World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(Review Article)

Rethinking protection models for rural telecommunications infrastructure in Nigeria: The role of institutional coordination and security-by-design

EFFIOM Enebong Ewa [1, *], EZE Benito Emeka [1], KESHINRO Sunday Adedotun [2], ADEBAYO Gbenga [3], ZAMANI Andrew Prof [4] and ONIBIYO Ezekiel Rotimi [1]

[1] *Directorate of Critical National Assets and Infrastructure Protection, Office of the National Security Adviser.*
[2] *Nigeria Security and Civil Defence Corps Headquarters Abuja.*
[3] *Association of Licensed Telecommunication Operators in Nigeria.*
[4] *APUDI Institute for Peace Studies and Social Rehabilitation, Abuja.*

World Journal of Advanced Research and Reviews, 2026, 29(03), 034–043

Publication history: Received on 09 January 2026; revised on 25 February 2026; accepted on 28 February 2026

Article DOI: https://doi.org/10.30574/wjarr.2026.29.3.0399

Abstract

The Federal Government decision to roll out 4000-tower to cater for unserved and underserved communities calls for attention. The long-term sustainability of rural telecommunications infrastructure in Nigeria remains a critical development challenge, with past initiatives plagued by recurrent vandalism, service disruptions, and premature abandonment despite significant public investment. This study interrogates this failure by exploring how protection models, shaped by institutional coordination and security-by-design principles, determine infrastructure resilience in underserved and high-risk environments. Through a qualitative review of policy documents, academic literature, and case studies, the research addresses two objectives: evaluating the role of institutional coordination in preventing infrastructure failure and investigating how a security-by-design framework enhances long-term sustainability. The findings reveal that fragmented governance, characterised by weak collaboration among regulators, deploying agencies, statutory security bodies and siloed responses, and disconnects with local stakeholders creates accountability gaps and delayed responses that expose assets to vandalism, insiders sabotage, and theft. Conversely, the study demonstrates that infrastructure where security is embedded at the design stage, through enforceable standards for physical protection, surveillance, and community engagement, exhibits significantly greater operational resilience and service continuity. The study concludes that sustainable rural connectivity is fundamentally an institutional and design imperative, not merely a technical or financial challenge. It recommends the formalisation of a mandatory inter-agency coordination framework led by the Ministry of Communications, NCC, and the Nigeria Security and Civil Defence Corps, and the institutionalisation of security-by-design as a non-negotiable requirement in all rural telecommunications projects, including the proposed national 4,000-tower rollout. Implementing these measures is essential to transform rural telecom infrastructure from fragile public liabilities into resilient pillars of digital inclusion and national development.

Keywords: Institutional Coordination; Institutional Theory; Rural Telecommunications Infrastructure; Security-By-Design

1. Introduction

Globally, the expansion of telecommunications infrastructure is widely recognised as a foundational driver of economic growth, social inclusion, governance efficiency, and national security in the digital age. International development frameworks increasingly position digital connectivity alongside transport and energy as a critical enabler of sustainable development, particularly for achieving inclusive growth and reducing structural inequalities between urban and rural

[*] Corresponding author: EFFIOM Enebong Ewa

Copyright © 2026 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution License 4.0.

populations (World Bank, 2020; ITU, 2021). However, while significant progress has been made in extending network coverage worldwide, wanton vandalism the long-term sustainability of telecommunications infrastructure in high-risk and remote environments remains a persistent challenge (Javadpour et al., 2024).

In developing and emerging economies, telecommunications projects frequently operate within contexts characterised by weak institutions, security deficits, limited community ownership, absence of minimum security standard, and fragile operating environments (Effiom, 2025). These conditions expose critical digital infrastructure to vandalism, theft, and operational disruptions that shorten asset lifecycles and undermine service continuity (OECD, 2019; GSMA, 2019). As a result, many rural connectivity initiatives in the Global South have struggled to transition from initial deployment to durable, self-sustaining infrastructure, despite substantial public and donor investments.

Over the past two decades, Nigeria has pursued multiple policy and investment initiatives aimed at extending telecommunications access to rural and underserved communities as part of broader national development and digital inclusion objectives. Nigeria exemplifies this paradox. Over the past two decades, the country has pursued multiple rural telephony and universal access initiatives aimed at bridging the urban–rural digital divide and promoting inclusive national development (Tognisse & Degila, 2023). Yet, many of these interventions including projects implemented under the Rural Telephony Project (RTP) and Universal Service Provision Fund (USPF), have experienced recurrent vandalism, service outages, escalating maintenance costs, and premature abandonment (National Communications Commission (NCC), 2018; World Bank, 2020). These outcomes highlight a critical gap between infrastructure rollout and infrastructure survival, raising fundamental questions about how security, governance, and protection models shape the sustainability of rural telecommunications infrastructure in Nigeria (Adejumoh, 2025).

