INTERNATIONAL JOURNAL OF SOCIAL SCIENCE, MANAGEMENT, PEACE AND CONFLICT RESEARCH (IJSMPCR)
Journal homepage: https://ijsmpcr.com/

Community stewardship, technological integration, and sustainable funding architecture in Nigeria's electricity infrastructure: Strategies for combating vandalism

By

[1]AHMED Abubakar Audi Prof., [2]BITRUS Alice Larai., [3]KESHINRO Adedotun Sunday., [4]KARSHI Kasimu Bako., [5]JIMOH Wasiu Ademola., [6]SULE Garba Abdullahi., & [7]ONIBIYO Rotimi Ezekiel

[1,2&3] Civil Defence Academy, Abuja

[3,4,5&6]Institute of Governance and Development Studies, Nasarawa State University Keffi

[7]Directorate of Critical National Assets and Infrastructure Protection, Office of National Security Advisers

International Journal of Social Science, Management, Peace and Conflict Research, 10(01), 020-032

Publication history: Received on November 05; Revised November 09; Accepted November 10, 2026

Abstract

Vandalism of power transmission infrastructure has become a structural threat to Nigeria's economic trajectory, yet the dominant policy response remains state-centric, reactive, and under-resourced. This paper investigates the interplay of three under-examined variables community buy-in, technology-integrated security response, and funding architecture in shaping anti-vandalism outcomes for Nigeria's transmission grid. Drawing on Elinor Ostrom's design principles for governing shared resources, the study opines that transmission corridors function as a "security commons" whose protection requires the active, incentivised participation of host communities rather than their passive acquiescence. Through an integrative review of peer-reviewed literature, policy documents, and institutional reports, the study submits that community buy-in influences anti-vandalism outcomes primarily through the mechanisms of social license, localised intelligence, and collective monitoring. This study validates that technology integration without community embeddedness produces detection without deterrence; and that Nigeria's funding architecture remains fragmented, with the Trace-Clearing Fund, the TCN Reserve Fund, and development-partner support operating in isolation rather than as a coherent financing system. The study proposes the establishment of an NSCDC Infrastructure Protection Trust Fund modelled on the recently renewed Police Trust Fund as the institutional anchor for a conditional, pooled, and performance-linked funding architecture that protects not only power transmission but also telecommunications and road infrastructure, thereby securing Nigeria's one-trillion-dollar economy ambition. The paper concludes that securing the grid requires a tripartite architecture in which communities are paid stewards, technology is community-embedded, and funding is pooled and conditional. Specifically, the paper recommends adoption of a Span-Based Community Stewardship model through registered Community Tower Trusts with performance-verified payments; establishment of a community-connected joint monitoring centre linking detection to community reporting and agency response; and finally the creation of the NSCDC Infrastructure Protection Trust Fund to ring-fence stewardship payments, fund technology and verification infrastructure, and establish State-Level Security Architecture in each state to synchronise Critical National Assets and Infrastructure Owners and Operators (CNAIO&O), security agencies, and communities in achieving infrastructure protection.

Keywords: Community Buy-In, NSCDC Infrastructure Protection Trust Fund, Power Transmission Tower Vandalism, Technology-Integrated Security

Introduction

Vandalism of electricity transmission infrastructure is not a Nigerian peculiarity, but its intensity and economic consequences are unusually severe in Nigeria. Globally, the World Bank has estimated that infrastructure vandalism and theft impose losses of approximately US$429 billion annually across developing economies, with power sector assets among the most exposed (World Bank Group, 2024). In Nigeria, the

* Corresponding author: **AHMED Abubakar Audi**
Nigeria Security and Civil Defence Corps Academy, Sauka, Abuja, Nigeria.

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.

Transmission Company of Nigeria (TCN) recorded a 25% increase in vandalism incidents in the last fiscal year, with the North-Central and South-South regions identified as high-volatility zones (NERC & GIZ, 2026). The vandalism of six transmission towers along the Apir–Makurdi line and 14 spans of conductors along the Lambata 132kV line illustrates the operational reality: repairs are mobilised, vandals strike again, and the cycle repeats (TCN, 2026a).

