International Journal of Intellectual Discourse (IJID)
ISSN: 2636-4832 Volume 9, Issue 2. June, 2026

Effect of telecommunication network regulation and cybercrime legislation on security outcome in north central Nigeria

*Zakaree Saheed[1] and Ismail Momoh Zakari[2]

[1]*Department of Economics, Faculty of Management Sciences, Nigerian Defence Academy Kaduna, Nigeria.*
[2]*Centre for Strategic Research and Studies (CSRS), National Defence College, Abuja – Nigeria.*

*Corresponding Author: szsaheed@nda.edu.ng

Abstract
Telecommunication networks play a significant role in national security through the provision of secure and reliable communication channels that enable government security agencies to coordinate efforts in addressing security challenges. However, these networks also provide avenues through which criminal actors carry out attacks against national interest. Consequently, in the interest of protecting national security and maintaining public order, the government has established regulatory frameworks and cybercrime legislation. This study therefore examines the effect of telecommunication network regulation and cybercrime legislation on security outcomes in North Central Nigeria. The study adopted quantitative research design, utilizing descriptive statistics, Analysis of Variance (ANOVA), and multiple regression techniques for data analysis. Empirical findings revealed that telecommunication network regulation ($\beta = -0.042$, $p > 0.05$) exerted negative statistically insignificant effect on security outcome, while cybercrime legislation ($\beta = 0.034$, $p > 0.05$) shows a positive but statistically insignificant effect on security outcomes in the study area. In contrast, urbanization exhibited a positive and statistically significant effect ($\beta = 0.421$, $p < 0.05$) on security outcomes in the study area. The study concludes that while existing telecommunication regulations and cybercrime legislation have not significantly improved security outcomes, urbanisation remains a critical factor influencing security dynamics in the region. The study therefore recommends that government and relevant stakeholders should strengthen the enforcement capacity of telecommunication regulatory institutions through improved monitoring systems, greater institutional autonomy, and stricter compliance mechanism to enhance national security.

Keywords: Cybercrime Legislation, Network, Security Outcome, Telecommunication Regulation, Urbanisation

1. Introduction

Globally, telecommunication network has served as an important instrument in the society through the dissemination of information. It has made easy interaction, transaction and collaboration among the people. However, as in the case of many technological advancement, there will always be some drawbacks resulting from misuse or abuse of the technology by the consumers of the services, including cybercrimes and threat to national security. Telecommunication network plays a significant role in national security through the provision of secure and reliable communication channels that enable government security agencies to

coordinate their efforts in addressing security challenges. They facilitate the rapid and efficient dissemination of intelligence, as well as timely responses to emerging threats. Telecommunication network also play a critical role in monitoring and detecting threats to national security, as they help security agencies intercept and analyse communications from any hostile actors. By monitoring and analyzing such communications, national security institutions can identify and neutralize threats before they materialize into harm (Bridge Connect, 2024). However, the criminal actors, including terrorists, also rely on telecommunication systems to commit crimes or carry out attacks on national interests.

Communication in whatever form is pivot to the national security, as it is employed in severance of security and also provide opportunities in tackling security challenges. The United Nations on Drugs and Crimes (UNODC) (2017) analyses the means through which telecommunication network, particularly the internet is used for terrorism. For instance, internet has become a highly developed means of communication, reaching an ever growing target worldwide.

Telecommunication network particularly internet provide the means through which many terrorist groups easily disseminate propaganda, which may take the form of multimedia communications providing ideological, explanation or promotion of terrorist activities. In the same vein, according to Catone (2009) as cited in (Dairo, 2017), social media are in forefront in creating hoaxes that can threaten the security of a nation as it afford people to hide under false identity and spread rumors which can disrupt the peace, or propagate a sense of heightened anxiety, fear or panic across the nation, without being traced.

Internet may be an effective medium for the recruitment of minors who are the majority users. It provides the terrorist and other organisations and their sympathisers with a global pool of potential recruits through restricted access cyber forums which offer a venue for recruits, learn and provide support towards the objectives of the organization.

