ASSESSING THE ROLE OF SURVEILLANCE TECHNOLOGIES IN ADDRESSING INSECURITY IN NIGERIA

Samuel, Aretha Rekiya (PhD)
Department of Sociology,
Faculty of Social Sciences, University of Jos

Fullpower, Tamarautare Esther
School of Postgraduate Studies,
Department of Sociology & Anthropology,
Federal University Otuoke, Bayelsa State, Nigeria

Oyedoyin Abiola Oyerinde
Department of Sociology,
Faculty of Social Sciences, University of Jos

Abstract

Nigeria's persistent insecurity crisis, which includes terrorism, kidnapping, banditry, and armed insurgency, has exposed a lingering failure by the government to achieve its core obligation of protecting its citizens. Within the social contract tradition, state legitimacy depends on its capacity to protect (Hobbes, 1651; Locke, 1689), a capacity that the Nigerian government has consistently struggled to do. Since modern surveillance technologies have shown measurable reductions in crime in other contexts, academic attention to how these tools have been governed and deployed in Nigeria remains limited. This study assesses the role of surveillance technologies, especially closed-circuit television (CCTV), biometric systems, facial recognition platforms, and predictive policing tools, in addressing Nigeria's insecurity challenges. The study also identifies the institutional, legal, and technical obstacles that limit their effective use. The study relies on qualitative document analysis and thematic coding (Braun & Clarke, 2006) of peer-reviewed literature, official policy documents, and international security reports from 2005 to 2023. It is anchored in structural functionalist theory (Parsons, 1951). Findings from the study show that while these technologies have worked in similar settings, their use in Nigeria has been fragmented, underfunded, and poorly governed. The primary obstacle is weak institutional capacity rather than a shortage of technology. The study therefore recommends a phased, governance-centred national surveillance framework supported by the right legislation, sustained budget commitment and mandatory capacity building across security agencies.

Keywords: Surveillance Technologies, Security Governance, Insecurity, Nigeria, Structural Functionalism and ICT.

Introduction

Technology is playing a very important role in crime control globally. According to the United Nations Office on Drugs and Crime (UNODC, 2021), countries that have integrated digital surveillance technologies into law enforcement frameworks have recorded measurable reductions in crime rates, particularly in urban areas. In Sub-Saharan Africa, nations such as

Kenya and South Africa have begun using CCTV and biometric systems to ensure public safety, highlighting the growing relevance of these tools on the continent.

Modern surveillance technologies refer to digital systems used to track or monitor persons, places, or activities (Lyon, 2007; Zureik & Salter, 2013). These include facial recognition platforms, biometric identity systems, license plate readers, satellite imagery, data mining tools, and predictive policing algorithms. Each extends the state's capacity to detect threats before they occur, identify suspects after incidents, and monitor environments that might otherwise remain ungoverned.

Nigeria is not absent from this worldwide conversation. Some CCTV infrastructure has been installed in Lagos, biometric identity projects have been launched, and official policy documents reference the importance of ICT in security governance. However, the gap between stated intention and operational reality remains wide. Oludare, Omolara, Umar, and Kemi (2015) observed over a decade ago that addressing Nigeria's insecurity problem requires embracing technologies such as satellite monitoring, data interception, and digital intelligence. This observation has gained rather than lost relevance as both the nature of Nigeria's security threats and the available technological options have continued to evolve.

The consequences of insecurity in Nigeria are concrete and daily. Communities have been displaced by Boko Haram in Borno State. Kidnappings in Kaduna have shattered families. Farmers cannot reach their fields for fear of armed herders. Traders factor ransom costs into their business calculations. Conventional responses such as troop deployments, vigilante funding, and emergency management committees have not contained these challenges. Technology-based approaches offer an additional set of tools for monitoring, anticipating, and disrupting criminal activity.

Nigeria's security conditions have declined in recent years. Boko Haram and its various factions continue to make the North-East unstable. Bandits carry out unconstrained attacks across large parts of the North-West and North-Central. Violent clashes between herders and farmers generate recurring fatalities across the Middle Belt. Kidnapping has become a regularised criminal enterprise in several regions. This study does not ask whether Nigeria has a security problem, since that is well established, but rather asks: to what extent can modern surveillance technologies serve as a governance instrument for addressing these challenges, and what has prevented their effective deployment?

The existing literature on Nigerian insecurity has largely focused on political drivers, socioeconomic roots of radicalisation, military counterterrorism failures, and humanitarian consequences of armed conflict. Relatively little scholarly attention has been directed at the surveillance technology dimension as a governance issue. Key questions remain underexplored: which technologies are available; how they are being deployed within Nigeria's security architecture; and what institutional, legal, and resource conditions would need to change for effective deployment. This study addresses those questions by linking global surveillance technology governance frameworks to the Nigerian context and identifying the structural barriers constraining effective adoption.