The economic stakes are captured in two figures. First, the daily GDP loss from power outages, measured through the Value of Lost Load metric, is estimated at ₦15 billion (Wakeel, 2026). Second, the broader economic damage lost productivity, alternative energy expenditure, and foregone investment is compounded by the fact that manufacturers spent over ₦1 trillion on alternative energy in 2024 alone (Audu-Ohwavborua, 2026). If Nigeria is to reach the trillion-dollar economy target, the transmission grid cannot remain a vandalised bottleneck.

Yet the policy response has remained predominantly state-centric: more guards, more patrols, more prosecutions. The Nigeria Security and Civil Defence Corps (NSCDC) the lead agency for the protection of Critical National Assets and Infrastructure (CNAI) under the NSCDC Act 2003 (as amended) has called for a deliberate shift from ad hoc and reactive approaches to a standardised, intelligence-led and technology-driven operational doctrine (Anumihe, 2026, Eze, 2026). The Office of the National Security Adviser (ONSA), through the Directorate of Critical National Assets and Infrastructure Protection (DCNAIP), has proposed a three-tier asset protection strategy of delay, awareness, and response (TCN, 2026a). These are necessary but insufficient. They address the *how* of protection but not the *who* and the *why*: who has a reason to protect the corridor, and why would they act on it?

Research Questions

This paper addresses the study gap through three research questions:

- **i.** To what extent does community buy-in influence anti-vandalism of power transmission infrastructure in Nigeria?
- **ii.** How does technology-integrated security response influence anti-vandalism of power transmission infrastructure in Nigeria?
- **iii.** Which funding models can secure Nigeria's one-trillion-dollar economy amid anti-vandalism of power transmission infrastructure?

Objective of the Study

The main objective of this study interrogates securing the grid, securing the economy: interplay of community buy-in, technology-integrated security, and funding architecture in Nigeria's Power Transmission Anti-Vandalism Strategy. While the specific objectives;

i. Examine how community buy-in influence anti-vandalism of power transmission infrastructure in Nigeria.
ii. Investigates the influence of technology-integrated security response on anti-vandalism of power transmission infrastructure in Nigeria
iii. Interrogates how funding models can secure Nigeria's one-trillion-dollar economy amid anti-vandalism of power transmission infrastructure.

Statement of the Problem

The problem is not a shortage of diagnoses. It is a shortage of integration. Nigeria has community sensitisation programmes, technology procurement ambitions, and development partner support through GIZ. What it lacks is an architecture that connects them. Communities are sensitised but not paid to do trace-clearing that can generate Community-buy in; technology is deployed but not embedded in community reporting networks and security agencies response; funding exists but is fragmented across mandates and institutions. The result is a protection system that detects some incidents, repairs some damage, and deters very little.

The consequence is not merely operational. It is economic. A vandalised transmission line is a destroyed revenue stream, a disrupted industrial corridor, and a signal to investors that Nigeria's infrastructure is unsecured. The trillion-dollar economy ambition cannot be financed on a grid that is treated as an open-access commons by those who live beside it. The work of Effiom et al. (2026) focused on rethinking protection models for rural telecommunications infrastructure in Nigeria, role of institutional coordination and security-by-design. while Gandi et al. (2025) also attended to the Unregulated scrap economy and the security of telecommunications infrastructure in Nigeria, Obasa et al. (2025) assessed the regulatory gaps in the Electricity Act 2023 through the Imo State electricity crisis as Nigeria unbundles electricity from the Exclusive list to both Concurrent and Residual list of the Nations constitution. Paucity of literature on community buy in, NSCDC Infrastructure Protection Trust Fund and Technology-Security response integration is a gap this study sets out to fill.

Significance of the Study

This significance of this study could be seen in its relevance to policy makers, Office of the National Security Advisers, Office of the Nigeria Homeland Security, National and State House of Assemblies, and Federal and State ministry of Power, Transmission Company of Nigeria, State Regulatory Agencies, Nigeria Security and Civil Defence Corps. This study integrates literatures on community-based security, technology adoption in infrastructure protection, and infrastructure financing that are usually treated separately. This study provides a theoretical grounding for community buy-in in infrastructure protection by applying Ostrom's design principles to transmission corridors as a “security commons”, moving the debate beyond the

assumption that communities are either threats or passive beneficiaries. This study opines the establishment of an NSCDC Infrastructure Protection Trust Fund as the institutional mechanism for a funding architecture that is conditional, pooled, and performance-linked, with direct implications for the protection of power transmission, telecommunications, and road infrastructure across Nigeria.