Many illegal organisations and supporters may use internet to finances or raises fund for their illegal activities include terrorism. Terrorist groups for instance, can use internet to raise and collect funds and resources through direct solicitation via websites, chat group, or mass mailing to seek donation, through e-commerce and through charitable organisations. In northern Nigeria, particularly the North West and North Central geopolitical zones, where activities of the banditry groups engaged in kidnapping of the citizens for ransom, mobile networks are mostly used to coordinate attacks and negotiated for ransoms from the families of their victims. Telecommunication networks, particularly internet technology can be used to facilitate the preparation of acts of terrorism, including via communications within and between organisations promoting violent extremism. Evidences have shown that planning an act of terrorism involves remote communication among several parties. For instance, in the Abuja-Kaduna train attacks by the terrorist organisation in the northern Nigeria in March 2022, it was established that there were communications via mobile network between members of the group in the train who passed information about the movement of the train to other members stationed along the railway routes. More so, the latest terrorist attack on the Medium Prison in Kuje Abuja, where many inmates including the 64 Boko Haram members serving various prison terms were set free, was coordinated via mobile network.

The UNODC recognized that preventing and deterring incitement to terrorism and other criminal activities in the interest of

protecting national security and public order is a legitimate ground for restriction in the use of internet or limiting freedom of speech.

In Nigeria, the government has expressed concerned over the use of social media network to perpetuate crimes and support terrorists activities in the country arising from increasing use of social media among the citizens and escalating level of insecurity nationwide (Uchendu et.al. 2025). In an effort to curb the abuse of telecommunication network, particularly, social media, the government attempted to regulate the use of digital platforms including social media platform, through the proposed bill for an Act prohibiting frivolous petitions and Protection from Internet Falsehood and Manipulations Bill 2019. The bills seek to criminalise the use of social media in peddling false or malicious information (Mabika & Ogu, 2021) and other acts deemed likely to be prejudicial to national security.

Furthermore, the government through the Nigerian Communications Commission (NCC), introduced and implemented SIM card registration which is governed by the Registration of Communication Regulations of 2022, and the Registration Rules and Operation processes for implementation of Registration of Communication Subscribers Regulations. The framework is considered important for safeguarding national security and consumer protection (Akindipe, Adepoju & Akinola, 2025). However, the extents to which these measures have effectively reduced security threats remain uncertain, thereby necessitating further investigation to address this policy gap.

Moreover, despite the significance of this subject, particularly in light of the prevailing security challenges in the study area, there is a dearth of empirical literature on the issue. Consequently, this policy gap, coupled with the limited existing literature, motivates the present study to examine the effect of telecommunication network regulations and cybercrime legislation on security outcomes in North Central Nigeria.

To this end, the study is arranged into five sections. Following the introduction, the section two of the study presents the review of some related literature and theoretical framework on the subject matter. The third section captures the methodology. While the analyses and interpretation of the data make up the fourth section. The fifth section summarises the observations and offer some policy recommendations.

2. Literature Review

Theoretical Framework

The study is anchored on Securitization Theory, which posits that security issues are social constructed rather than inherently objective. According to this perspective, an issue becomes a security threat when a relevant actor frames it as an existential danger to a referent object such as the State or Society, through a speech act. This framing legitimizes the adoption of extraordinary measures that transcend the bounds of normal political procedures.

Securitization Theory as propounded by the Copenhagen School, argues that national security is not a natural given condition but a product of deliberate political and institutional processes. Policy makers and security actors play a central role in defining what constitutes a threat and in mobilizing legislative support for exceptional interventions. Thus, security is not merely about objective threats but also how such threats are constructed, communicated, and accepted within a given socio-political context.

Within this framework, certain political or social issues such as abuse of telecommunication networks, can be elevated to the level of security concerns when they are framed as posing significant risks to national security. When security

institutions, endowed with the authority and legitimacy to interpret such phenomena, designate the misuse of telecommunication infrastructure as a threat, it justifies the implementation of stringent regulatory and surveillance measures beyond conventional governance mechanisms.

Furthermore, Securitisation theory maintain that the use of telecommunication networks is not inherent threatening, rather it is the process labeling and interpreting such usage as a security concern that transforms it into a matter of national security. In the context of Nigerian context, for instance, the utilization of telecommunication network by the terrorist groups to plan, coordinate and execute criminal activities constitute a significant threat to the national security, hence this constructed perception of risk necessitates proactive government intervention, including formulation and enforcement of robust telecommunication regulations aimed at controlling and monitoring usage. The theory therefore, provides a valuable analytical lens for understanding how telecommunication regulation and cybercrime legislation in Nigeria is shaped by the securitization of communication technologies, thereby linking regulatory frameworks directly to national security outcome in North Central Nigeria. However, the estimated effects of telecommunication regulation and cybercrime legislation may be biased if differences in security outcomes are attributable to variations in urban development rather than the policy variables themselves. Hence there is need to include urbanisation as a control variable in the model. This is particularly important because urban areas generally possess better telecommunications and digital infrastructure, greater access to internet services and digital technologies, increased exposure to both cyber-related opportunities and threats, and a higher concentration of law enforcement and security agencies. Therefore controlling for urbanization helps to isolate the independent effects of telecommunication regulation and cybercrime legislation on security outcomes.