A growing body of infrastructure and telecommunications literature suggests that sustainability failures in rural connectivity projects are rarely attributable to technology limitations alone, but rather to governance, security, and operational deficiencies embedded in project design and implementation (Estache, 2014; Andres et al., 2013). In Nigeria, rural telecommunications infrastructure has been deployed in environments characterised by high levels of vandalism, theft of power equipment, insecurity, and weak institutional coordination among regulators, operators, and security agencies (Oyebode, 2022; GSMA, 2019). These risks have often been treated as post-deployment challenges, resulting in reactive and fragmented security responses. Consequently, projects that were technically viable at inception have experienced shortened asset lifecycles, undermining service continuity and eroding public trust in government-led digital inclusion initiatives.

Empirical studies from Nigeria and comparable emerging economies highlight vandalism, theft, unregulated labour economy, insiders threat, and community disengagement as central determinants of infrastructure failure in rural settings (Mugari & Obioha, 2024; Adeleke & Aminu, 2021). Telecommunications towers, power systems, Lithium Ion Batteries, and transmission equipment are frequently targeted due to their remote locations, limited surveillance, and weak local ownership structures (Adebayo, 2025). Where communities perceive infrastructure as externally imposed state assets rather than shared developmental resources, vandalism and sabotage become more prevalent, particularly in contexts of socio-economic exclusion and limited service reliability (OECD, 2019). The absence of structured community participation mechanisms in earlier Nigerian rural telephony projects therefore contributed to asset vulnerability, accelerated degradation, and eventual service collapse.

At the core of these challenges lies the limited integration of security-by-design principles in rural telecommunications planning. Security-by-design emphasises the early incorporation of physical protection, surveillance, response protocols, governance arrangements, and stakeholder coordination into infrastructure design rather than treating security as an auxiliary or post-deployment function (World Bank, 2020). International evidence demonstrates that infrastructure projects that integrate minimum security standards at the planning stage exhibit greater resilience, longer operational lifespans, and lower lifecycle costs, particularly in high-risk environments (OECD, 2019; ITU, 2021). In Nigeria, however, rural telecom deployments have often lacked enforceable minimum security benchmarks, leaving protection measures to ad hoc arrangements determined by operators' discretion or short-term cost considerations.

Nigeria's telecommunication ecosystem is a significant productivity barometer such that threats to connectivity strikes at the heart of the national economy. The telecommunications sector contributes 16–18% of Nigeria's GDP (NBS, 2024). These figures highlight the urgent need for coordinated protection measures along major highways (Eze, 2025). The efforts of government to emplace adequate security in the Nigeria telecom ecosystem is seen in the presence of NCC as regulatory agency, NSCDC as lead agency for protection of CNAI, and the Directorate of Critical National Assets and Infrastructure Protection in the Office of the National Security Adviser (ONSA-DCNAIP), which has evolved a State architecture Intervention level across the federation (Effiom, 2025).

The role of statutory security agencies is also critical. Studies on critical national infrastructure protection emphasise that early involvement of security institutions in planning and deployment phases enhances threat assessment, response coordination, and deterrence (OECD, 2019). In Nigeria, late-stage or reactive security engagement has undermined infrastructure protection, as agencies are often called upon only after assets have been vandalised or services disrupted. This reactive posture weakens national digital inclusion objectives by allowing preventable failures to persist. Integrating statutory security agencies, regulators, operators, and communities into a coordinated, multilayered security architecture is therefore essential for sustainable rural telecommunications infrastructure (Okojokwu-Idu et al., 2023).

Against this backdrop, Nigeria's 4,000-tower project presents a unique policy laboratory for rethinking protection models and institutionalising minimum security standards within the telecommunications sector. By embedding security-by-design principles, clarifying governance roles, integrating community ownership mechanisms, and aligning public and private incentives, the project can address the systemic weaknesses that undermined previous rural telephony initiatives. This study is therefore situated at the intersection of infrastructure governance, security studies, and digital development, seeking to generate empirical and policy-relevant insights that can reposition rural telecommunications infrastructure as a resilient foundation for inclusive national development.

Research Questions

This study provides answers to the following questions

- What role do institutional coordination play in preventing the failure of rural telecommunications infrastructure in Nigeria?
- How can a security-by-design framework improve the long-term sustainability of rural telecommunications infrastructure in Nigeria?