Literature Review

Community buy-in

Community Buy-in is the active endorsement and co-ownership of a project by local stakeholders, secured through inclusive decision-making, which grants social legitimacy, reduces socio-environmental risks, and ensures equitable access to benefits (Mehedi Hasan et al., 2026). This study operationalises it as the extent to which host communities perceive transmission infrastructure as a shared asset, accept a role in its protection, and act on that acceptance through reporting, monitoring, and non-interference. Operationally, it is measured through three indicators: community participation in corridor stewardship arrangements, the frequency and quality of community-originated incident reports, and the incidence of community-based obstruction (including vandalism by community members).

Technology-integrated security response

Technology Integrated with Security Responses is the embedding of IoT, AI, sensor networks, and real-time communication into a unified ecosystem that automates threat detection and response, while creating new privacy and security risks that require governance (Shekhar, 2026). This study operationalises it as the deployment of surveillance, detection, and communication technologies CCTV, sensors, drones, digital incident-reporting platforms, and central monitoring systems in coordination with security agencies and community reporting nodes. Operationally, it is measured through detection latency, response time, and the proportion of incidents detected by technology rather than by post-hoc inspection. Evolving technology profiled by local technology Solutions and advanced through DCNAIP-ONSA, NSCDC, Federal Ministry of Power, Nigerian Communication Commission has shown that technology-integrated security response that is woven round NSCDC and the community for responses can roll back power and telecom vandalism (Eze, 2026).

Funding architecture

This refers to the structure, sources, and conditions of financial flows dedicated to anti-vandalism. It encompasses the Trace-Clearing Fund, the TCN Reserve Fund, development partner contributions, and any performance-based or community-dividend mechanisms. Operationally, it is assessed through the adequacy, predictability, conditionality, and integration of funding streams.

NSCDC Infrastructure Protection Trust Fund

This is a dedicated, statutory funding mechanism modelled on the Nigeria Police Trust Fund established to provide sustainable, predictable, and ring-fenced financing for the protection of Critical National Assets and Infrastructure (CNAI) across Nigeria. It is conceived as the institutional anchor for a conditional, pooled, and performance-linked funding architecture that secures not only power transmission infrastructure but also telecommunications and road infrastructure the three asset classes that drive Nigeria's development and underpin the one-trillion-dollar economy ambition. Operationally, it is assessed through its statutory basis, funding adequacy, disbursement conditionality, and integration with existing funding streams and institutional mandates. Budgetary allocation in this order as done with the resuscitated Police Trust Fund will go a long way to protect Nigerias strides towards a trillion-dollar economy (Find it News, 2026)

Anti-vandalism

This is the prevention, detection, deterrence, and prosecution of acts that damage, disable, or interfere with transmission towers, conductors, and associated infrastructure. The Nigeria Security and Civil Defence Corps (NSCDC) is the lead agency for the protection of Critical National Assets and Infrastructure (CNAI) in Nigeria, as provided under the NSCDC Act 2003 (as amended). The Corps' mandate encompasses the protection of power transmission, telecommunications, road, oil and gas, and other designated CNAI sectors. The Directorate of Critical National Assets and Infrastructure Protection (DCNAIP) in the Office of the National Security Adviser (ONSA) coordinates the efforts of CNAI Owners and Operators (CNAIO&O), security agencies, and communities in achieving infrastructure protection. This coordination role is essential to synchronising the various actors and ensuring that infrastructure protection is approached as a collective responsibility rather than a fragmented institutional mandate.

Empirical Literature Review

Community Buy-In and Infrastructure Protection

The empirical literature on community-based security in Nigeria is consistent on one point: community-led mechanisms succeed where legal recognition, oversight, and intergroup trust are present, and fail where fragmentation and impunity persist (Jatau et al., 2025). This finding, derived from a review of community policing initiatives across Nigeria, applies directly to transmission corridors. The most cited Nigerian case is the Niger Delta pipeline surveillance arrangement, where a private contractor (Tantita) employed thousands of local guards, monitors, and informants under a community-based surveillance model (Zenodo, 2026). Analysts attribute a reported 50% rise in oil production and a decline in oil theft to the combination of technological surveillance and community-based intelligence gathering (Rufus & Tokpo, 2026). The

Petroleum Industry Act 2021 institutionalised a parallel structure through Host Community Development Trusts (Sections 234–258), empowering host communities to participate in safeguarding critical oil and gas infrastructure (Vanguard, 2026).

