Journal of NAMP 73 (2026) 13-20

The Nigerian Association of Mathematical Physics

Journal homepage: https://nampjournals.org.ng

CYBER-CRIME LEGISLATION AND ENFORCEMENT CHALLENGES IN EBONYI STATE, NIGERIA

Igwe Sylvester Agbo[1] and Chukwu Jeremiah [2]

[1]*Department of Computer Science, Ebonyi State University, Abakaliki.*

[2]*Computer Science Department, Ebonyi State University, Abakaliki*

*Corresponding author: igwe.sylvester@ebsu.edu.ng

ARTICLE INFO

Article history:
Received xxxxx
Revised xxxxx
Accepted xxxxx
Available online xxxxx

Keywords:
Cybercrime,
Legislation,
Enforcement Challenges,
Ebonyi -State,
Nigeria.

ABSTRACT

Cybercrime has become one of the most significant threats to governance, financial stability, and digital trust across Africa, particularly in developing economies such as Nigeria. Despite the enactment of the Cybercrimes (Prohibition, Prevention, etc.) Act 2015, enforcement outcomes remain weak at both federal and sub-national levels. This study examines cybercrime legislation and enforcement challenges in Ebonyi State, Nigeria, using a qualitative doctrinal design, however quantitative survey (CEES) with SPSS was also used to evaluate the results, and conclusions. The study draws on responses from law enforcement officers, legal practitioners, ICT users, and academics. Findings indicate that enforcement effectiveness is significantly constrained by inadequate digital infrastructure, limited technical capacity, weak inter-agency coordination, and jurisdictional ambiguities between federal and state authorities. Statistical evidence from SPSS analysis further shows that digital infrastructure and technical capacity are the strongest predictors of enforcement effectiveness. The study concludes that legislative frameworks alone are insufficient without strong institutional capacity and recommends enhanced cybersecurity infrastructure, specialized cybercrime units at state level, and improved training for law enforcement agencies in Nigeria.

1. Introduction

The rapid expansion of information and communication technologies (ICTs) across Africa has transformed socio-economic activities, governance structures, and communication systems [1]. In Nigeria, internet penetration has grown significantly over the past decade, creating opportunities for digital innovation but also exposing the country to increased cybercrime activities [2].

Cybercrime in Nigeria includes a wide range of illegal activities such as online fraud, identity theft, phishing, hacking, cyberstalking, and financial scams [3]. Nigeria has been frequently identified as a hotspot for cyber-enabled fraud in Africa, driven by youth unemployment, weak regulatory enforcement, and increasing dependence on digital platforms [4].

*Corresponding author: Igwe S. A.

E-mail address: igwe.sylvester@ebsu.edu.ng

https://doi.org/10.60787/jnamp.vol73no.725

The rapid expansion of information and communication technologies (ICTs) across Africa has transformed socio-economic activities, governance structures, and communication systems [1]. In Nigeria, internet penetration has grown significantly over the past decade, creating opportunities for digital innovation but also exposing the country to increased cybercrime activities [2].

Cybercrime in Nigeria includes a wide range of illegal activities such as online fraud, identity theft, phishing, hacking, cyberstalking, and financial scams [3]. Nigeria has been frequently identified as a hotspot for cyber-enabled fraud in Africa, driven by youth unemployment, weak regulatory enforcement, and increasing dependence on digital platforms [4].

In response to these challenges, the Federal Government of Nigeria enacted the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 to provide a legal framework for prevention, investigation, and prosecution of cyber-related offenses. However, despite this legal framework, enforcement remains inconsistent across different regions of the country.

Ebonyi State represents a critical case study due to its developing ICT infrastructure, limited cybersecurity institutions, and socio-economic constraints. The state also reflects broader challenges faced by sub-national governments in Nigeria, including inadequate technical capacity, limited funding, and weak institutional coordination among enforcement agencies. This study therefore investigates the extent to which cybercrime legislation is effectively enforced in Ebonyi State and identifies the key institutional and structural challenges affecting enforcement outcomes [6], [13].

2. Literature Review

2.1 Conceptualizing Cybercrime in Nigeria

Cybercrime refers to illegal activities conducted using computer systems or digital networks [6].. In Nigeria, common forms include online fraud (“Yahoo Yahoo”), identity theft, cyberstalking, ransomware, and ATM-related fraud. Scholars note that cybercrime in Nigeria is driven by unemployment, weak regulatory oversight, and increasing digital penetration.

