internet either as a tool, or as a target.

BRIEF HISTORY OF CYBERCRIME LEGISLATION IN NIGERIA

The advent of Cybercrime in Nigeria is an offspring of the infamous "419 scam" culled from section 419 of the Criminal Code, which began in the late 1990s and early 2000s, when uneven internet access created an opening for unemployed, tech-inclined youths popularly addressed as "Yahoo Boys" to pioneer global advance-fee fraud schemes. These scams relied on persuasive emails promising wealth in exchange for upfront payments, among other persuasive tactics employed to scam unsuspecting individuals. Unsurprisingly, they generated millions of dollars while tarnishing Nigeria's international image. According to The Register, as of 2003, U.S. annual losses alone had exceeded $500 million, with Nigeria taking a chunk enough to garner a reaction from the government of the day under the leadership of President Olusegun Obasanjo to constitute the Presidential Committee on 419 Activities in Cyberspace to investigate the growing problem and propose solutions.

From 2005 onwards, attempts were made to enact legislation on cybercrime and related issues, such as:

IJCJR VOL. 2, ISSUE 1, PP 45– 67, 2026
DOI: HTTPS://DOI/10.5281/ZENODO.19191611
PUBLISHED 23-03-2026
WWW.EMSAJPUBLISHERS.ORG/IJCJR

A. Computer Security and Critical Infrastructure Bill (2005); Electronic Service Provision Bill (2008)
B. Interception and monitoring Bill (2009); Cyber Security Bill (2011); Criminal Code Amendment for Offences Relating to Computer Misuse and Cybercrimes (2011); Electronic Transfer of Funds Crime Bill (2011)

It is instructive to state that none of these bills were passed into law.

Interestingly, in 2011, an amendment of the Evidence Act facilitated the cause to an extent by formally recognizing digital evidence in court. However, without a specifically dedicated cybercrime law upon which they can institute actions, prosecutors relied on sparse Statutes such as the 2004 EFCC Act and the 2006 Advance Fee Fraud Act, which resulted in merely a few convictions and significant complications, especially in cases of cross-border incidents, and new technologies.

A massive breakthrough came in February 2015 with the release of the National Cybersecurity Policy and Strategy, which officially recognized cyber threats as matters of national security, and a follow-up later in May 15, 2015, when President Goodluck Jonathan signed the Cybercrimes (Prohibition, Prevention, etc). Act into law. It became Nigeria's first unified legal framework for tackling offenses such as unauthorized access, online fraud, and attacks on critical infrastructure, while also strengthening international cooperation. Thus, it can be posited that after what seemed like years of operating in a digital wild west, Nigeria finally has a long-overdue working Sheriff.

CYBERCRIME AND LEGAL FRAMEWORK IN NIGERIA

According to the National Bureau of Statistics (NBS), cybercrime in Nigeria is a serious problem, with the country being ranked as one of the top countries in the world known for internet fraud. The International Criminal Police Organization (Interpol) has also reported an increase in the number of cybercrime cases in Nigeria, especially financial fraud committed with the aid of the internet and social media platforms.

Cybercrime has become an issue of concern all over the world today. This is invariably due to the widespread adoption of technology and the internet in different

sectors of the economy. It is also true that despite the massive advantage of Information, Communication, and Technology, the risks occasioned by the advent of the internet keep becoming enormous by the day. The loopholes created in cyberspace have become a tool for cybercriminals to use in the exploitation of others. The growth of cybercrime in Nigeria has put Nigeria at an economic loss and loss of good international reputation, amongst other things. Due to the increasing rate of cybercrime, the legislative arm of government enacted the Cybercrime Act of 2015.

This paper explores the legal ecosystem governing cybercrime in Nigeria, with the Cybercrime (Prohibition, Prevention, etc.) Act of 2015, other legislations, their effectiveness, challenges, and recommendations for improvements.

Below are some of the Legislations Governing Cybercrime in Nigeria:

PRIMARY LEGISLATION

1. Cybercrime (Prohibition, Prevention, etc.) Act 2015

OTHER LEGISLATIONS

1. Economic and Financial Crimes Commission Act 2004
2. Advance Fee Fraud and other Fraud Related Offences Act
3. Money Laundering (Prevention and Prohibition) Act
4. Evidence Act 2011
5. Administration of Criminal Justice Act (ACJA) 2015

1. CYBERCRIME (PROHIBITION, PREVENTION, ETC.) ACT 2015

The Cybercrime Act is the primary legislation governing the jurisprudence of Cybercrime in Nigeria. This Act outlines a range of specific cyber-related offences in Part III (Offences and Penalties). The provisions criminalize various digitized illegitimate acts, with penalties typically including fines, imprisonment, or both in certain instances. The Act focuses on protecting computer systems, data, critical infrastructure, and children from exploitation, and public order, while also addressing fraud and content-based crimes.