For power transmission specifically, TCN has intensified community sensitisation across the country, engaging host communities, traditional rulers, and security agencies to promote collective ownership and protection of transmission facilities (TCN, 2026a). NERC and GIZ have explicitly integrated the "human element" into their anti-vandalism framework, training local technicians and engaging host communities to recognise power assets as public utilities rather than isolated government properties, with the stated aim of reducing the "social license" that allows vandals to operate undetected (Uma, 2026). However, no peer-reviewed empirical study has yet measured the causal effect of community buy-in on transmission vandalism rates in Nigeria. The literature establishes plausibility and mechanism but not magnitude.

Technology-Integrated Security and Vandalism

The technology literature is more developed but equally fragmented. Ogidan et al. (2021) developed an image surveillance system for transformer substations, finding that automated visual monitoring produces a great reduction in power facilities vandalism and improved supply security. Enoch (2023) demonstrated a dual-surveillance monitoring technique using PIR sensors for perimeter detection. Umunnakwe et al. (2023) addressed the situational-awareness deficit in the Nigerian grid, arguing that reliability issues and vandalism are exacerbated by minimal situational awareness available to operators. At the institutional level, NSCDC has called for CCTV systems, sensors, drones, and digital incident-reporting platforms to complement gates, fences, and patrols (Anumihe, 2026), while TCN and NSCDC have proposed a joint monitoring centre for real-time monitoring of transmission assets (TCN, 2026a).

The empirical limitation is significant. Most studies evaluate technology in laboratory or single-site conditions. None measures the interaction between technology deployment and community reporting density. The three-tier strategy proposed by ONSA delay, awareness, response implicitly recognises that technology alone is insufficient: awareness" requires a reporting network, and "response requires local presence (TCN, 2026a). The literature does not yet tell us whether technology without community embeddedness produces detection without deterrence.

Funding Models for Anti-Vandalism

The funding literature is the thinnest of the three. NERC and GIZ have partnered through the Nigerian Energy Support Programme, co-funded by the European Union and the German Federal Ministry for Economic Cooperation and Development, to provide technical assistance for community-based surveillance and

electronic monitoring (Uma, 2026). The Federal Government has signalled the need for stricter laws and increased funding, with the Minister of Power describing vandalism as economic sabotage (Oladipo, 2025). An "Anti-Theft Fund" has been proposed to incentivise aggressive enforcement (Vanguard, 2026). The TCN Reserve Fund held at the Central Bank of Nigeria has been identified as a potential source for infrastructure vulnerability reduction (Committee document, 2026). The Petroleum Industry Act provides a statutory three per cent operational expenditure allocation for host community development in the oil sector (Vanguard, 2026), but no equivalent statutory community fund exists for power transmission and other infrastructure.

The gap is not the absence of money. It is the absence of a funding architecture, the absence of funding model to protects Nigeria's CNAI similar to Police Trust fund is concerning and cast doubts on the Nigerias determination towards her one-trillion-dollar economy which is mainly driven by infrastructure deployment. The vulnerability of infrastructure will be the absence of a protection fund. This paper treats that gap as central, hence the need for the NSCDC Infrastructure Protection Trust Fund as the institutional solution even as the National Assembly budgeted ₦403billion for Police Trust Fund (Katuka, 2026; Find it news, 2026).

Theoretical Framework

Ostrom's Design Principles and the Security Commons

This paper is underpinned by Elinor Ostrom's institutional theory of collective action, specifically her design principles for governing common-pool resources (Ostrom, 1990). Ostrom demonstrated that communities can and do self-organise to manage shared resources sustainably when eight conditions are met: clearly defined boundaries; rules that fit local conditions; collective-choice arrangements that include affected users; effective monitoring by accountable monitors; graduated sanctions; accessible conflict-resolution mechanisms; recognition of the right to organise; and nested enterprises for larger systems (Ostrom, 1990; Ostrom, 2005).