Background to the Study

Nigeria faces very serious and underlying security issues. According to the Global Terrorism Index 2023, Nigeria ranked eighth among the most terrorism-affected countries in the world. The Armed Conflict Location and Event Data Project (ACLED, 2023) recorded over 5,000

conflict-related deaths in 2022 alone. The principal terrorist group, which is the Boko Haram, has waged an insurgency in the North since 2009, targeting civilians, schools, markets, and military bases. The Islamic State West Africa Province (ISWAP), which is a faction of Boko Haram, continues to carry out attacks alongside other armed groups.

Beyond terrorism, banditry is on the rise in the North-west and North-central regions of Nigeria. Armed groups, also known as gunmen, have carried out attacks on villages, as well as kidnappings and livestock rustling. Contributing factors include: poverty, unemployment, limited state presence, and a weakened formal justice system in affected areas. Violent clashes between herders and farmers represent an additional dimension of insecurity, exacerbated by population growth, environmental degradation, and competition for land and water resources. Kidnapping has grown from an insurgency tool in the North-east and South-south to a widely criminalised enterprise, with both short-term ransom cases and long-term ideologically motivated abductions recorded across multiple geopolitical zones in Nigeria.

These overlying threats create what scholars describe as the critical 'surveillance deficit' (Lyon, 2007; Zuboff, 2019): the Nigerian state lacks the technological infrastructure to monitor and foresee criminal activity, while criminal actors exploit physical and digital spaces with relative freedom. Deploying modern surveillance technologies has therefore become a governance imperative, not just a technological upgrade. Without effective monitoring systems, the Nigerian government may not be able to fulfil its obligations to protect its citizens, maintain territorial integrity, or create conditions for socioeconomic development.

Conceptual Framework

Surveillance Technologies and Security Governance

Information and Communication Technology (ICT) refers to the integration of computing and telecommunications into a single technological ecosystem. Over the past three decades, this convergence has expanded across a wide range of applications. These range from routine functions such as office data management and email communication to more strategically critical uses, including remote sensing, satellite monitoring, biometric identification, and real-time surveillance networks. For security governance, the implications are significant. According to Uchenna, Chukwuemeka, and Chukwuka (2018), the same networks that connect businesses and universities also enable the collection, processing, and dissemination of security-relevant intelligence at speeds and scales that were previously unthinkable.

Adams (2016) describes ICT as a general term for communication and information management devices such as radio, cellular, satellite, and computer-based systems. These tools are morally neutral; that is to say, a facial recognition system can help police identify a terrorist or be misused to target journalists or political opponents. This dual-use character also suggests that governance is central. The relevant question is not whether the technology works but who uses it, under what rules, and with what accountability.

The Concept of Security

Security as a concept carries a long and much-contested intellectual pedigree. Its classical formulation is rooted in the social contract tradition, and centres on the state as the primary guarantor of safety. This is to say that citizens surrendered a certain percentage of their freedom to a governing authority in exchange for protection from violence, disorder, and

external threat (Stan, 2004; Hobbes, 1651; Locke, 1689). For the greater part of the twentieth century, this state-centric conception dominated both policy and academic discourse. The end of the Cold War began to unravel this narrow framing. The United Nations Development Program (UNDP, 1994), in its landmark Human Development Report, argued cogently that security must be reconceived around the individual rather than the state. A citizen who is hungry, diseased or living in daily-to-day fear of criminal violence is not secure, regardless of how well defended the nation's borders may be. This human security model has long been an important reference point in security studies (Nwanegbo & Odigbo, 2013; Krahmann, 2003).

Odeh and Umoh (2015) situate national security within this broader conceptual terrain, defining it as the safety and survival of both the state and the citizens from harm, destruction, or dangerous threats. They identified about seven overlapping dimensions,including economic, food, health, environmental, personal, community, and political security. Security is therefore not simply the absence of armed conflict in a country but the presence of conditions that allow citizens to live, work, and pursue their ambitions without constant threats to their safety or welfare.

In the twenty-first century, digital security has emerged as a critical dimension of national security governance. Scholars, including Zureik and Salter (2013) and Lyon (2007), have argued that modern states increasingly rely on surveillance technologies such as CCTV systems, biometric databases, and digital intelligence networks as instruments of security governance. This reflects a broader shift away from purely military- or police-centred security approaches toward technology-supported methods that can monitor, detect, and respond to threats in real time.