In outlining some of the key provisions of the acts, we included the relevant section number, a brief description of the offence, and key penalties below:

1. **Section 27 (1) a, and b**: Aiding or Abetting Cybercrimes, Conspiracy and Attempts, knowingly assisting in any offence under the Act (e.g., providing tools for hacking). Penalty: Same as the principal offence. Agreeing to commit or attempting any cyber offence. Penalty: Up to half the term for the completed offence.
2. **Section 23**: Child Pornography and Child Exploitation Production, distribution, or possession of child pornography via electronic means, or luring minors online for sexual purposes. The penalty provided ranges from 10 years imprisonment to a minimum of 5 years or a fine of ₦20 million, ₦10 million, or both, depending on the particular subsection flouted
3. **Section 18:** provides for the offence of cyber terrorism, and sanctions it with life imprisonment. For clarity, the act defines Cyber terrorism as having the same meaning under the Terrorism (Prevention) Act, 2011, as amended.
4. **Section 5**: of the Act provides that a person who, with intent, commits any offence punishable under this Act against any critical national information infrastructure is liable to be punished with 10, 15, or life imprisonment, depending on the section that was flouted.
5. **Section 24**: Cyberstalking Using electronic means to monitor, threaten, or harass another person without consent. Penalty: Up to 3 years imprisonment or a fine of ₦7 million, or both.
6. **Section 42:** establishes the Cybercrime Advisory Council, while **Section 43** goes ahead to delineate their functions, such as:

    a) Formulating and providing general policy guidelines for the implementation of the provisions of the Act,
    b) To advise on measures to prevent and combat computer-related offences, cybercrimes, threats to national cyberspace and other cyber security related issues;
    c) To establish a program to award grants to institutions of higher education to establish Cyber security Research Centers to support the development of new Cyber security defences, techniques and processes in the real-world environment;

d) to promote Graduate Traineeships in Cyber security and Computer and Network Security Research and Development
e) The Council is also empowered to regulate its proceedings and make standing orders with respect to the holding of its meetings, notices to be given, the keeping of minutes of its proceedings and such other matters as Council may, from time to time determine.

7. **Section 51:** makes offences under the act extraditable, under the Extradition Act, CAP E25, Laws of the Federation of Nigeria, 2004. Along with **Section 52-56** of the Cybercrime Act**,** all bolster the readiness of the federation to grant assistance in terms of international incidents.

For more details and perusal on the provisions of the Cybercrime Act, they are provided under Part III particularly from Sections 5-49

ECONOMIC AND FINANCIAL CRIMES COMMISSION ACT 2004

The Economic and Financial Crimes Commission (Establishment, etc.) Act, 2004 was enacted on June 4, 2004. It established the Economic and Financial Crimes Commission (EFCC) as Nigeria's primary agency for combating economic and financial crimes, including those with digital or cyber elements like advance-fee fraud (e.g., "419 scams" via email) and computer-related credit card fraud. The Act does not define the term "cybercrime" explicitly, but empowers the EFCC to investigate and prosecute financial crimes facilitated by technology and cyber-related offences indirectly through powers over economic/financial crimes, and the functions that is provided in Part II of the Act.

Key sections under the EFCC Act:

Section 6: Outlines the EFCC's general functions, including: Investigating and prosecuting offences under the Criminal Code, Penal Code, and other laws (e.g., fraud via digital platforms). Specific duties such as tracing assets from cyber-enabled crimes and coordinating with international bodies for cross-border digital frauds. **Section 7**: Mandates the EFCC to enforce all economic/financial crime laws, with subsection (2) listing specific statutes (e.g., the Money Laundering Act 2003, the

Advance Fee Fraud and Other Fraud Related Offences Act 1995, the Failed Banks (Recovery of Debts) and Financial Malpractices in Banks Act 1994, as amended, the Banks and other Financial Institutions Act 1991, as amended, Miscellaneous Offences Act) that encompass cyber variants like email-based deception and electronic money laundering. **Subsection (2)(f)** coordinates with the Criminal and Penal Codes for digital fraud prosecutions.
Sections 6 and 34: Empowers the commission to freeze accounts and assets that are obtained from economic and financial crimes.