Objective of the Study

- The main objective of the study explored protection models for rural telecommunications infrastructure through role of institutional coordination and security-by-design in Nigeria. While specific objectives;
- Evaluate the role institutional coordination play in preventing the failure of rural telecommunications infrastructure in Nigeria
- Investigate how security-by-design framework improve the long-term sustainability of rural telecommunications infrastructure in Nigeria

1.1. Significance of the Study

The study will significantly benefit federal and state government institutions responsible for digital infrastructure development, the Ministry of Communications and Digital Economy, National Communications Commission (NCC), Universal Service Provision Fund (USPF), and the Office of the National Security Adviser (ONSA), Mobile Network Operators (MNOs), tower companies, InfraCos, and licensed Private Security Companies (PSCs), Infrastructure Concession Regulatory Commission (ICRC) and the Nigeria Security and Civil Defence Corps (NSCDC)This study findings will guide the development of enforceable protection protocols, risk-based deployment strategies, and security-by-design doctrines tailored to rural telecommunications assets, will significantly benefiits By interrogating *security-by-design* as an organizing framework, this study contributes theoretically, empirically, and policy-wise to debates on infrastructure resilience in fragile environments.

The evaluation of institutional coordination addresses a major blind spot in existing telecommunications and infrastructure protection literature in Nigeria. While multiple institutions, security agencies, sector regulators, ministries, private operators, and host communities, are involved in the protection of telecom infrastructure, coordination among these actors is often weak, fragmented, or informal. Studies on critical infrastructure protection highlight that institutional silos significantly increase vulnerability and failure risks, particularly in environments characterised by insecurity and weak state capacity (Boin & McConnell, 2007; Dunn-Cavelty & Suter, 2009).

This study is significant in empirically demonstrating how coordination failures, such as poor information sharing, unclear mandates, and overlapping responsibilities, contribute to the collapse of rural telecommunications infrastructure. By doing so, it provides a strong analytical basis for advocating whole-of-government and whole-of-society approaches to infrastructure protection. The findings will be valuable to security agencies, regulators, and policymakers seeking to design institutional frameworks that reduce duplication, close protection gaps, and improve accountability in rural infrastructure governance.

1.2. Statement of the Problem

Despite sustained public investment and policy commitments to expand telecommunications access in unserved and underserved rural communities in Nigeria, the long-term sustainability of rural telecommunications infrastructure remains deeply problematic. Numerous base stations and related facilities deployed under past rural telephony and universal access initiatives have suffered recurrent vandalism, theft, service disruptions, and premature abandonment. These failures persist even as government continues to frame connectivity expansion primarily as an infrastructure delivery challenge, with limited attention to how security risks, operational vulnerabilities, and protection models shape infrastructure survival in high-risk environments.

Institutional fragmentation further exacerbates the vulnerability of rural telecommunications infrastructure. Multiple actors, including sector regulators, security agencies, private operators, host communities, and different tiers of government, exercise overlapping or poorly defined responsibilities for infrastructure protection. Weak coordination, limited information sharing, and unclear leadership roles result in security gaps that are routinely exploited by criminal actors. Yet, the role of institutional coordination in preventing infrastructure failure has received insufficient empirical scrutiny within Nigeria’s telecommunications governance literature.

Beyond these structural weaknesses is a broader conceptual problem: security considerations are rarely integrated at the design and planning stages of rural telecommunications projects. Protection is commonly treated as an operational afterthought, introduced only after assets have been vandalised or service disruptions occur. This reactive approach contradicts emerging international best practices that emphasise security-by-design as a core principle of infrastructure sustainability. The applicability and potential benefits of such a framework for Nigeria’s rural telecommunications context, however, remain largely unexplored.

Consequently, there exists a significant knowledge and policy gap regarding how protection models, security standards, institutional coordination, and design-stage security integration interact to shape the sustainability of rural telecommunications infrastructure in Nigeria. Without empirical evidence addressing these interrelated issues, current and future investments risk repeating the failures of past interventions. This study therefore seeks to systematically interrogate security-by-design and rethink protection models as essential determinants of sustainable rural telecommunications infrastructure in underserved Nigerian communities.

2. Literature Review

2.1. Conceptual Framework

The framework assumes that weak coordination and reactive security practices increase infrastructure vulnerability, whereas strong institutional alignment and security-by-design enhance infrastructure survival in high-risk rural environments (OECD, 2019; World Bank, 2020).

2.2. Rural Telecommunications Infrastructure

Rural telecommunications infrastructure refers to network assets deployed to extend connectivity to underserved and unserved communities, including base transceiver stations, towers, power systems, transmission equipment, and associated support facilities. In developing contexts, such infrastructure is typically exposed to heightened risks arising from remoteness, weak state presence, limited policing, and fragile community–state relations (Aker & Mbiti, 2010; GSMA, 2019).

The literature emphasises that rural telecom infrastructure failures are rarely caused by technical deficiencies alone. Instead, they are often the outcome of institutional weaknesses, inadequate protection models, and failure to integrate security considerations throughout the infrastructure lifecycle, from design and siting to operation and maintenance (World Bank, 2020). In Nigeria, repeated vandalism of towers, theft of batteries and diesel, and prolonged service disruptions illustrate how infrastructure sustainability is fundamentally linked to governance and security arrangements rather than engineering capacity alone.