Empirical Review

Empirically, many studies have also been carried out to verify the relationship between telecommunication and national security, for instance, Frimpong et. Al (2026) adopted systematic review approach guided by the SPIDER framework and PRISMA 2020 guideline to assess the effectiveness of cybercrime law in Africa. The review integrates empirical studies, legal analyses, and policy documents to provide a comprehensive synthesis of cybercrime governance across the continent. The findings revealed a persistent gap between the formal existence of cybercrime laws and their practical enforcement. Specifically, enforcement effectiveness is constrained by institutional, technological, legal, and socio-cultural barriers, including limited technical expertise, inadequate digital forensic capacity, weak inter-agency coordination and low levels of digital literacy. Furthermore, the results indicated that the proliferation of cybercrime legislation has not translated into proportional improvement in enforcement outcomes. However, the study focused solely on the effectiveness of cybercrime law in Africa, and did not examine telecommunication network regulations and their implication for security outcome, which constitute the primary focus of the current study.

Okonko, Okon and Harcourt-White (2024) investigate the statutes that regulates digital media operations in Nigeria and the modalities for their enforcements, using content analysis and survey research design which is on focused group discussion. The findings revealed that there are no laws regulating what people publish

or consume in the digital media space. The study's focus was mainly on the availability of regulations governing the digital media, with no recourse to its effect on national security, whereas the current study is tilted towards the effect of the regulation on security outcome.

Kolawole and Yusuf (2022) examined the effectiveness of Nigeria's cybercrime legislation in curbing cyber offenses, and identified existing gaps that undermine enforcement and the prosecution of cybercrime-related cases. The study adopted a qualitative approach to analyse key legislative frameworks including the cybercrimes Act of 2015 in comparison with international best practices. The findings revealed that although Nigeria has made significant progress in establishing legal mechanisms to address cybercrime, challenges such as weak enforcement, jurisdictional limitation and inadequate technical expertise, and legislative loopholes continue to hinder effective implementation. While the study examined the effectiveness of cybercrime legislation in combating cybercrimes, it did not consider its effect on security outcome, which is the main focus of the current study.

In same vein, Asogwa (2020) examined the impact of internet-based communication channels on national security in Nigeria, using correlation and multiple regression model. The conclusion from the study is that there are specific ways through which impact could impact negatively on national security, especially in recruiting agents of national security challenges, radicalizing and training such agents and spreading incitement that may undermine the national security. However there is need to redirect the focus of research on the influence of telecommunication services in the rural areas on regional security in northern Nigeria.

Mahmood and Jetter, (2019), examine the impact of communication technology on terrorism, hypothesizing that the Communication technology level in a society is systematically related to terrorism. Assessing data gathered from 199 countries for the period of 1970 to 2014, the study shows evidence supporting the predictions that terrorism peaks at intermediate ranges of communication technology and magnitudes.

Uchenna, Chukwuamaka and Chukwuka (2018) assessed the impact of ICT on national security with focus on the Nigeria Security and Civil Defence Corps. The study relied on hypothetic deductive method involving survey design, Chi-Square and discriminant analysis. The results revealed that the NSCDC relied on ICT tools in combating crime, where the information gathered through the use of ICT do help them in actualisation of their technological goal. The results showed that ICT has impact on security and fight against cybercrime. The study though touched on telecommunication, however the focus was on the use of ICT in fighting crime, as against the effect of telecommunication regulation and cybercrime legislation on security outcome which is the focus of the current study.

Dairo (2017) also explores the symbiosis relationship existing between national security and communication in Nigeria, anchoring the study on the systems theory. The study affirmed that communication within a nation can threaten the security of a nation, the same way issues of national security can influence the information that pervades various institutions in the society including the media. Meanwhile, Ukwueze, (2014), appraised the regulation of the telecommunications industry in Nigeria to ascertain the level of protection enjoyed by consumers, using an exploratory approach. The findings revealed that a fairly adequate regulatory framework has been established for the protection of the consumers of telecommunications services in the

country. However, the level of enforcement and consumers' lack of awareness of their rights under the regulation framework have hindered the full realisation of these protections. The study focused on the provision of regulatory framework and its effectiveness in protecting the consumers' right, however, it did not consider its effect on security outcomes, which is the main focus of the current study.