The application to transmission corridors requires a conceptual move. A transmission line is not a common-pool resource in the traditional sense: it is a state-owned asset, not a subtractable resource harvested by users. But the *security* of that line is a commons. It is produced jointly by the operator (TCN), the security agency (NSCDC), and the host community. It is degraded by any single actor's failure, a community that allows vandals passage, an operator that neglects monitoring, an agency that does not respond. No single actor can secure the corridor alone, and the benefits of a secure corridor are non-excludable across the host community. This is the defining structure of a commons dilemma: individual rationality (look the other way, or even collaborate with vandals) produces collective irrationality (a vandalised corridor that harms everyone).

Ostrom's principles map directly onto the three research questions posed by this study. On community buy-in; Principles 1 of Ostrom theory clearly defined boundaries, 3 speaks on collective-choice arrangements, and principle 4 doted on monitoring and all these specify what buy-in must look like institutionally not sensitisation alone, but boundaries (who is responsible for which span), voice (community participation in corridor governance), and monitoring (community members as accountable monitors as farmers, herders, loggers, wood hewers, and traders around the transmission towers). The absence of these conditions explains why sensitisation without payment and governance produces acquiescence without guardianship.

For technology security integration; Principles 4 (monitoring) and 8 (nested enterprises) locate technology within a layered monitoring system. Technology is a monitoring instrument, but Ostrom's principle requires that monitors be accountable to the users which means technology must be embedded in community reporting structures, not imposed from above. On the funding to secure CNAI protection; Principles 2 (local fit), 5 (graduated sanctions), and 6 (conflict resolution) imply that funding must be conditional, locally calibrated, and tied to verifiable behaviour. A fund that pays for clearing but not for stewardship violates the principle that rules must fit local conditions and that sanctions (or bonuses) must be graduated and earned. The proposed NSCDC Infrastructure Protection Trust Fund is the institutional mechanism that operationalises these principles at scale providing the pooled, conditional, and performance-linked financing that Ostrom's theory requires. Ostrom's theory therefore does more than describe the problem. It specifies the design conditions under which community buy-in, technology, and funding become complementary rather than substitutable.

Research Methodology

This study adopts qualitative desktop research design, also known as documentary or secondary data analysis. Desktop research is a systematic method of collecting, evaluating, and synthesising existing published and unpublished sources to answer specific research questions without the need for primary data collection (Bowen, 2009). This design is particularly appropriate for the present study for three reasons. First, the security environment across much of Nigeria remains volatile, making primary data collection in conflict-affected communities both dangerous and ethically problematic. This study sourced data from Peer-reviewed journal articles, Policy reports and working papers, government documents, and credible media reports and investigative journalism from established Nigerian and international news outlets/

Discussion of Findings

The literature supports a positive relationship between community buy-in and anti-vandalism outcomes, but the mechanism is institutional rather than attitudinal. Sensitisation alone TCN's community engagement

programmes, for example creates awareness but not obligation (TCN, 2026b). The Niger Delta case demonstrates that when communities are employed, paid, and embedded in surveillance, intelligence quality improves and large-scale theft declines (Zenodo, 2026; Rufus & Otokpo, 2026). The PIA's Host Community Development Trust model formalises this insight: participation is structured, funded, and legally recognised (Vanguard, 2026). The finding aligns with Jatau et al. (2025), who conclude that community-led security succeeds only where legal recognition and oversight are present. It contradicts the implicit assumption in much of the policy discourse that communities are either threats to be policed or beneficiaries to be sensitised. The evidence suggests they are *suppliers* of a security service who will supply it reliably only when the terms of supply are clear, funded, and enforceable. The limitation of the existing literature is that no study has measured the dose-response relationship: how much buy-in produces how much reduction in vandalism. The Tantita experience suggests the effect is large, but it is confounded by the simultaneous deployment of technology and by the distinctive political economy of the Niger Delta.