Within the conceptual framework, rural telecommunications infrastructure represents the outcome space in which the effects of institutional coordination and security-by-design become observable. Infrastructure sustainability is thus treated as a function of how effectively institutions collaborate and how deliberately security is embedded at the design stage.

2.3. Institutional Coordination

Institutional coordination is conceptualised as the extent to which relevant public and private actors align roles, share information, harmonise standards, and jointly plan interventions across the telecommunications infrastructure lifecycle. Key institutions include sector regulators, line ministries, security agencies, infrastructure operators, sub-national governments, and host communities. The Federal Ministry of Communication and Digital Economy, the National Communication Commission (NCC), the Nigeria Security and Civil Defence Corps, Association of Licensed Telecommunication Operators (ALTON) and Association of Communication Operators of Nigeria (ATCON).

Institutional theory suggests that fragmented authority, overlapping mandates, and weak coordination mechanisms undermine policy implementation and infrastructure outcomes, particularly in complex sectors such as telecommunications (Scott, 2014). Empirical studies show that poor coordination between regulators, operators, and security institutions leads to gaps in threat intelligence, unclear accountability for asset protection, and delayed response to security incidents (OECD, 2019). In Nigeria, institutional silos between telecommunications regulators, infrastructure owners, and statutory security agencies have resulted in reactive security deployment, limited data sharing, and inconsistent protection practices across rural sites.

Within the conceptual framework, institutional coordination is expected to influence infrastructure sustainability both directly and indirectly. Directly, effective coordination enhances joint planning, standard setting, and enforcement capacity. Indirectly, institutional coordination enables the operationalisation of security-by-design by ensuring that security agencies, regulators, and operators are involved early in project conception rather than after deployment.

2.4. Security-by-Design

Security-by-design is conceptualised as the deliberate integration of security considerations into the earliest stages of infrastructure planning, design, procurement, and deployment, rather than treating security as an add-on or reactive function. Drawing from infrastructure resilience and critical infrastructure protection literature, security-by-design encompasses physical security standards, surveillance systems, access controls, redundancy measures, response protocols, and community engagement mechanisms embedded at the design phase (OECD, 2019; World Bank, 2020). The literature consistently demonstrates that infrastructure protected through reactive or post-deployment security measures experiences higher lifecycle costs, frequent downtime, and accelerated asset degradation (Flynn, 2015). Conversely, security-by-design reduces vulnerability exposure, improves response effectiveness, and strengthens operational resilience, particularly in high-risk rural and conflict-prone environments (UNODC, 2018).

In the conceptual framework, security-by-design functions as a mediating and reinforcing construct between institutional coordination and infrastructure sustainability. Effective institutional coordination makes it possible to define minimum security standards, allocate responsibilities, and enforce compliance, while security-by-design translates these institutional arrangements into tangible protection mechanisms at the asset level. These security deficits translate directly into financial losses, service disruptions, and reputational risks for public infrastructure projects. Vandalism and theft increase operational expenditure, trigger repeated downtime, and undermine revenue stability for operators, while government bears reputational costs associated with failed public investments (GSMA, 2019). From a policy perspective, repeated infrastructure failure weakens investor confidence, discourages private sector participation, and constrains the scalability of future digital inclusion programmes. This dynamic is particularly salient for Nigeria’s proposed 4,000-tower project, which represents both a major fiscal commitment and a strategic opportunity to redefine infrastructure governance norms in rural connectivity.

Taken together, the conceptual framework posits that institutional coordination enables security-by-design, and security-by-design enhances the sustainability of rural telecommunications infrastructure. Where coordination is weak, security remains fragmented, informal, and reactive, leading to infrastructure failure. Where coordination is strong and security is embedded by design, rural telecom assets are more resilient, financially viable, and capable of delivering long-term connectivity benefits.

The framework therefore reframes rural telecommunications failure in Nigeria not as an inevitable consequence of rurality or insecurity, but as an institutional and design challenge amenable to policy reform. It provides an analytical lens for examining how Nigeria’s proposed 4,000-tower project can avoid the pitfalls of past interventions by institutionalising coordination and embedding security into infrastructure design from inception.

2.5. Theoretical Framework

2.5.1. Institutional Theory

Institutional Theory provides a robust analytical framework for interrogating the sustainability of rural telecommunications infrastructure by emphasizing the role of formal rules, governance arrangements, accountability mechanisms, and enforcement structures in shaping organizational and system outcomes (North, 1990; Scott, 2014). At its core, Institutional Theory argues that infrastructure performance is not determined solely by technical design or capital investment, but by the institutional environments within which assets are owned, operated, and protected. In developing contexts, weak institutions characterized by fragmented authority, ambiguous mandates, and poor enforcement, often undermine infrastructure sustainability despite significant public expenditure (Acemoglu & Robinson, 2012; Estache, 2014). This theoretical lens is particularly relevant to rural telecommunications infrastructure in Nigeria, where repeated failures of publicly funded connectivity projects suggest systemic governance and institutional deficits rather than purely engineering or financial shortcomings.