On his part, Olayemi (2014) examined the sociological and technological factors influencing cybercrime and cybersecurity, as well as the threats they pose to Nigeria. The study adopted a qualitative approach using structured interview to collect data, which were subsequently analysed descriptively. The findings revealed that there were no exiting laws in the Nigerian statues that directly address cybercrime at the time of the study. However, the study was conducted before the enactment of the cybercrime (Prohibition, Prevention, etc) Act, 2025, therefore, its findings have limited relevance to the current study, which focuses on the effect of established cybercrime legislation on security outcome.

Based on the reviewed of literature, it is observed that several studies have been conducted on telecommunication networks and national security, including those of Dairo, (2017), Uchenna, Chukwuamaka and Chukwuka (2018) on ICT and National security; and Mahmood and Jetta (2019) on the impact of communication technology on terrorism. However none of these studies examined the effect of telecommunication network regulations on security outcome. Similarly, a few studies have independently examined cybercrime legislation, such as Kolawole and Yusuf, (2022) on the effectiveness of cybercrime legislation and Olayemi, (2014), on the sociological and technological factors influencing cybercrime. Nevertheless, these studies did not investigate the effect of cybercrime legislation on security outcomes. This observation on its own amount to gap in literature, hence necessitate the current study took a critical assessment of the effect of both telecommunication network regulations and cybercrime legislation on security outcome in the North Central Nigeria.

This omission constitutes a significant gap in literature. Consequently, the current study aim to critically assess the effects of both telecommunication network regulations and cybercrime legislation on security outcomes in North Central Nigeria

3. Methodology

3.1 Research Design

This study adopts a quantitative research design, specifically a cross-sectional survey design. The choice of this design is informed by the need to collect data from respondents at a single point in time to examine the relationship between telecommunication regulation, cybercrime legislation, urbanization, and security outcomes. The quantitative approach is appropriate because it allows for objective measurement and statistical analysis of relationships among variables using the Statistical Package for Social Sciences (SPSS). This design is widely used in social science research to establish empirical relationships and test hypotheses.

3.2 Area of the Study

The study focuses on North Central Nigeria, also known as the Middle Belt, a strategically significant and socio-culturally heterogeneous region comprising six states: Plateau, Benue, Nassarawa, Kogi, Niger and Kwara. The region, with an estimated population of over 20 million people, occupies a central geographical position within Nigeria.

Economically, the region is predominantly agrarian and plays a vital role in Nigeria's food production system. It is widely recognnised for cultivation of staple crops

such as yam, rice, cassava, sorghum, maize, and legumes, as well as cash crops like cashew. Beyond agriculture, the region possesses considerable but largely underexploited mineral resources, including tin, columnbite, coal, and iron ore, which if well harnessed, present significant opportunities for industrialization and economic diversification.

Notwithstanding these endowments, the North Central Nigeria has, over the years, become increasingly vulnerable to a complex web of security challenges, including banditry, herder-farmer conflicts, kidnapping, communal violence, and sporadic insurgent activities. These security challenges have weakened both local and regional economic systems. Economically, the implications of insecurity in the North Central are profound, as it imposes significant costs on the regional economy. Empirical estimates suggest that economic losses associated with these crises run into hundreds of billions of naira annually (Baba & Abeysingbe, 2017). These losses not only constrain regional development but also pose a broader threat to national economic and stability.

3.3 Population of the Study

The population of the study consists of individuals residing in North Central Nigeria who are users of telecommunication services and are exposed to digital platforms. This includes civil servants, business owners, students, and other stakeholders who interact with telecommunications infrastructure and may be affected by cybercrime and regulatory frameworks. According to the National Bureau of Statistics, as at the first quarter of 2024, the total active internet subscriber in the region excluding FCT, Abuja, is estimated at 24,948,902.

3.4 Sample Size and Sampling Technique

Based on Taro Yamane approach, the sample size is estimated at 400 respondents selected across the six states that made up the North Central region:

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

where n = required sample size

N = the total population size

e = the acceptable margin of error (0.05)

$$n = 24,948,902 / 1 + 24,948,902(0.05)^2$$

$$n = 24,948,902 / 62,373.255$$

$$n = 399.994$$

The study employs a multi-stage sampling technique, which includes, purposive sampling to select rural areas within North Central Nigeria where telecommunication activities are visible, stratified sampling to ensure representation across different demographic groups (e.g., occupation, age, and gender), and simple random sampling to select respondents within each stratum. This approach ensures that the sample is representative and reduces sampling bias.