Empirical literature on technology enhance security establishes that surveillance and detection systems reduce vandalism in controlled settings (Ogidan et al., 2021; Enoch, 2023). The institutional literature establishes that technology is being deployed and that agencies recognise its necessity (NSCDC, 2026; TCN, 2026a). But the two literatures do not meet. No study demonstrates that a technology-integrated response system, operating at corridor scale and connected to community reporting, produces a measurable reduction in transmission vandalism in Nigeria. The finding that emerges is conditional; technology influences anti-vandalism outcomes when it is embedded in a response architecture that includes community reporting and rapid agency action. ONSA's three-tier strategy delay, awareness, response is an implicit acknowledgment that technology is the middle tier, not the whole system (TCN, 2026a). A drone that detects a vandal but cannot trigger a community guardian or an NSCDC patrol within the relevant time window produces data, not deterrence. This aligns with Umunnakwe et al. (2023), who locate the Nigerian grid's problem in "minimal situational awareness" rather than in the absence of sensors per se. It contradicts the technology-determinist strand in the policy discourse that treats procurement as the solution.

The literature reveals a funding landscape that is plural but uncoordinated. GIZ and NERC operate a technical assistance programme (Uma, 2026); the Federal Government has proposed an Anti-Theft Fund (Vanguard, 2026); the TCN Reserve Fund is a potential domestic source; and the PIA provides a statutory community fund for the oil sector that has no power-sector equivalent. The finding is that the funding *model* matters more than the funding *amount*. A fund that pays only for clearing produces cleared corridors that revert. A fund that pays only for enforcement produces enforcement without intelligence. A fund that pays communities for stewardship conditional on verified absence of unreported incidents produces the monitoring

behaviour that Ostrom's theory predicts. This paper proposes that the institutional solution is the establishment of an NSCDC Infrastructure Protection Trust Fund, modelled on the Nigeria Police Trust Fund, which was recently renewed through budgetary provision. The Police Trust Fund demonstrates that Nigeria can legislate and fund a dedicated, statutory mechanism for security-related expenditure. The NSCDC Infrastructure Protection Trust Fund would extend that logic to the protection of Critical National Assets and Infrastructure (CNAI) power transmission, telecommunications, and roads which are the drivers of Nigeria's development and the foundation of the one-trillion-dollar economy ambition. The Fund would (i) ring-fence a stewardship component for community guardian payments; (ii) provide dedicated financing for technology and verification infrastructure; (iii) support the establishment of State-Level Security Architecture in each state to synchronise CNAIO&O, security agencies, and communities; and (iv) disburse all funding against a single performance framework that measures communities, TCN, and NSCDC on the same corridor-level outcomes. This aligns with the broader literature on performance-based financing in infrastructure, which finds that conditionality and verification are more important than volume. It contradicts the implicit assumption in much of the policy advocacy that the problem is simply more money for power infrastructure. Nigeria's power sector faces a ₦4 trillion funding gap, but a gap filled with unconditional money will produce the same outcome as no funding at all as repaired towers are vandalised again.

Conclusion

Community buy-in influences anti-vandalism outcomes to the extent that it is institutionalised as a paid, governed, and monitored relationship rather than a sensitisation campaign. The evidence from Nigeria's oil sector and from TCN's community engagement suggests that communities will supply security intelligence and corridor stewardship when the terms are clear, funded, and enforceable. Sensitisation without stewardship produces awareness without obligation.

Technology-integrated security response influences anti-vandalism outcomes when it is embedded in a layered architecture that connects detection to community reporting and agency response. Technology alone produces data; technology embedded in a commons-governance structure produces deterrence.

The funding model that can secure Nigeria's trillion-dollar economy is not a single fund but a conditional architecture anchored in the proposed NSCDC Infrastructure Protection Trust Fund pooled resources from the Trace-Clearing Fund, the TCN Reserve Fund, and development partners, disbursed against verified performance, with a ring-fenced stewardship component that pays communities for protection rather than only for labour. The Trust Fund would secure not only power transmission but also telecommunications and road infrastructure; the three asset classes that drive Nigeria's development and underpin the one-trillion-

dollar economy ambition. It would establish State-Level Security Architecture in each state to synchronise CNAIO&O, security agencies, and communities in achieving infrastructure protection.