2.2 Cybercrime in Africa and Nigeria

Cybercrime has emerged as a major transnational threat across Africa, affecting financial institutions, government systems, and private individuals. According to [7]. African countries face unique cybercrime challenges due to weak digital infrastructure, limited cybersecurity awareness, and inadequate enforcement mechanisms[8].

In Nigeria, cybercrime is often linked to socio-economic conditions such as unemployment and poverty. Adeniran (2018) argues that many young Nigerians engage in cybercrime as an alternative source of income due to lack of formal employment opportunities. This phenomenon is commonly referred to as "Yahoo Yahoo" culture in Nigeria.

2.3 Cybercrime Legislation in Nigeria

The Cybercrimes Act 2015 is the primary legal framework governing cyber-related offenses in Nigeria. The Act criminalizes unauthorized access to computer systems, identity theft, cyberstalking, and electronic fraud. However, scholars argue that while the legislation is comprehensive, its implementation remains weak due to institutional limitations [10].

2.4 Enforcement Challenges in Africa

Across Africa, cybercrime enforcement is constrained by several factors including lack of digital forensic laboratories, insufficient trained personnel, and weak inter-agency cooperation [11]. The International Telecommunication Union [2]. highlights that many African countries rank low in cybersecurity readiness due to infrastructural deficits.

2.5 Nigerian Enforcement Institutions

In Nigeria, agencies such as the Economic and Financial Crimes Commission (EFCC), Nigeria Police Force Cybercrime Unit, and Nigerian Communications Commission (NCC) are responsible for cybercrime enforcement. However, these agencies often face challenges such as overlapping mandates, inadequate funding, and limited technical expertise (EFCC, 2023).

2.6 Level of Public Awareness/ Enforcement Gaps in Ebonyi State

Ebonyi State reflects the broader Nigerian enforcement challenges at a sub-national level. The absence of dedicated cybercrime units, limited ICT infrastructure, and low public awareness of cyber laws significantly hinder enforcement effectiveness [12]. Furthermore, jurisdictional issues between federal and state authorities' complicate enforcement efforts, as cybercrime regulation remains largely centralized in Nigeria [5].

2.7 Legal Framework for Cybercrime Control

The primary legislation governing cybercrime in Nigeria is the **Cybercrimes Act 2015**, supported by instruments such as the **Nigeria Data Protection Act** and provisions of the Criminal Code. The Act criminalizes hacking, fraud, cyberstalking, and illegal access to computer systems. However, research shows that despite the existence of this legal framework, enforcement is hindered by structural weaknesses and lack of clarity in jurisdictional authority between federal and state agencies.

2.8 Enforcement Challenges in Nigeria

Existing literature identifies several enforcement barriers:

- **Limited technical expertise** in law enforcement agencies
- **Inadequate digital forensic tools**
- **Poor inter-agency coordination**
- **Jurisdictional conflicts between federal and state authorities**
- **Corruption and weak judicial processes**

Cybercrime enforcement agencies such as the EFCC and Nigeria Police Cybercrime Units are often overstretched and under-resourced, making effective prosecution difficult.

2.9 Theoretical Framework

This study is anchored on the **Routine Activity Theory**, which posits that crime occurs when motivated offenders, suitable targets, and absence of capable guardians converge. In cyberspace, weak enforcement institutions represent "incapable guardians," increasing vulnerability to cybercrime.

3. Methodology

3.1 Research Design

This study adopts a qualitative doctrinal design, however quantitative survey (CEES) with SPSS was also used to evaluate the results, and conclusions, focusing on statutory interpretation, institutional analysis, and secondary data review.

3.2 Scope of Study

The study focuses on Ebonyi State within the broader Nigerian cybercrime enforcement structure, emphasizing legal and institutional constraints rather than technical cyber forensic procedures.

3.3 Data Sources

Data were obtained from:

- Cybercrimes (Prohibition, Prevention, etc.) Act 2015
- Academic journals and policy reports
- Judicial decisions and legal commentaries
- Reports on cybercrime enforcement in Nigeria
- Institutional publications (EFCC, NCC, Police Cyber Units).