3.5 Sources and Method of Data Collection

The study relies primarily on primary data, which were collected directly from respondents through structured questionnaires. The use of primary data is justified because it allows the researcher to obtain first-hand information on perceptions of telecommunication regulation, cybercrime legislation, and security outcomes, which may not be readily available from secondary sources. Data were collected using a structured questionnaire designed in line with the study objectives. The questionnaire was divided into sections covering, demographic characteristics of respondents, telecommunication regulation (TELCR), cybercrime

legislation (CYBL), urbanization (URB), and security outcomes (SECOM).

The questionnaire utilized a five-point Likert scale, ranging from 1 = Strongly Disagree, 2 = Disagree,3=Neutral,4=Agree, 5 = Strongly Agree, This scaling method allows for quantitative measurement of respondents' perceptions.

3.6 Model Specification

The study adopts a multiple regression model to examine the relationship between the dependent and independent variables. The functional relationship is specified as:

SECOM = f(TELCR, CYBL, URB)

1

The econometric form of the model is expressed as:

$SECO = \beta_0+\beta_1 TELCR+\beta_2 CYBL+\beta_3 URB + \varepsilon$

2

Where

SECOM = Regional Security

TELCR = Telecommunication Regulation

CYBL = Cybercrime Legislation

URB = Urbainsation

β_0 = Intercept (constant term)

$\beta_1 – \beta_3$ = Parameters to be estimated

ε = Error term

3.7 Measurement of Variables

The variables used in this study are measured as follows:

1. Security Outcome (SECOM): Measured using respondents' perceptions of safety, crime reduction, and effectiveness of security systems.
2. Telecommunication Regulation (TELCR): Measured through respondents' assessment of regulatory effectiveness, compliance, and monitoring of telecom operators.
3. Cybercrime Legislation (CYBL): Measured based on awareness, enforcement, and effectiveness of cybercrime laws.
4. Urbanization (URB): Measured using indicators such as infrastructure development, population concentration, and access to services.

All variables are measured using Likert-scale responses, making them suitable for quantitative analysis.

3.8 Method of Data Analysis

The data collected were analyzed using the Statistical Package for Social Sciences (SPSS). The study employed statistical tools include Descriptive statistics (mean, minimum, maximum standard deviation) to summarize the data; Multiple regression analysis to examine the effect of independent variables on security outcomes; ANOVA (Analysis of Variance) to test the overall significance of the model; and t-test statistics to evaluate the significance of individual coefficients

4. Results and Discussion

4.1 Descriptive Statistics

The descriptive statistics table summarizes the basic characteristics of the variables used in the study: Security Outcome (SECOM), Telecommunication Regulation (TLCR), Cybercrime Legislation (CYBL), and Urbanization (URB).

All variables have 400 observations, indicating a complete dataset with no missing values (Valid N = 400). The summary of the descriptive statistics of the data collected is presented in table 1 as follows;

Table 1
Descriptive Statistics

Variable	N	Minimum	Maximum	Mean	Std. Deviation
SECOM	400	1	5	3.75	1.348
TLCR	400	1	5	2.93	1.335
CYBL	400	1	5	3.37	1.283
URB	400	1	5	3.87	1.185
Valid N (listwise)	400				

Source: Researcher's SPSS Multiple Regression Analysis Output, 2026

The descriptive statistics in Table 1 provides an overview of the distributional characteristics of the study variables, namely Security Outcome (SECOM), Telecommunication Regulation (TLCR), Cybercrime legislation (CYBL) and Urbanisation (URB). The analysis focuses on the minimum and maximum values, mean scores, and standard deviations of the variables based on 400 valid responses.

The result indicates that all variables recorded minimum and maximum values ranging from 1 to 5, suggesting that the study adopted a five-point Likert scale in measuring respondents perceptions of the subject matter. The uniformity in the response range implies consistency in the measurement scale and allows for comparative interpretation among the variables.

The result show a mean value of 3.75 and standard deviation of 1.348 suggesting that respondent generally agreed that security outcome relatively significant within the context of the study. The relatively high mean score indicates positive perceptions towards security outcome within the region. However, the standard deviation shows a moderate level of dispersion in responses, implying that although many respondents shared similar views, some variations in opinion still existed among participants.

The results from the table also show that Telecommunication Regulation (TLCR) recorded a mean value of 2.93, which is below the midpoint of 3 imply that respondents were either uncertain or moderately disagreed regarding the effectiveness telecommunication regulation. This finding may be an indication of inadequacies in regulatory frameworks, weak enforcement mechanism or limited public confidence in the regulatory policies. The moderate standard deviation further indicates that respondents' opinions varied considerably across the sample population.