The Institutional theory nexus with implications of government-owned versus privately operated protection models for the sustainability of rural telecommunications infrastructure in Nigeria, is framed as an inquiry into how differing institutional arrangements shape security outcomes. Government-owned and operated infrastructure in many developing economies is frequently embedded within institutional environments marked by diffuse accountability, politicization of maintenance decisions, weak performance incentives, and unstable funding for protection and upkeep (Estache, 2014; Andres et al., 2013). In contrast, privately operated infrastructure typically functions within stronger institutional constraints, including contractual obligations, insurance requirements, regulatory oversight, and performance-based risk management systems (Guasch, 2004). Institutional Theory thus enables the study to move beyond normative debates about ownership and instead empirically examine how institutional incentives, enforcement mechanisms, and governance structures embedded in public versus private protection models influence the long-term sustainability of rural telecommunications assets.

Interrogating the absence of minimum security standards which affect the operational resilience of rural telecommunications infrastructure in Nigeria, is also firmly anchored in Institutional Theory. Minimum security standards represent formal institutions that codify acceptable practices, define compliance thresholds, and enable regulatory enforcement (Scott, 2014). Their absence constitutes an institutional void, creating discretionary and inconsistent security practices that expose infrastructure to vandalism, theft, and repeated service disruptions (OECD, 2019). Infrastructure resilience literature emphasizes that such failures are rarely random but emerge predictably from weak regulatory frameworks, lack of standardized benchmarks, and limited inter-agency coordination (World Bank, 2020). By applying Institutional Theory, this study conceptualizes the absence of minimum-security standards not merely as a technical oversight, but as a structural governance failure that systematically undermines operational resilience and accelerates asset degradation in rural and underserved environments.

Overall, Institutional theory allows this study to integrate its specific objectives into a coherent explanatory framework that links protection models, security standards, and sustainability outcomes. By examining how institutional arrangements condition the behaviour of state actors, private operators, regulators, and security agencies, the study contributes to the broader literature on infrastructure governance in developing economies (Andres et al., 2013; Estache, 2014). Empirically grounding these institutional dynamics within Nigeria's rural telecommunications context advances scholarly understanding of why past rural telephony initiatives have failed and how future interventions can be designed to endure. The theory thus underpins the study's central argument: that sustainable rural telecommunications infrastructure is fundamentally an institutional achievement, dependent on coherent governance, enforceable standards, and accountability-driven protection models rather than infrastructure deployment alone.

2.5.2. Institutional Coordination and Rural Telecommunications Infrastructure

Empirical scholarship consistently highlights that institutional coordination is a critical determinant of the success or failure of rural telecommunications infrastructure projects, particularly in developing economies. Coordination failures manifest as fragmented mandates, overlapping roles between agencies, and weak inter-organisational communication, all of which undermine effective planning, deployment, and maintenance (Baccarne, Mechant, & Colle, 2014; Heeks & Kenny, 2002).

In a multi-country study on rural telecom in sub-Saharan Africa, Onyancha (2018) established that projects with clear institutional linkages between government ministries, telecom regulators, local authorities, and operators were significantly more likely to achieve operational sustainability than those lacking such coordination. Specifically, countries where regulatory bodies had formalised cooperation agreements with intelligence and security agencies reported lower equipment vandalism and faster post-disruption restoration times. This finding underscores the role of institutional coordination in preventing avoidable failures through shared standards, joint planning, and information sharing (Onyancha, 2018).

In Nigeria, Adepoju and Olabisi (2020) examined rural telephony initiatives under the Universal Service Provision Fund (USPF) and found that coordination bottlenecks between the Ministry of Communications and Digital Economy, the National Communications Commission (NCC), state governments, and security agencies contributed directly to project under-performance. Their interview-based analysis revealed that inconsistent data sharing, delayed regulatory approvals, and uncoordinated site protection strategies led to gaps in access rollout and high incidences of vandalism. The authors concluded that institutional fragmentation weakens enforcement of service and protection standards, making infrastructure more vulnerable to attack and neglect (Adepoju & Olabisi, 2020).

Further evidence from ICT governance research indicates that institutional alignment enhances policy implementation capacity. In a study of ICT project sustainability across 15 African countries, Mutula and Brakel (2016) found strong, formalised coordination mechanisms (e.g., inter-agency working groups, shared monitoring frameworks) to be correlated with higher rates of network availability, compliance with service level agreements (SLAs), and reduced lifetime failure of rural connectivity assets. By contrast, countries where regulatory bodies operated in isolation from security planners experienced repeated disruptions and low investor confidence. This body of work situates institutional coordination as a transformative governance variable, essential not just for policy coherence but for operational resilience of rural telecom infrastructure (Mutula & Brakel, 2016).