ADVANCE FEE FRAUD AND OTHER FRAUD RELATED OFFENCES ACT

The Advance Fee Fraud and Other Fraud Related Offences Act, 2006 (Cap. A5, Laws of the Federation of Nigeria 2004, as amended through Act No. 62 of 2007) was enacted on June 5, 2006, replacing the earlier Advance Fee Fraud and Other Fraud Related Offences Decree No. 13 of 1995 and its 2005 amendment. It specifically targets advance-fee schemes such as common "419 scams" along with related fraudulent inducements, which were frequently executed using electronic channels like email and the internet, making the Act a key instrument for prosecuting cyber-enabled fraud before the enactment of the 2015 Cybercrimes Act. Although the Act does not explicitly refer to "cybercrime," it criminalizes digital fraud by addressing false pretences and technologically facilitated inducement, enforceable by the EFCC or the police.

Key Sections that relate to Cybercrime

The Act concentrates on fraud transmitted through communicative channels, including electronic media such as email and online solicitations. Key provisions include:

Section 1: Obtaining Property by False Pretence, etc.
Prohibits obtaining property (including money) through false pretence with intent to defraud by any medium, including electronic communication (e.g., phishing emails that offer inheritance payouts contingent on upfront payments). Applies to fraudulent inducement originating either in Nigeria or abroad.
Penalty: 7–20 years imprisonment, with no option of fine.

Section 2: Other Related Offences
Addresses broader fraudulent acts, including inducing others to confer economic benefits based on deceptive claims (e.g., online requests for "processing fees") and evading obligations using digital channels.
Penalty: Up to 20 years imprisonment.

Section 3: Use of Premises
Forbids knowingly using premises (including cybercafés or residential setups) for activities involving offences under the Act, such as electronically run scam operations.
Penalty: Up to 15 years imprisonment; forfeiture of the premises.

Section 4: Fraudulent Invitation
Makes it an offence to invite or persuade victims to enter Nigeria for fraudulent purposes (e.g., fake online travel-linked advance-fee arrangements). This part aligns particularly where there is evidence of online correspondence between both parties.
Penalty: 7–20 years imprisonment.

Section 5: Receipt of Fraudulent Document by Victim Constituting Attempt
Treats receipt of fraudulent material (including fake emails and PDF attachments) as an attempt to commit fraud, allowing prosecution of cyber-related preparatory activities.
Penalty: Same as the completed offence (up to 20 years imprisonment).

Section 6: Possession of Fraudulent Document Constituting Attempt
Criminalizes possession of fraudulent documents (e.g., digital scam templates, spoofed emails) intended to facilitate fraud, targeting possession of cyber-fraud toolkits.
Penalty: Up to 15 years imprisonment.

Section 7: Laundering of Funds Obtained Through Unlawful Activity, etc.
Prohibits laundering proceeds derived from fraudulent activity (including routing electronic scam proceeds through bank accounts or digital-wallet transfers), and applies to financial institutions that fail to exercise required diligence in electronic transactions.

Penalty: 7–14 years imprisonment; fines up to twice the amount laundered; asset forfeiture.

MONEY LAUNDERING (PREVENTION AND PROHIBITION) ACT

The Money Laundering (Prevention and Prohibition) Act, 2022, was signed into law on 12 May 2022 by Muhammadu Buhari, replacing the earlier Money Laundering (Prohibition) Act of 2011 (as amended). It is Nigeria's current principal anti-money laundering statute, and it explicitly treats most cybercrimes, especially online fraud, ransomware, cryptocurrency scams, and business email compromise as predicate offences. Proceeds from such crimes must be reported and can be confiscated under the new law. Because cyber-fraud (especially online scams) remains one of Nigeria's largest sources of illicit funds, the 2022 Act has effectively become the single most important tool, after the 2015 Cybercrimes Act itself, for disrupting and confiscating proceeds from cybercrime. By tying cyber-fraud to money-laundering offences and extending regulation to virtual-asset service providers, it significantly closes some substantial loopholes.

Specific Sections that Directly or Indirectly Address Cybercrime

1. **Section 3: Offence of Money Laundering** Criminalizes converting, transferring, concealing, or disguising proceeds of any "unlawful act." The Act's First Schedule lists more than 30 predicate offences, many of which are cybercrimes under the 2015 Cybercrimes Act (e.g., computer-enabled fraud, identity theft, phishing, hacking for financial gain). Thus, proceeds from scams, SIM-swap frauds, ransomware payments, or crypto scams fall within its scope.
2. **Section 7: Retention of Proceeds of Criminal Conduct** Makes it an offence for any person or entity to retain funds known or suspected to be derived from cyber-fraud. This empowers banks, fintech firms, and other regulated institutions to freeze accounts tied to romance scams, business email compromise schemes, or other online frauds.
3. **Section 10: Obligation to Report Suspicious Transactions** Obligates banks, fintech, crypto exchanges, and other regulated entities (Designated Non-Financial Businesses and Professions, DNFBPs) to file Suspicious Transaction Reports (STRs) with the Nigerian Financial

Intelligence Unit (NFIU) within 24 hours if a transaction appears to involve proceeds of cyber-fraud. In practice, this is the most frequently used mechanism for freezing or investigating online-fraud-linked accounts.