Recommendations

i. That the Federal Ministry of Power should adopt a Span-Based Community Stewardship model in which host communities are contracted, through registered Community Tower Trusts, to clear and maintain defined spans of the transmission corridor and are paid a recurring stewardship bonus conditional on the absence of unreported incidents on those spans. Payment should be verified through geotagged evidence, triple sign-off (TCN, NSCDC, community), and random re-inspection. No community should be mobilised until its funds are in the Trust account.

ii. On technology Technology-Integrated Security; TCN and NSCDC should establish the proposed joint monitoring centre as a community-connected node, not a stand-alone operations room. Community Tower Guardians should be registered as reporting nodes on the Central Incidence Reporting and Monitoring System and the toll-free reporting line. Technology procurement should be assessed against a single criterion: does it shorten the time between detection and community-or-agency response? Drones and sensors that do not feed into that loop should be deprioritised. The DCNAIP should coordinate the synchronisation of CNAIO&O, security agencies, and community reporting nodes to ensure a unified response architecture.

iii. The Federal Government should establish an NSCDC Infrastructure Protection Trust Fund, modelled on the Nigeria Police Trust Fund, to provide dedicated, statutory, and ring-fenced financing for the protection of Critical National Assets and Infrastructure (CNAI) power transmission, telecommunications, and roads. The Fund should ring-fence a stewardship component within the Trace-Clearing Fund, distinct from the clearing component, so that guardian payments cannot be diverted to labour; (b) provide dedicated financing for technology and verification infrastructure (satellite imagery, geotagged evidence, random re-inspection); (c) support the establishment of State-Level Security Architecture in each state to synchronise CNAIO&O, security agencies, and communities; and (d) disburse all funding against a single performance framework, so that communities, TCN, and NSCDC are measured on the same corridor-level outcomes. The Fund should be positioned as the institutional mechanism for securing Nigeria's one-trillion-dollar economy through the deliberate protection of the infrastructure that drives development.

References

Anumihe, I. (2026, September 5). NSCDC moves for technology-driven operations to tackle vandalism, theft of CNAI. *The Sun Nigeria*. Retrieved from https://thesun.ng/nscdc-moves-for-technology-driven-operations-to-tackle-vandalism-theft-of-cnai/ Accessed on September 28 2026

Audu-Ohwavborua, E. (2026, January 16). Nigeria's power crisis: A security and economic emergency. *LinkedIn*. https://www.linkedin.com

Committee on Protection of Critical Power Infrastructure. (2026). *Report of the Inter-Agency Committee on Protection of Critical Power Infrastructure in Nigeria*. Federal Ministry of Power.

Effiom, E. E., Eze, B. E., Keshinro, S. A., Adebayo, G., Zamani, A. E. Prof., and Onibiyo, E. R. (2026). Rethinking protection models for rural telecommunications infrastructure in Nigeria: The role of institutional coordination and security-by-design. *World Journal of Advanced Research and Reviews, 29*(03), 034–043 https://doi.org/10.3057 4/wjarr.2026.29.3.0399

Enoch, A. (2023). Development of distribution transformer substation anti-vandalism using dual-surveillance monitoring technique. *KWASU Space*. https://kwasuspace.kwasu.edu.ng

Erunke, J. (2026, June 2). Niger Delta leaders, Reps reject calls to break up Tantita contract. *Vanguard*. Retrieved from https://www.vanguardngr.com/2026/06/niger-delta-leaders-reps-reject-calls-to-break-up-tantita-contract/ Accessed October 17, 2026

Eze, B. E. (2026). *Critical Infrastructure Protection in Nigeria: The NSCDC CNAI Experience. ISBN:978-978-68-9923-7. K-Media Consult Limited*

Find it News. (2026, November 3). NSCDC Gombe Nabs 22-Year-Old Cable Vandal, Recovers 968.4 Metres in Twin Anti-Vandalism Breakthrough. *Find it News*. Retrieved from https://finditnews.com.ng/nscdc-gombe-nabs-22-year-old-cable-vandal-recovers-968-4-metres-in-twin-anti-vandalism-breakthrough/ Accessed November 7, 2026

Gandi, A. A, Adesuyi, O. M., Zamani, A. E. Prof., Onibiyo, e. R. (2025). Unregulated scrap economy and the security of telecommunications infrastructure in Nigeria. International *Journal of Social Science, Management, Peace and Conflict Research, I11*(01), 173-185.

Jatau, P. M., Lenshie, N. E., & Okoli, A. C. (2025). Security governance and the necessity for community-led approaches in Nigeria. *African Solutions (AfSOL) Journal, 6*(1), 29.