Furthermore, Cybercrime Legislation (CYBL) shows a mean value of 3.37 and standard deviation of 1,283. This implies that there is a fair awareness and understanding of cybercrime legislation among respondents, with a moderate perception of its effectiveness. Respondents appear to believe cybercrime laws exist but may not be strongly enforced or fully effective. The standard deviation indicates moderate variability in responses, implying that knowledge and awareness of cybercrime legislation and its effectiveness in improving security outcome may differ across respondents.

The results indicate that Urbanization (URB) shows a mean value of 3.87. This indicates that respondents strongly perceived urbanization as significant within the study context. The relatively lower standard deviation (1.185) compared to other variables implies that respondents opinions were more closely clustered around the mean, reflecting greater consensus among respondents.

Generally, the descriptive statistics show that URB and SECOM are the most rated variables in the study, indicating stronger respondent agreement regarding their relevance or effectiveness in the subject matter. In contrast, TLCR recorded the lowest mean score, suggesting concerns about the effectiveness of telecommunication regulation framework. The moderate standard deviation value across all variables indicates that responses were reasonably distributed without extreme variability, thereby enhancing the reliability of the dataset for further inferential statistical analysis.

4.2 Regression Results

Table 2

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.382[a]	.146	.139	1.251

a. Predictors: (Constant), URB, TLCR, CYBL

Source: Researcher's SPSS Multiple Regression Analysis Output, 2026

Table 2 presents the model summary of the multiple regression analysis conducted in this study. The results reveal a coefficient of correlation (R) of 0.382, indicating a moderate positive relationship between the predictors (TLCR, CYBL, URB) and security outcomes. The coefficient of determination (R^2) is 0.146, shows that 14.6% of the variation in security outcomes is explained by telecommunication regulation, cybercrime legislation, and urbanization. Furthermore, the adjusted R^2 (0.139) adjusts for sample size and number of predictors, confirming that about 13.9% of the variation is reliably explained. The standard error (1.251) indicates the average deviation of observed values from the regression line.

Table 3

ANOVA

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	105.646	3	35.215	22.516	.000[b]
Residual	619.354	396	1.564		
Total	725.000	399			

Note: a. Dependent Variable: SECOM

b. Predictors: (Constant), URB, TLCR, CYBL

Source: Researcher's SPSS Multiple Regression Analysis Output, 2026

Table 3 presents the analysis of variance (ANOVA) results for the multiple regression model, assessing the joint statistical significance of the independent variables in explaining variations in security outcome in north central Nigeria. The computed F-statistic of 22.516 serves as a test of the overall model fit, specifically whether the regression model accounts for a significant proportion of the variance in the dependent variable. The associated p-value (0.000) is below the conventional significance threshold of 0.05, indicating that the regression model is valid and suitable for explaining the relationship between telecommunication regulation, cybercrime legislation, urbanization, and security outcomes.

Table 4
Regression Coefficients Table

Variable	(β)	Std. Error	Beta	t	Sig. (p-value)	Tolerance	VIF
(Constant)	2.126	.289		7.358	.000		
TLCR	-.042	.047	-.042	-.887	.375	.984	1.016
CYBL	.034	.050	.033	.693	.489	.966	1.035
URB	.421	.054	.370	7.845	.000	.968	1.033

Note: a. Dependent Variable: SECOM
Source: Researcher's SPSS Multiple Regression Analysis Output, 2026

The regression result in Table 4 shows the effect of Telecommunication Regulation (TLCR), Cybercrime Legislation (CYBL), and Urbanization (URB) on Security Outcome (SECOM), which serves as the dependent variable. The estimated regression model is expressed thus:

SECOM = 2.126 – 0.042TELCR+ 0.034CYBL+0.421URB

The constant (intercept) value of 2.126 is positive and statistically significant at $p < 0.05$. It implies that when all the independent variables (TLCR, CYBL, and URB) are held constant at zero, security outcome (SECOM) would still record a baseline value of 2.126. The result indicates that the model possesses predictive relevance.

Furthermore, the table shows that the regression coefficient of telecommunication regulation (TLCR) is negative and statistically insignificant at 5% level ($\beta = -0.042$, $p = 0.375$), indicating an inverse relationship between telecommunication regulation and security outcome. This implies that a unit increase in telecommunication regulation is associated with 0.042 decreases in regional security outcome holding other factors constant. The standardized beta coefficient (-0.042) further indicates that TLCR contributes very little to the variation in SECOM.