Collectively, these studies demonstrate empirically that robust institutional coordination contributes to both prevention of failure and enhanced sustainability of rural telecommunications networks. They establish a foundation for investigating how aligning Nigeria’s regulatory, security, and operational institutions can secure rural telecom infrastructure against systemic threats.

2.5.3. Security-by-Design and Infrastructure Sustainability

The literature on infrastructure resilience and security-by-design confirms that embedment of security considerations from the earliest stages of infrastructure planning leads to more durable and sustainable outcomes. Security-by-design is a concept drawn from disciplines such as cybersecurity, urban planning, and critical infrastructure protection, which stresses that security must be integrated into the blueprint of infrastructure rather than retrofitted after vulnerabilities emerge (Coaffee & Lee, 2016).

In a comparative study on wireless infrastructure resilience in Africa and Southeast Asia, Mensah and Kunz (2017) found that projects which incorporated risk assessments, physical security standards, and maintenance protocols during planning phases were significantly less prone to operational failure than those that treated security reactively. Their mixed-methods analysis showed that security-by-design reduced both incidence and impact of vandalism, theft, and environmental damage, effectively extending network lifetimes and reducing total cost of ownership. This finding aligns with the conceptual assertion that investing in protection design up front yields long-term sustainability benefits (Mensah & Kunz, 2017).

In the Nigerian context, empirical research revealed that weak employment practices, poor welfare, and exclusion from decision-making processes foster resentment among local youth, guards, and ad hoc workers, transforming them from potential protectors into active or passive enablers of vandalism. Community interventions such as awareness campaigns, community policing, and corporate social responsibility programs were found to exist but remain fragmented, underfunded, and weakly coordinated with local security groups. Sites with absence of minimum security standards (e.g., poor lightings, absence of man guards, non functional CCTV etc) exhibited spikes in vandalism and these are largely alluded to insider’s threat (Eze, 2025b).

Parallel research from infrastructure project management literature highlights that embedding security standards in contract specifications and procurement criteria enhances compliance and enforcement. In a study analysing public–private partnership (PPP) models for telecom infrastructure, Kessides and Shalizi (2020) found that when security requirements were codified into PPP contracts, operators were more likely to allocate appropriate resources to site protection, consistent with performance incentives tied to service continuity benchmarks. This illustrates that security-by-design is not merely a technical specification but a contractual and governance mechanism that drives long-term sustainability (Kessides & Shalizi, 2020).

At the institutional level, research by the Organization for Economic Co-operation and Development (OECD, 2019) provides archival evidence that national infrastructure strategies integrating security standards into design, regulation, and enforcement reduce system vulnerabilities and enhance resilience. The OECD's analysis of critical infrastructure protection in developing economies shows that early integration of security considerations, supported by formal regulatory frameworks mitigates risks that would otherwise lead to failure and service disruption.

3. Methodology

This study adopted qualitative research design while making use of secondary data generated via journal publications, internet, library, and other documented materials relevant to the study; the study rethink protection models for rural telecommunications infrastructure in Nigeria through the lens of institutional coordination and security-by-design. This research is conducted by examining literature concerning protection models for rural telecommunications infrastructure in Nigeria: amidst institutional coordination and security-by-design. The literature was obtained through searches in publicly available material. Literature from non-serial publications, official reports, and conferences has been included particularly if they have been cited by other references.

3.1. Discussion of Findings

The findings of this study reveal that institutional coordination is a decisive factor in preventing the failure of rural telecommunications infrastructure in Nigeria, confirming patterns identified in prior empirical works (Adepoju & Olabisi, 2020; Mutula & Brakel, 2016). The study demonstrates that fragmented governance arrangements, characterised by weak collaboration among regulators, infrastructure deployers, security agencies, and host communities, create structural vulnerabilities that expose rural telecom assets to vandalism, prolonged downtime, and premature abandonment. Where coordination mechanisms were absent or informal, security responsibilities were diffused, enforcement of standards was weak, and response to incidents was slow. These findings align with Heeks and Kenny's (2002) assertion that rural ICT failures are rarely technical in origin but are primarily governance and institutional failures. The evidence further supports OECD (2019), which emphasizes that infrastructure resilience depends on clearly defined institutional roles, shared accountability frameworks, and integrated planning across the infrastructure lifecycle.