4. **Section 16: Offences by Financial Institutions and DNFBPs**
   Imposes heavy penalties, potentially very large fines, on financial or non-financial institutions that fail to monitor or report suspicious electronic transfers linked to cyber-fraud.
5. **Section 18: Virtual Asset Service Providers (VASPs)**
   A new 2022 inclusion: The Act extends its reach to crypto-related platforms, explicitly bringing cryptocurrency exchanges, virtual assets, wallets, and peer-to-peer traders under AML regulation for the first time. This directly targets the laundering of cyber-fraud proceeds via cryptocurrencies such as Bitcoin, USDT, and others, closing a major loophole present under the 2011 Act.
6. **First Schedule – Predicate Offences**
   Lists offences under the 2015 Cybercrimes Act, the 2006 Advance Fee Fraud Act, and the relevant provisions of the Terrorism (Prevention) Act among the predicate offences whose proceeds trigger money-laundering liability under the 2022 Act. This schedule legally binds virtually every major form of cybercrime to money-laundering liability under the ML(PP)A.

EVIDENCE ACT & ADMINISTRATION OF CRIMINAL JUSTICE ACT

The Evidence Act and the Administration of Criminal Justice Act are both procedural laws that govern the trial and prosecution of persons under the various Legislations. Trials of offences are treated as regular trials; hence, there is no express provision as to cybercrimes and definitions, except for the Evidence Act in Section 84, which provides for the admissibility of computer-generated evidence. It also goes ahead to provide the conditions that must be fulfilled before they can be admissible.

IJCJR VOL. 2, ISSUE 1, PP 45– 67, 2026
DOI: HTTPS://DOI/10.5281/ZENODO.19191611
PUBLISHED 23-03-2026
WWW.EMSAJPUBLISHERS.ORG/IJCJR

INSTUTIONAL FRAMEWORK AND THEIR ROLES.

THE ECONOMIC AND FINANCIAL CRIMES COMMISSION (EFCC)

The EFCC's Role in Enforcing the Cybercrimes Act in Nigeria is that of a go-to agency for cracking down on economic sabotage, including the digital underscore of cybercrimes that have made headlines for years. Set up under the Economic and Financial Crimes Commission (Establishment, etc.) Act of 2004, it was largely a response to global outcry over "419" scams and money laundering dragging Nigeria's name through the mud. Its job is clear: investigate, prosecute, and prevent financial crimes, with cybercrimes like advance-fee fraud, phishing, and ransomware falling right under its umbrella, often paired with the 2015 Cybercrimes Act for muscle.

Section 6 of its Act gives it the green light to probe digital frauds from romance scams to big-league business email compromises. With a record of nearly 1,000 suspects in Lagos and Abuja raids nabbed, including 177 Chinese nationals tied to organized scam factories, they have also teamed up with Interpol and the FBI for cross-border busts, like seizing assets from UK-based rings with Nigerian roots.

Despite the advancement and grounds gained on paper, it is necessary to also address the loopholes of the Economic and Financial Crimes Commission in the same breath, over the years, there has been alleged deviation from the spirit of the legislation by the enforcement unit of the EFCC, with recorded incidents purportedly carried out by officers of the commission, for instance, in the early hours of November 1 2025, officers of the commission carried out a raid at the Obafemi Awolowo University off-campus that led to the mass arrest of over 50 students, this resulted in backlashes and protests from various quarters, the chairman of the Commission subsequently placed a ban on night time sting operations pending review of arrest/bail procedures, on the other hand, there has been repeated judicial rulings showing limits on EFCC’s extra-judicial freezes such as in the cases of Mike Ozekhome, Raymond Dokpesi, demonstrating a pattern of courts checking EFCC practices on asset restrictions.

It is important to mention that the Nigeria Police Force is saddled to work in conjunction with officers of the Financial Crimes Commission to investigate and prosecute cybercriminals.

NIGERIAN COMMUNICATIONS COMMISSION (NCC)

The Nigerian Communications Commission (NCC) plays a vital role in curbing cybercrime in Nigeria. The NCC is the regulatory authority responsible for managing Nigeria's communication sector, including internet services and telecommunications. As part of its duties, the NCC works with other stakeholders, such as law enforcement agencies, to develop policies and strategies to prevent cybercrime.