The coefficient of cybercrime legislation ($\beta = 0.034$, $p = 0.489$) is positive but statistically insignificant at the 5% level. The positive coefficient indicates that better cybercrime laws may improve regional security. Specifically, a unit increase in CYBL would lead to a 0.034 improvement in SECOM. However, the effect is statistically insignificant (p-value of 0.489 exceeds the 0.05 threshold). The t-value (0.693) also indicates weak explanatory power to impact security outcomes.

Urbanization showed a positive significant effect on regional security, with coefficient value ($\beta = 0.421$, $p = 0.000$). This implies that a unit increase in urbanization leads to a 0.421 increase in regional security. The positive significant effect could be due to better infrastructure, improved surveillance systems, stronger institutional presence, and increased access to security services. The standardized beta coefficient (0.370) further reveals that URB is the strongest predictor among all the independent variables in the model.

The findings imply that while urbanization significantly enhances security outcomes and economic prospects, weak telecommunication regulation and ineffective cybercrime legislation constrain the full realization of digital economy benefits in North Central Nigeria. The multicollinearity statistics indicates no multicollinearity problem among the

variables as shown by the Tolerance value being 0.968, which is less than 1, and since all VIF values are approximately 1, the predictors are independent of one another and do not distort the regression estimates. Therefore, the regression model is statistically reliable and suitable interpretation

Discussion of Findings

The regression results reveal that Urbanisation is the only variable with a statistically significant effect on Security Outcome (SECOM) in the North Central Nigeria. this implies that technological infrastructure and urban digital development are critical determinants of effective security output in the study area.

The result of the effect of Telecommunication regulation on security outcome shows a p-value of 0.375 is greater than the 0.05 significance level, while the t-value (-0.887) is relatively weak. This suggests that TLCR does not significantly influence SECOM within the context of the study. This result indicates that telecommunication regulation, as currently implemented, does not significantly influence security outcomes in North Central Nigeria. This may imply that existing telecommunication network regulatory mechanism may not be sufficiently effective in improving security outcome in the North Central Nigeria. This may be attributed to weak implementation, inadequate monitoring framework or poor coordination among the regulatory institutions and security agencies. It further suggest that Telecommunication regulatory policies alone may not automatically translate to improved security outcome except accompanied by effective implementation, institutional capacity, monitoring mechanisms, and stakeholder collaboration

Furthermore, the findings of insignificant relationship between Cybercrime legislation and Security Outcome (SECOM) may indicate that the cybercrime legislation framework in the study area may not yet be effectively integrated into national security policy yet. The insignificant relationship may also suggest challenges such as weak enforcement of cybercrime laws, and rising sophistication of cyber threat. The standard beta value of just 0.033 equally shows that CYBL contributes just little to explaining variations in security outcome in North Central Nigeria.

The result further reveals that URB is the strongest predictor among all the independent variables in the model. This may be attributed to the fact that urban areas generally possess better telecommunications facilities, surveillance technologies, internet penetration, and emergency response systems, which collectively improve intelligence gathering, information dissemination, and security coordination. The result aligns with modernization and technological diffusion theories, which argue that advanced infrastructure and digital integration improve institutional efficiency and security performance.

Overall, the findings suggest that while Telecommunication network regulations policies and cybercrime legislation are important, their effectiveness largely depends on the availability of robust infrastructure and strong institutions.

5. Conclusion and Policy Recommendations

The empirical evidence indicates that telecommunication regulation and cybercrime legislation, although theoretically important for enhancing regional security, do not exert statistically significant effects in the context of North Central Nigeria. This suggests a disconnect between policy design and practical effectiveness, likely driven by weak enforcement mechanisms, institutional inefficiencies, and limited technological capacity.

The regression model explains only 14.6 per cent of the variation in security outcome, indicating that although these factors contribute to a broader security framework, they are not the dominant determinants of security outcomes in the region. Consequently, a substantial proportion of the variation in security outcome is attributed to other factors not captured in the model. The study therefore conclude that effective telecommunication network regulations and cybercrime legislation are essential components of a broader security framework but must be complemented by other institutional, technological, and socio-economic measures to achieve significant improvements in security outcomes.

In light of these findings, several policy actions are imperative:

First, there is a need to strengthen the enforcement capacity of telecommunication regulatory institutions through improved monitoring systems, institutional autonomy, and stricter compliance mechanisms. Regulatory frameworks should be updated to reflect evolving digital threats, while ensuring that enforcement is consistent and technology-driven.