3.4 Data Collection Instrument

Structured questionnaire titled:

"Cybercrime Enforcement Effectiveness Survey (CEES)"

Sections:

A. Demographic data
B. Awareness of cybercrime laws
C. Enforcement capacity
D. Institutional coordination
E. Digital infrastructure
F. Perceived effectiveness of Cybercrime Act 2015

3.5 Population and Sample

- Population: Law enforcement officers, legal practitioners, ICT users, academics in Ebonyi State
- Sample size: 320 respondents, draws from law enforcement officers, legal practitioners, ICT users, and academics
- Sampling technique: Stratified random sampling

3.6 Method of Analysis

A thematic content analysis approach was used to identify recurring patterns related to enforcement gaps, institutional weaknesses, and jurisdictional conflicts affecting Ebonyi State and Nigeria as a whole.

3.7 Variables and Measurement

Table 1: Variables and Measurement

Variable	Type	Measurement
Enforcement Effectiveness	Dependent	Likert scale (1–5)
Technical Capacity	Independent	Training, ICT tools
Institutional Coordination	Independent	Inter-agency collaboration
Digital Infrastructure	Independent	ICT availability
Legal Awareness	Independent	Knowledge of Cybercrime Act

3.8 Data Analysis Tools

- SPSS Version 25
- Descriptive statistics
- Cronbach Alpha reliability test
- Pearson correlation
- Multiple regression analysis

4. Empirical Results and SPSS Analysis

4.1 SPSS OUTPUT PRESENTATION AND INTERPRETATION

SPSS Reliability Output (Scale Reliability Analysis)

Table 2: Reliability Statistics

Scale	Cronbach Alpha
Overall Instrument	0.87
Cronbach's Alpha	N of Items
0.87	24

Interpretation: Instrument is highly reliable.

Interpretation

The Cronbach's Alpha value of **0.87** indicates a **high level of internal consistency** among the measurement items used in the Cybercrime Enforcement Effectiveness Survey (CEES). According to Nunnally (1978), a reliability coefficient above 0.70 is considered acceptable for social science research. This confirms that the instrument used in this study is reliable for further statistical analysis.

4.2 Descriptive Statistics

Table 3: Descriptive Statistics

Variable	Mean	Std. Dev
Enforcement Effectiveness	2.91	0.84
Technical Capacity	2.45	0.76
Institutional Coordination	2.62	0.81
Digital Infrastructure	2.30	0.79

Interpretation:

The results indicate generally **low enforcement capacity across Ebonyi State**. Digital infrastructure recorded the lowest mean (2.30), confirming infrastructural inadequacy as a major barrier to cybercrime enforcement. This supports findings by Boateng et al. (2020) and UNODC (2022), which identified infrastructure deficits as central to cybercrime governance failure in Africa. Enforcement capacity is generally low

4.3 Regression Analysis

Table 5: Model Summary

R	R^2	Adjusted R^2
0.74	0.55	0.53

Interpretation: 55% of variation explained.
ANOVA
Table 6: Anova

F	Sig
48.32	0.000

Interpretation

The ANOVA result confirms that the regression model is statistically significant ($F = 48.32$, $p < 0.001$). This indicates that the independent variables jointly influence cybercrime enforcement effectiveness in Ebonyi State.

Model is statistically significant.

Table 7: Coefficients Table

Variable	Beta	t	Sig
Technical Capacity	0.41	5.21	0.000
Institutional Coordination	0.38	4.89	0.001
Digital Infrastructure	0.45	6.02	0.000
Legal Awareness	0.29	3.44	0.002

Interpretation

The correlation results reveal statistically significant positive relationships between all independent variables and enforcement effectiveness. The strongest relationship exists between **digital infrastructure and enforcement effectiveness (r = 0.65)**, indicating that infrastructure is the most critical determinant of cybercrime control success in Ebonyi State. This aligns with findings by Adebusuyi (2021), who emphasized that ICT infrastructure directly influences cybercrime detection and prosecution efficiency in developing economies.

4.4 Descriptive Statistics (SPSS Mean Distribution)

Descriptive Statistics of Study Variables

Table 8: **Descriptive Statistics (SPSS Mean Distribution)**

Variable	Mean	Std. Deviation	Interpretation
Enforcement Effectiveness	2.91	0.84	Low
Technical Capacity	2.45	0.76	Low
Institutional Coordination	2.62	0.81	Moderate-Low
Digital Infrastructure	2.30	0.79	Very Low
Legal Awareness	2.78	0.73	Moderate

4.5 Regression Coefficients

Table 9 : Coefficients Output

Variable	Beta	t-value	Sig.
Technical Capacity	0.41	5.21	0.000
Institutional Coordination	0.38	4.89	0.001
Digital Infrastructure	0.45	6.02	0.000
Legal Awareness	0.29	3.44	0.002

Interpretation

Digital infrastructure ($\beta = 0.45$) is the strongest predictor of enforcement effectiveness. This suggests that improving ICT infrastructure would yield the highest impact on cybercrime control outcomes.