JURISDICTIONAL COMPARISON

CHINA

GENERAL OVERVIEW OF CHINA'S CYBERCRIME JURISDICTION

KEY LEGISLATIVE BACKBONE: As of 2025, China's cybercrime jurisprudence is embedded in a state-centric, multi-layered legal framework that prioritizes national security, data sovereignty, and technological innovation while imposing stringent controls on Networks and Artificial Intelligence. The cornerstone of Cybercrime in China is the Cybersecurity Law (CSL) of 2017, amended on October 28, 2025 (set to become effective on January 1, 2026), a major update since its enactment, which strengthens enforcement, introduces AI-specific governance, and aligns with the Personal Information Protection Law (PIPL, 2021) and Data Security Law (DSL, 2021).

The amendments in the Cybersecurity Law adopt a "small-incision" approach, strengthening sanctions (including penalty increases of up to ten times for certain violations), incorporating Artificial Intelligence (AI) governance measures, such as requirements for "secure and controllable" AI development supported by risk assessments, tightening regulatory obligations for network operators and Critical

Information Infrastructure (CII), and extending the law's extraterritorial reach to address foreign-based threats.

The revised CSL is also more closely harmonized with the Personal Information Protection Law (PIPL, 2021) and the Data Security Law (DSL, 2021), forming a coordinated regulatory framework enforced primarily by the Cyberspace Administration of China (CAC) and the Ministry of Public Security (MPS).

In China, Criminal offenses of a cybersecurity nature are prosecuted under Criminal Law Articles (e.g., unauthorized access, data infringement, up to life imprisonment for severe cases), with administrative enforcement by the Cyberspace Administration of China (CAC) and the Ministry of Public Security (MPS). The Supreme People's Court (SPC) plays a pivotal role through exemplary rulings for guidance and binding precedents, emphasizing systemic risks over individual harms. With courts focusing on AI-enabled crimes, data scraping, and extortion incidents.

Judicial interpretation of the CSL is significantly influenced by guiding cases and typical cases issued by the Supreme People's Court (SPC), which are binding on lower courts and frequently emphasize assessments of "social harm." In 2025, enforcement activity included more than 67,000 indictments for telecommunications and cyber-fraud offences, according to Beijing Dacheng Law Offices LLP in their monthly Data Protection Update 2025.

Below is a chapter-by-chapter examination of the 2017 Cyber Security Law with reference to the 2025 amendments where relevant. It is followed by a comparative discussion vis-à-vis Nigerian jurisprudence. For ease of reference and clarity, the articles are grouped into chaptered batches with a general heading.

Chapter I: General Provisions (Articles 1–14)
This chapter establishes the core principles of the Cybersecurity Law by defining its application to mainland China and emphasizing the simultaneous development of cybersecurity and digital advancement. It introduces a national cybersecurity strategy, systems for risk monitoring and prevention, and standards for lawful and responsible online behavior. The framework promotes international cooperation toward a secure and open cyberspace, assigns a central coordinating role to the national cyberspace authority, and places clear security obligations on network

operators while encouraging industry self-regulation. It prohibits conduct that endangers national security or infringes lawful rights, provides special protection for minors, and sets up formal reporting mechanisms. The 2025 amendments broaden the law's reach to cover harmful foreign conduct and strengthen the role of Communist Party leadership in cybersecurity governance.

Chapter II: Support and Promotion of Network Security (Articles 15–20) This chapter focuses on strengthening cybersecurity through the establishment of technical standards, state investment in cybersecurity technologies, and the development of supporting services such as certification and risk assessment. It addresses the secure use and management of data, promotes public education on cybersecurity, and emphasizes the training and development of skilled cybersecurity professionals. The 2025 amendments expand this framework to explicitly include artificial intelligence, introducing requirements for ethical oversight, risk supervision, and assessments to support the development of AI that is secure and controllable.

Chapter III: Network Operations Security (Articles 21–39) This chapter sets out comprehensive operational security obligations for network operators, distinguishing between general requirements and stricter rules for critical information infrastructure. Operators are required to adopt tiered protection systems, establish internal controls, monitor network activity, protect data, ensure their products and services meet security standards, apply real-name registration, and maintain effective emergency response mechanisms. Unauthorized intrusions are prohibited, and operators must cooperate with lawful investigations. Critical information infrastructure receives enhanced protection, including security safeguards during construction, specialized management, national security reviews for sensitive procurements, data localization, and regular security assessments, all coordinated by the Cyberspace Administration of China through inspections, testing, and drills. The 2025 amendments significantly strengthen enforcement by increasing penalties, extending supply-chain responsibility to users and purchasers of non-compliant products, and imposing stricter incident reporting obligations.