Second, cybercrime legislation must be complemented with robust enforcement infrastructure. This includes investment in digital forensic capabilities, specialized training for law enforcement agencies, and the establishment of dedicated cybercrime units and judicial processes. Enhancing public awareness and digital literacy is equally important in reducing exposure to cyber threats and improving compliance with legal provisions.

Third, given the significant role of urbanization, policymakers should prioritize planned and inclusive urban development. Investments in smart infrastructure, surveillance systems, and integrated urban security planning can further enhance security outcomes. At the same time, efforts should be made to manage the challenges associated with rapid urbanization, such as congestion, inequality, and urban crime.

Greater attention should be given to rural digital inclusion to reduce communication gaps that may weaken national security operations

Lastly, a comprehensive and integrated security strategy should be adopted that combines effective telecommunications regulation, robust cybercrime legislation, technological innovation, institutional capacity building, stakeholder collaboration, and socio-economic development initiatives. Such a multifaceted approach is more likely to produce sustainable improvements in security outcomes in North Central Nigeria than reliance on regulatory and legislative measures alone.

Acknowledgement:
This research received financial support from the TETFUND Institution-based Research Intervention (2025)

References

Akindipe, O., Adepoju, A. & Akinola, O. (2025). SIM Registration In Nigeria: What Telecom Operators Must Know. Mondaq Intellegence, available at: https://www.mondaq.com/nigeria/telecoms-mobile-cable-communications/1698902/sim-registration-in-nigeria-what-telecom-operators-must-know

Asogwa, C. E. (2020). Internet-Based Communications: A Threat or Strength to National Security? *Sage Open Access Journal,*

https://journals.sagepub.com/doi/10.1177/215824402091458

Baba, I. and Abeysinghe, C. (2017). Farmers-Herdsmen Conflict in the North Central Region of Nigeria (An Analysis of Cause and Effect). *International Journal of Social Science and Humanities Research*, 5 (3), 53-62. Available at: www.researchpublish.com

Bridge Connect (2024). What Is The Role Of Telecom In National Security. Available at: https://www.bridge-connect.com/post/what-is-the-role-of-telecom-in-national-security

Dairo, M. (2017). The Connection between National security and Communication, *Specialty Journal of Knowledge Management, 2(4), 1-11*

Frimpong, S., C.C. Udechukwu, M.I. Adeoba, T.K. Mensah, D. Mensah (2026). Assessing the Effectiveness of Cybercrime Laws in Africa: A Systematic Review of Enforcement Barriers and Policy Reform Options. Current Research in Interdisciplinary Studies, 5(4):1–12, 2026. https://doi.org/10.58614/cris54

Kolawole, A. and Yusuf, M. (2022). Cybercrime Legislation in Nigeria: Effectiveness and Gaps. https://www.researchgate.net/publication/388634111_Cybercrime_Legislation_in_Nigeria_Effectiveness_and_Gaps

Mabika, V. and Ogu, E.C. (2021). Internet Impact Brief Nigeria's Protection from Internet Falsehood and Manipulation Bill 2019. *internetsociety.org CC BY-NC-SA*

Mahmood, R. & Jetter, M. (2019). Communications Technology and Terrorism. *Journal of Conflict resolution*, 64(1), 127-166.

Okonko, B.B., Okon, G.B., and Harcourt-White, D. (2024). Digital Media Regulations in Nigeria: Discourses on Statutes and Enforcements. *International Journal of Sub-Saharan African Research (IJSSAR)* 2(4), 376-387.

Olayemi, O.J. (2014). A socio-technological analysis of cybercrime and cyber security in Nigeria *International Journal of Sociology and Anthropology 6(3), pp. 116-125,*

Uchenna,C.P., Chukwuamaka, O. and Chukwuka, O. (2018)The Impact of ICT on National Security: A Case of Nigeria Security and Civil Defence Corps. *International and Public Affairs* 2 (3)

Uchendu, C. E., Omolara Oluwabusayo Akin-Odukoya, Funmi Falobi, Perpetua Ogechi

Aondover, & Louis Benard. (2025). Social Media Regulations and Government Censorship in Nigeria. *Scientific Journal of Politics*, *5*(1), 16-30. https://doi.org/10.33258/polit.v5i1.1241

Ukwueze, F.O.(2014).Consumer Protection In the Regulation of Telecommunications Services in Nigeria: Not Yet "Uhuru" for Consumers. *The Nigerian Juridical Review Vol. 12 [2014], 125 – 150*

UNODC (2017). The Drug Problem and Organized Crime, Illicit Financial Flows, Corruption and Terrorism. https://www.unodc.org/wdr2017/field/Booklet_5_NEXUS.