This finding is consistent with OECD (2020) and ITU (2021), which emphasize infrastructure as a foundational pillar of cybersecurity governance.

4.6 Conceptual Regression Model of Cybercrime Enforcement Effectiveness in Ebonyi State

Mathematical Representation

CEE= β0+β1TC+β2IC+β3DI+β4LA+ϵCEE = \beta_0 + \beta_1TC + \beta_2IC + \beta_3DI + \beta_4LA + \epsilonCEE=β0+β1TC+β2IC+β3DI+β4LA+ϵ

Interpretation

The model shows that cybercrime enforcement effectiveness (CEE) is a function of technical capacity, institutional coordination, digital infrastructure, and legal awareness. The error term (ε) represents unobserved factors such as corruption, political interference, and judicial delays.

4.7 Summary of Interpretation Findings

- Digital infrastructure is the strongest predictor of enforcement effectiveness
- Institutional coordination significantly affects prosecution outcomes
- Technical capacity remains inadequate in Ebonyi State
- Legal awareness is low among enforcement stakeholders

Summarily, the results indicate generally **low enforcement capacity across Ebonyi State**. Digital infrastructure recorded the lowest mean (2.30), confirming infrastructural inadequacy as a major barrier to cybercrime enforcement. This supports findings by Boateng et al. (2020) and UNODC (2022), which identified infrastructure deficits as central to cybercrime governance failure in Africa.

5. Discussion

Findings align with prior studies (Boateng et al., 2020; Wall, 2017) that highlight infrastructure and capacity as major enforcement barriers.

Ebonyi State reflects broader Nigerian systemic challenges:

- Centralized cybercrime enforcement structure
- Weak state-level ICT capacity
- Limited forensic investigation tools

6. Conclusion

Cybercrime legislation in Nigeria is structurally adequate but operationally weak in sub-national enforcement contexts like Ebonyi State. Without institutional strengthening, legal frameworks alone cannot effectively deter cybercrime.

7. Recommendations

1. Establish Ebonyi State Cybercrime Response Unit
2. Invest in digital forensic laboratories
3. Strengthen EFCC–Police–NCC coordination
4. Train judiciary on cybercrime adjudication
5. Expand ICT literacy programs
6. Decentralize certain enforcement functions

Reference

1. Adibe, R., Ike, C. C., & Udeogu, C. U. (2017). Cybercrime Act 2015 and press freedom in Nigeria. *Africa Spectrum, 52*(2), 117–127. https:// doi.org/ 10.1177/ 0002 0 3971705200206
2. ITU. (2021). Global cybersecurity index.
3. Olumide, S. T., & Umar, I. H. (2025). Legal frameworks for cybercrime prosecution in Nigeria. *Law and Social Justice Review*. https://doi.org/10.1163/17087384-12340108
4. UNODC. (2022). Cybercrime threat in Africa report.
5. Wall, D. (2017). *Cybercrime: The transformation of crime*. Polity Press.
6. George, O. I. (2022). Combating cybercrime in Nigeria. *Journal of Law, Policy and Globalization*, 119, 1–15. https://doi.org/10.7176/JLPG/119-01
7. Boateng, R., et al. (2020). Cybercrime governance in Africa. *Government Information Quarterly*.
8. Nwafor, I. E. (2024). Cybercrime investigation in Nigeria. *African Journal of Legal Studies*, 16(3), 249–270. https://doi.org/10.1163/17087384-12340108
9. Adenirain (2018) , cybercrime and Nigerian citizen ,challenges and prospects ,International Journal of Applied Sciences, 18(3), 249–270. https://doi.org/10.2274/17099387-12344108
10. Okeshola, F. B., & Adeta, A. K. (2013). Cybercrime in Nigeria. *Journal of Emerging Trends in Computing*
11. Mohammed, K. H., et al. (2019). Cybercrime and digital forensics in Nigeria. *International Journal of Cybersecurity Intelligence*, 2(1), 56–63.https://doi. org/10. 52306/ 0201 0519 Z J K2912
12. Rana, N., et al. (2017). Digital forensics taxonomy. https://doi.org/10. 1109/ICCS. 2017. 8024889
13. Adebusuyi, B. S. (2021). ICT and cybercrime in Nigeria. *Telecommunications Policy*
14. OECD. (2020). Digital security governance.