Chapter IV: Network Information Security (Articles 40–50) This chapter focuses on protecting network information and personal data. It requires confidential handling of user information, lawful and consent-based data collection,

and the adoption of strong security safeguards. Individuals are granted rights to correct or delete their data, while the unlawful acquisition, use, or sale of personal information is strictly prohibited. Government authorities are also subject to confidentiality obligations. The law bans platforms that facilitate criminal activity, places clear content management responsibilities on network operators, and prohibits the creation or spread of malicious software. It further establishes complaint mechanisms and regulatory oversight to ensure compliance. The 2025 amendments significantly strengthen enforcement by imposing much higher fines on platforms that fail to remove illegal content and by streamlining procedures for responding to data breaches.

Chapter V: Monitoring, Early Warnings, and Emergency Responses (Articles 51–58)
This chapter provides a national framework for monitoring cybersecurity risks and responding to incidents. It establishes early-warning and monitoring systems, sector-specific reporting channels, and comprehensive emergency response plans. The chapter sets out graduated measures for managing risks, clear procedures for incident response, supervisory engagements with network operators, and coordination with other emergency response laws, including the option of temporary network restrictions to protect security. The 2025 amendments introduce only limited changes, mainly strengthening coordination in addressing risks associated with artificial intelligence.

Chapter VI: Legal Responsibility (Articles 59–75)
This chapter outlines the legal consequences for violations of the law, covering penalties for failures to comply with security obligations, the creation or use of malicious programs, breaches of real-name registration requirements, and infringements of personal data rights. Stricter sanctions apply to violations involving critical information infrastructure, alongside the possibility of public security measures and criminal liability. The law also sanctions against foreign actors whose conduct harms China's cybersecurity. The 2025 amendments substantially increase penalty levels, introduce opportunities for leniency where violations are voluntarily corrected, and add stronger enforcement tools such as business suspension.

Chapter VII: Supplementary Provisions (Articles 76–79)
The final chapter defines key terms, clarifies the interaction with state secrecy laws,

addresses military networks, and specifies the law's effective date. There is no amendment to this chapter for 2025.

ASPECT-BY-ASPECT COMPARISON BETWEEN CHINA'S CYBERCRIME JURISPRUDENCE AND NIGERIA

AI Governance
China explicitly regulates artificial intelligence by requiring ethical standards and risk assessments, with courts actively addressing deepfake misuse. Nigeria has no dedicated AI provisions, leaving issues such as deepfakes to be addressed indirectly under general fraud laws.

Data Localization and Export Controls
China mandates that certain data be stored domestically and subjected to security reviews before cross-border transfer. Nigeria does not impose compulsory data localization, relying instead on a separate data protection framework.

Critical Information Infrastructure (CII) Protection
China operates a structured, tiered protection regime for critical infrastructure, including security reviews, backups, and heavy penalties for non-compliance. Nigeria lacks a defined CII framework and relies on broadly framed national security provisions.

Real-Name Registration
China requires real-name registration for network services as a core security measure. Nigeria does not impose a general real-name registration obligation, applying it only selectively.

Extraterritorial Enforcement
China provides for sanctions against foreign actors whose conduct threatens its cybersecurity, including asset freezes. Nigeria's approach is largely territorial, with weak mechanisms for cross-border enforcement.

Civil and Administrative Penalties
China employs graduated administrative penalties, including fines, suspensions, and leniency mechanisms. Nigeria's framework is primarily criminal in nature, with limited use of flexible or preventive remedies, despite the fact that there has been a

recent campaign for the application of plea bargains in certain instances, a welcome development which is still in its infancy.

Specialized Judicial Structures
China assigns complex cyber and data disputes to specialized internet courts. Nigeria relies on general courts, without dedicated cyber or technology-focused jurisdictions.

Overall, China's Cybersecurity Law supports a preventive, security-oriented digital economy, while Nigeria's framework remains reactive, creating significant gaps in risk management and enforcement.