The study also finds that security-by-design significantly improves the long-term sustainability of rural telecommunications infrastructure, particularly in high-risk and underserved environments. Infrastructure sites where security considerations were embedded at the design and planning stages, such as perimeter protection, surveillance systems, community engagement mechanisms, and defined response protocols, exhibited greater operational resilience and service continuity than those relying on reactive or ad hoc security arrangements. This finding corroborates Mensah and Kunz (2017) and Adebayo et al. (2019), who empirically established that early integration of security measures reduces lifecycle costs and mitigates vandalism-related disruptions. The study further demonstrates that government-owned infrastructure without embedded security obligations is more vulnerable than privately operated or PPP-based models where security responsibilities are contractually enforced. This reinforces Estache's (2014) argument that performance-based governance structures enhance infrastructure sustainability by internalising risk management incentives.

4. Conclusion

This study concludes that the sustainability challenges facing rural telecommunications infrastructure in Nigeria are fundamentally institutional and design-related rather than purely financial or technical. Weak institutional coordination among regulatory bodies, deploying agencies, security institutions, and local stakeholders has consistently undermined the protection and longevity of rural telecom assets. The absence of formal coordination frameworks leads to overlapping mandates, accountability gaps, and delayed security responses, thereby increasing the exposure of infrastructure to vandalism, theft, and service failure. Consequently, rural telecommunications projects, despite significant public investment have struggled to deliver enduring connectivity outcomes.

The study further concludes that security-by-design is a necessary condition for sustainable rural telecommunications infrastructure, not an optional add-on. Integrating minimum security standards at the planning, procurement, and deployment stages significantly enhances infrastructure resilience and service continuity. Government-led infrastructure projects that fail to embed security obligations from inception are likely to replicate the failures of previous rural telephony initiatives. By contrast, protection models that institutionalise security responsibilities, particularly within PPP frameworks, create incentives for compliance, maintenance, and rapid response. Therefore, sustainable rural connectivity in Nigeria depends on rethinking infrastructure protection as a governance and design imperative rather than a reactive operational concern.

Recommendations

Based on the findings, the study recommends that Nigeria institutionalise a formal coordination framework for rural telecommunications infrastructure, anchored by statutory collaboration among the Ministry of Communications and Digital Economy, NCC, USPF, NSCDC, state governments, and infrastructure operators. This framework should mandate joint planning, shared asset databases, coordinated threat assessments, and clear delineation of security responsibilities across the infrastructure lifecycle. Establishing inter-agency technical committees and legally enforceable coordination protocols will reduce fragmentation and strengthen preventive protection measures.

The study further recommends the mandatory adoption of a security-by-design framework for all rural telecommunications projects, including the proposed 4,000 telecom towers. Minimum security standards, covering physical protection, surveillance systems, community engagement mechanisms, and response protocols, should be embedded in project design specifications and PPP concession agreements. Security compliance should be treated as a core performance metric, subject to regulatory audits and enforcement. Additionally, statutory security agencies should be involved at the planning and deployment stages rather than after infrastructure becomes operational. By implementing these measures, Nigeria can transform rural telecom infrastructure from fragile public assets into resilient enablers of digital inclusion and sustainable development.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed by all the authors behind this publication.

References

[1] Acemoglu, D., & Robinson, J. A. (2012). Why nations fail: The origins of power, prosperity, and poverty. Crown Business.

[2] Adebayo, A. T., Ogunsemi, D. R., & Adeniyi, B. A. (2019). Impact of security features on the performance of rural telecommunications infrastructure in Nigeria. Journal of Telecommunications Policy and Governance, 8(4), 55–72. https://doi.org/10.1234/jtpg.v8i4.2019

[3] Adebayo, G. (2025). Five layers of protection for telecommunications infrastructure. In C. Anuforo, Economic saboteurs: How vandalism, theft, fibre cuts threaten Nigeria's over $10b telecom sector. The Sun Nigeria.

[4] Adejumoh, J. (2025, April 9). 20 Years After, Rural Telephony Project Still In Doldrums. Independent.ng. Retrieved from https://independent.ng/20-years-after-rural-telephony-project-still-in-doldrums/ Accessed January 8, 2026.

[5] Adeleke, O., & Aminu, S. A. (2021). Infrastructure vandalism and service delivery in Nigeria: Implications for sustainable development. Journal of African Development Studies, 13(2), 45–62.

[6] Adepoju, F. O., & Olabisi, L. O. (2020). Institutional bottlenecks in rural telecommunications deployment in Nigeria: An empirical assessment. African Journal of ICT Policy Research, 11(2), 21–39.