Katuka, M. (2026, July 9). Senate Approves ₦403.1 Billion Police Trust Fund Budgets to Strengthen National Security and Operational Capacity. *National Assembly Library Trust Fund.* Retrieved from https://naltf.gov.ng/senate-approves-%E2%82%A6403-1-billion-police-trust-fund-budgets-to-strengthen-national-security-and-operational-capacity/ Accessed November 1, 2026.

Mehedi Hasan, M., Shafeeul Islam, S.M., Misra, V. (2026). Social Inclusion and Community Engagement in Sustainable Infrastructure Governance. In: Sharma, V., Idziak, E., de Vasconcelos, J.B., Kurucz, A. (eds) *Infrastructure Finance and Sustainable Governance. World Sustainability Series.* Springer, Cham. https://doi.org/10.1007/978-3-032-07224-5_9

Obasa, A. B., Adesuyi, O. M., Vinci, F. O., Zamani, A. E., Onibiyo, E. R. (2025). Assessing the regulatory gaps in the Electricity Act 2023 through the Imo State electricity crisis. *World Journal of Advanced Research and Reviews, 28*(03), 2226-2236. Article DOI: https://doi.org/10.30574/wjarr.2025.28.3.4321

Ogidan, O. K., Olakunle, O. R., & Temikotan, K. O. (2021). Intrusion detection and automated monitoring for protection of critical infrastructures. *Zenodo*. https://www.zenodo.org

Oladipo, O. (2025, May 20). FG accuses DisCos of frustrating power sector reforms. *BusinessDay*. Retrieved from https://businessday.ng/energy/power/article/fg-accuses-discos-of-frustrating-power-sector-reforms/ Accessed October 1 2026

Onibiyo E. R (2026). CNAI Protection and the Terrorism Nexus the Waste Economy, Metal Recycling Industries, and the Financing of Insecurity: Lessons from the NSCDC–Guards Brigade Joint Operation in Idu. In Eze Benito's *Critical Infrastructure Protection in Nigeria: The NSCDC CNAI Experience*. ISBN:978-978-68-9923-7. K-Media Consult Limited

Ostrom, E. (1990). *Governing the commons: The evolution of institutions for collective action*. Cambridge University Press.

Ostrom, E. (2005). *Understanding institutional diversity*. Princeton University Press.

Rufus, A., & Tokpo, C. E. (2026). Oil surveillance contracts and its impact on oil output and environmental protection in the Niger Delta. *International Journal of African Development and Sustainable Research*.

TCN. (2026a, June 18). TCN, ONSA and NSCDC strengthen collaboration against vandalism of power infrastructure. *TCN News*. https://www.tcnnews.ng

TCN. (2026b, October 24). TCN sensitises stakeholders on vandalism, right-of-way encroachment. *Leadership*. https://leadership.ng

Uma, B. (2026, February 17). NERC and GIZ partner to combat power vandalism. *Daily Times Nigeria*. Retrieved from https://dailytimesng.com/nerc-and-giz-partner-to-combat-power-vandalism/ Accessed October 24, 2026

Umunnakwe, A., Alimi, A., Davis, K. R., & Butler-Purry, K. L. (2023). Improving Situational Awareness in Power Grids of Developing Countries: A Case Study of the Nigerian Grid. *2023 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT),* Washington, DC, USA,pp. 1-5, doi: 10.1109/ISGT51731.2023.10066359.

Wakeel, A. (2026, May 28). Why are we vandalising our own future? *The Guardian Nigeria*. Retrieved from https://guardian.ng/opinion/why-are-we-vandalising-our-own-future/ Accessed October16, 2026

World Bank Group (2024). Benchmarking Infrastructure Development: PPP Regulatory Landscape, Assessing Quality and Exploring Reforms. World Bank Group. Retrieved from https://documents1.worldbank.org/curated/en/099091724141032233 /pdf/P5004 58-fa9a6675-ed6d-4129-a87d-a08e7c377b6f.pdf Accessed October 3, 2026

Zenodo. (2026). *Pipeline vandalism and energy security in Nigeria: The emerging role of non-state actors in infrastructure security*. https://www.zenodo.org