CHALLENGES OF THE VARIOUS CYBERCRIME LEGISLATIONS

The 2015 Act marked a major step in addressing cyber threats in Nigeria, yet even after the 2024 amendments, gaps remain that can be exploited, shaped by limited resources, fast-changing technology, and the country's socio-political context. Based on documented legal critiques and enforcement outcomes, the following are realistic loopholes rooted in actual vulnerabilities in identifying these loopholes, We placed priority on the Cybercrime Act of 2015 and the EFCC Act:

1. **Outdated Provisions for Emerging Threats:**
   The concept of an ever-changing landscape should always be envisaged by the legislators, as there abound instances where the law is outdated in the face of emerging trends, a proper demonstration of this concept is the definitions and categorization of offences under the Act that were drafted before the widespread use of cryptocurrencies, AI-generated deepfakes, ransomware-as-a-service, voice-based phishing (vishing), cloud-system breaches, and peer-to-peer botnets. In Nigeria's expanding fintech sector, this creates room for anonymous laundering via darknet channels and SIM-swap-based fraud that fall outside traditional notions of a "computer system." In their work, Challenges in Regulating Emerging Cybercrimes in Nigeria. Dayo Akindipe highlighted this as one of the challenges plaguing the efficacy of the Act where the Act does not envisage emerging crimes in the various types of

cybercrime listed under the Nigerian cybercrime act which include but are not limited to black basta, mindware, onyx, vishing, typo squatting, cloud security breaches, unstructured P2P Botnets, including advanced persistent threat, machine learning poisoning, and artificial intelligence fuzzing, and the advanced technique of Cybercriminals using bitcoins and other crypto-assets to execute transactions in the darknet. The Nigerian Cybercrime Act did not provide for the regulation of crypto-assets or the manipulation of Bitcoin ATMs.

2. **Weak Enforcement Mechanisms:** The Act contains no binding financial commitments, training requirements, or dedicated mandates for cyber forensic laboratories for bodies such as the EFCC or the police, in a country where policing budgets still prioritize physical and street-level crimes, digital investigations frequently stall due to weak coordination among agencies, and disparities between rural and urban technological capacity. Also, a glance at section 14 (2) of the EFCC Act provides for the compounding of offences in certain instances; it is our opinion that this would create room for negotiation with unscrupulous elements in the commission. In addition, it may defeat the spirit of the legislation in the sense that it creates a false morale in deviants that there is always room for settlement with the enforcers, which is not a great image to paint to the public. It is a well-known fact that Cybercriminals can operate from anywhere in the world, making it difficult for Nigerian authorities to arrest and prosecute offenders, especially in relation to non-citizens.
3. **Gaps in Critical Infrastructure Protections:** Although Sections 3-5 identify key national sectors like financial systems, there is no clear mechanism for updating coverage to reflect newer vulnerabilities, such as cybersecurity weaknesses in internet-enabled power infrastructures. This leaves state-controlled utilities exposed in an already fragile electricity system, where hacks increase the likelihood of outages.
4. **Inadequate Resources**: There is a lack of sufficient resources and skilled personnel to enforce the provisions of the Cybercrime Act in the various institutions created to oversee and end cybercrime. Law enforcement agencies in Nigeria are often underfunded, which results in low productivity as they are not able to purchase certain devices for tracking cybercriminals. it is also sad

that we lack the technical expertise needed to investigate complex cybercrimes effectively.

5. **Technological Advancements**: This challenge is a derivative of the problem identified above, because as technology evolves, so do the methods employed by cybercriminals. The rapid pace of technological change presents challenges for the legal framework, as new forms of cybercrime continue to emerge faster than laws can be amended and even faster than we are in the procurement of technological equipment, which can aid quick investigation and detection of cybercriminals.

OTHER CHALLENGES

1. **Low Public Awareness**: A good number of Nigerians are unaware of the legal consequences of engaging in online fraud or other cybercrimes, and without this awareness the number of cybercriminals keeps growing.
2. **Lack of International Cooperation**: Cybercrime is a global problem that requires international cooperation to address effectively. While Nigeria has signed international conventions such as the **Budapest Convention on Cybercrime**, there is still a lack of robust cooperation between Nigerian law enforcement agencies and their international counterparts especially in cases where there are international actors involved.

RECOMMENDATIONS FOR STRENGTHENING NIGERIA'S CYBERCRIME LEGAL FRAMEWORK

To enhance the effectiveness of the existing legal framework, we recommend that the following steps should be taken into consideration:

1. **Training of Law Enforcement officers**: Nigeria must invest in the training of law enforcement officers, judges, and other relevant officials in cybercrime detection and investigation. Specialized training programs can help improve the technical expertise needed to deal with cybercriminal activities.