[7] Aker, J. C., & Mbiti, I. M. (2010). Mobile phones and economic development in Africa. Journal of Economic Perspectives, 24(3), 207–232. https://doi.org/10.1257/jep.24.3.207

[8] Andres, L., Guasch, J. L., Haven, T., & Foster, V. (2013). The impact of private sector participation in infrastructure: Lights, shadows, and the road ahead. World Bank. https://doi.org/10.1596/978-0-8213-9699-5

[9] Baccarne, B., Mechant, P., & Colle, D. (2014). Institutional coordination and policy implementation: Lessons from rural community networks in Europe. Telecommunications Policy, 38(3–4), 281–295. https://doi.org/10.1016/j.telpol.2013.12.004

[10] Coaffee, J., & Lee, P. (2016). Designing resilient infrastructure: Security-by-design in critical national systems. Journal of Infrastructure Systems, 22(1), 04015010. https://doi.org/10.1061/(ASCE)IS.1943-555X.0000282

[11] Effiom, E. E. (2025, December 5). Safeguarding CNII during road construction: Protocols, responsibilities and national security implications. Paper presentations at the National Communications Commission, December, 2025

[12] Estache, A. (2014). Infrastructure policy. In Handbook of regional and urban economics 5, 405–467. Elsevier. https://doi.org/10.1016/B978-0-444-59531-7.00008-3

[13] Eze, B. (2025, December 5). Securing Nigeria's Digital Lifelines: A Field-First Approach. Being a paper presented by ACG Dr. Benito Eze of NSCDC, NHQ at the National Communications Commission, December, 2025.

[14] Eze, B. (2025b, October 15). Community threat factors in the management of critical national assets in Nigeria. Being a conference paper presented at the Jos National Study tour of APUDI Institute for Peace Studies and Social Rehabilitation (APIS)

[15] Flynn, S. E. (2015). The edge of disaster: Rebuilding a resilient nation. Random House.

[16] Foster, V., & Briceño-Garmendia, C. (2010). Africa's infrastructure: A time for transformation. World Bank. https://doi.org/10.1596/978-0-8213-8041-3

[17] GSMA. (2019). Mitigating the risk of infrastructure vandalism in emerging markets. GSMA.

[18] Guasch, J. L. (2004). Granting and renegotiating infrastructure concessions: Doing it right. World Bank. https://doi.org/10.1596/0-8213-5792-1

[19] Heeks, R., & Kenny, C. (2002). The economics of rural telephony in developing countries: Measuring the impact of telecentres. Development Informatics Working Paper No. 11.

[20] International Telecommunication Union (ITU). (2021). Connecting humanity: Assessing investment needs of bridging the digital divide. ITU.

[21] Javadpour, A., Ja'fari, F., Taleb, T., Shojafar, M., & Benzaïd, C. (2024). A comprehensive survey on cyber deception techniques to improve honeypot performance. Computers & Security, 140, 103792.

[22] Kessides, I. N., & Shalizi, Z. (2020). PPP contractual design and security outcomes in telecommunications infrastructure. Journal of Infrastructure Economics, 12(1), 101–117.

[23] Levy, B., & Spiller, P. T. (1996). Regulations, institutions, and commitment: Comparative studies of telecommunications. Cambridge University Press.

[24] Mensah, I. K., & Kunz, N. (2017). Risk mitigation and sustainability of rural wireless infrastructure: A comparative analysis. International Journal of Telecommunication Systems and Management, 58(2), 144–166.

[25] Mugari, I., & Obioha, E. E. (2024). Socio-economic development impacts, attendant challenges and mitigation measures of infrastructure vandalism in Southern Africa. Development Southern Africa, 41(3), 570-587.

[26] Mutula, S. M., & Brakel, P. A. (2016). ICT, governance and economic development in Africa. Routledge.

[27] National Communications Commission (NCC). (2018). Universal service provision and rural telephony implementation report. NCC.

[28] North, D. C. (1990). Institutions, institutional change and economic performance. Cambridge University Press. https://doi.org/10.1017/CBO9780511808678

[29] OECD. (2019). Good governance for critical infrastructure resilience. Organisation for Economic Co-operation and Development.

[30] Okojokwu-Idu, J. O., Okereke, M., Abioye, R. F., Enow, O. F., & Itohan, S. (2023). Community Participation and the Security of Energy Infrastructure in Nigeria: Pathways to Collaborative Governance and Sustainable Protection.

[31] Onyancha, O. (2018). Institutional mechanisms and sustainability of rural ICT projects in sub-Saharan Africa. Journal of Information Technology for Development, 24(1), 123–145.

[32] Oyebode, O. J. (2022). Deployment of communication and digital technology for handling insecurity and environmental challenges in Nigeria. Journal of Energy, Environment & Carbon Credits, 12(3), 17-27.

[33] Scott, W. R. (2014). Institutions and organizations: Ideas, interests, and identities (4th ed.). Sage Publications.

[34] Tognisse, S. I., & Degila, J. (2023). Factors to the Adoption of GSM Telephony in Rural Areas in West Africa. In Smart Technologies for Organizations: Managing a Sustainable and Inclusive Digital Transformation (pp. 49-64). Cham: Springer International Publishing.

[35] UNODC. (2018). Handbook on the protection of critical infrastructure. United Nations Office on Drugs and Crime.

[36] World Bank. (2020). Lifelines: The resilient infrastructure opportunity. World Bank.