2. **Public Awareness Campaigns**: There is a need for greater public awareness about the risks of cybercrime and its legal consequences. This will help reduce the rampage of cybercrimes in Nigeria.
3. **Strengthening International Cooperation**: Nigeria should work to strengthen its international partnerships with other nations, particularly in sharing information and collaborating on cybercrime investigations. This will help overcome jurisdictional challenges, bolster existing principles already in place, and ensure that cybercriminals face justice regardless of their location.
4. **Constant amendment of the law**: The Cybercrime Act should be regularly amended to meet the changing technological landscape.
5. **Creating a Cybercrime Specialized Court**: Establishing a court that is exclusively for cybercrime cases could help streamline the legal process for prosecuting offenders. This would ensure that cases are handled by judges with the appropriate expertise and improve the overall efficiency of the judicial process, just like we have in the National Industrial Court of Nigeria.
6. **Possible Cybercrime Academy** to flip young offenders into ethical hackers.
7. It is our opinion that the sanctions contained in the Cybercrime Act are not stringent enough to serve as a deterrent against new entrants, and exit of old cows in the cybercrime landscape. Hence, they should be reviewed to be stringent.

Conclusion

Cybercrime has significantly challenged Nigeria's security, economy, legal sectors, and social stability. The enactment of the **Cybercrime (Prohibition, Prevention, etc.) Act of 2015** was a step in the right direction, but the effectiveness of the law depends on its enforcement, public awareness, and international cooperation. While there are challenges, with the right resources and continued efforts, Nigeria can strengthen its legal framework to fight against cybercrime and protect its citizens from the growing threats in cyberspace.

REFERENCE:

1. National Bureau of Statistics, "Cybercrime Statistics in Nigeria," accessed November 28, 2024.
2. **Cybercrime (Prohibition, Prevention, etc.) Act, 2015**, Laws of the Federation of Nigeria.
3. Nigerian Criminal Code Act, Cap C38, Laws of the Federation of Nigeria.
4. **Nigeria Data Protection Regulation (NDPR), 2019**, Nigeria Data Protection Bureau.
5. **The Economic and Financial Crimes Commission (Establishment, etc.) Act, 2004**
6. **Advance Fee Fraud and other Fraud Related Offences Act, 2006.**
7. Interpol, "Global Crime Trend Report 2023," International Criminal Police Organization, accessed November 28, 2024.
8. **The Money Laundering (Prevention and Prohibition) Act, 2022**
9. **Cybercrime Budapest Convention on**, Council of Europe, signed by Nigeria in 2019.
10. **Personal Information Protection Law of the People's Republic of China (PIPL), 2021.**
11. **Cybersecurity Law Of China (CSL) of 2017, amended on October 28, 2025**
12. **China Monthly Data Protection Update: November 2025 Beijing Dacheng Law Offices LLP** **https://www.lexology.com/library/detail.aspx?g=60967a59-39c1-4d43-a298-6f74756e50b0** Accessed December 18, 2025
13. https://www.britannica.com/topic/cybercrime Accessed December 1, 2025
14. https://www.ice.gov/about-ice/hsi/investigate/cybercrime Accessed December 1, 2025
15. Cybercrime, Digital Forensics and Jurisdiction, (Mohamed Chawki, Ashraf Darwish Mohammad Ayoub Khan, Sapna Tyagi, 2015)

16. Cybercrime (Prohibitions and Preventions etc.) (Amendment) Act 2024
17. https://www.theregister.com/2003/05/30/us_cyber_crime_losses_tumble/ Accessed on December 3, 2025
18. Role of The EFCC on prosecution and enforcement of Cybercrime laws https://www.coe.int/en/web/octopus/-/nigeria
19. China-linked cybercrime rings tighten grip on Africa as Nigeria becomes global fraud hotspot https://www.tribuneindia.com/news/world/china-linked-cybercrime-rings-tighten-grip-on-africa-as-nigeria-becomes-global-fraud-hotspot/
20. Cybercrime policies/ Strategies https://www.coe.int/en/web/octopus/-/nigeria
21. Several students arrested as EFCC raids off-campus hostels at OAU https://www.thecable.ng/several-students-arrested-as-efcc-raids-off-campus-hostels-at-oau/?utm
22. Court order on the freeze of Mike Ozekhome's asset https://www.thecable.ng/appeal-court-rejects-efccs-plea-to-freeze-ozekhomes-account/?utm
23. Akindipe D, Adam E (2025) Challenges in Regulating Emerging Cybercrimes in Nigeria. Global J Eng Des Technol. 14:243.
24. https://corruptioncases.ng/cases/frn-vs-ikemesit-edet-proprietor-of-uyo assessed on December 12, 2025 by 3:12 pm
25. Revisions to China's Cybersecurity Law: Strengthened Oversight and Alignment with Emerging Technologies https://www.china-briefing.com/news/china-cybersecurity-law-amendment/ assessed on December 20, 2025 by 6:10 am