This study adopts a working definition of security drawn from the human security and digital governance traditions reviewed above. Security, in this context, refers to the state's effective protection of its citizens' lives, property, and fundamental freedoms from physical violence and criminal threat, achieved through functioning institutions and the deployment of technological monitoring systems capable of detecting and disrupting threats in real time (Zureik & Salter, 2013). This definition is institutional in emphasis. It does not exclude the military or social dimensions of security. However, itcentres on the governance capacity of the Nigerian state, as this study identifies it as the decisive variable.

Empirical Review

The empirical literature on surveillance technologies can be divided into geography and analytical focus. Three bodies of work are also relevant to this study, each with its own distinct strengths and limitations that inform how their outcomes are applied.

Evidence from Advanced Economies

The first and most substantial strand documents the effectiveness of surveillance technology in high-income countries. The case for CCTV is well established, Chainey and Ratcliffe (2005) found major crime deterrence from camera deployment across UK sites. Welsh and Farrington (2009) conducted a systematic review of 44 studies from the UK and the USA and reported an average crime reduction of 16% in surveillance areas. More recently, Ratcliffe, Groff, Haberman, and Taniguchi (2019) reported that predictive policing tools, when combined with meaningful community engagement, reduced violent crime in Philadelphia by about 20% over two years. These findings carry an important caveat: they were generated in high-income, technology-rich institutional environments with stable electricity, trained

personnel, and functioning accountability structures. Therefore, transposing these directly to Nigeria without accounting for its very different institutional, infrastructural, and governance realities would be an analytical carelessness.

African Context

The second strand narrows its geographic focus to Africa. Amara (2016) looks into Kenya's implementation of biometric surveillance following the 2013 Westgate Mall attack. The finding showed that technology adoption improved information sharing among agencies, but weak inter-agency coordination and the chronic unreliability of the power supply reduced operational effectiveness. Kariuki (2020) also assessed the CCTV networks in Johannesburg and Cape Town, South Africa, and found improved response times but raised pointed questions about whether surveillance coverage was equitably distributed or concentrated in wealthier areas. These studies may be instructive, but Kenya and South Africa are different from Nigeria in institutional capacity, legal tradition, and the sheer scale and multiplicity of security challenges they face.

Nigeria Specific Literature

Nigeria-specific scholarship on ICT and security is comparatively limited. Oludare et al. (2015), Afrifa, Ishaya, and Lami (2016), and Oghorodi (2014) constitute the core of this literature. Their shared contribution is an advocacy case for deploying surveillance technologies, specifically CCTV, biometrics, and satellite monitoring. This is to address Nigeria's security challenges, and that case is made cogently. However, none of these studies evaluates whether deployments have yielded measurable outcomes, nor do they examine the governance barriers that have prevented or distorted them, nor do they situate the argument within a theoretical framework that would permit generalizable conclusions. Adams (2016) and Uchenna et al. (2018) added useful institutional detail on capacity gaps, but without the governance framing needed to move from description toward prescription. The existing literature has established the case for technology adoption, but has not assessed why adoption has stalled or what would be needed to make it work. Addressing that gap is the purpose of this study.

Nigerian Surveillance Policy and Legal Framework

Understanding Nigeria's surveillance technology governance requires examining the policy and legal landscape in which these technologies operate, as this landscape explains much of the fragmentation in deployment. Nigeria has some significant legislation. The Cybercrimes Act of 2015, as amended in 2024, is the most directly applicable instrument authorising certain forms of electronic surveillance and communication interruption by law enforcement agencies (Federal Republic of Nigeria, 2015). The Act is reasonably broad in scope but has attracted continuous criticism for its omissions. Data protection provisions are thin, judicial oversight mechanisms for surveillance authorisation are also underdeveloped, and the boundaries of lawful interception remain unclearly defined. These gaps have raised civil concerns and hindered full implementation (Okonkwo, 2018).

The Nigeria Data Protection Regulation (NDPR) of 2019, issued by the National Information Technology Development Agency (NITDA), was a step forward in data authority. However, it, too, fell short of what constitutes an effective surveillance lapse. It established responsibilities around data collection, processing, and storage, with clear implications for how biometric and identity management systems should work, yet has been criticised for

weak implementation instruments and the absence of a genuinely independent data protection authority with the mandate and resources to hold government surveillance actors to account (Eke, 2020).

The National Security Strategy of 2019 and the National Cybersecurity Policy and Strategy of 2021 acknowledged the importance of technology in security governance, calling for enhanced intelligence-gathering and information sharing. However, neither document translates these aspirations into binding obligations, funding commitments or deployment standards for security agencies. Taken together, these instruments represent governance intentions without governance architecture. This thereby overlaps with inadequately enforced provisions that fail to provide the legal and institutional foundation required for effective, sustained deployment of surveillance technology.

Theoretical Framework

This study adopts structural functionalism as its theoretical framework. Security governance theory, systems theory, and critical security studies were each considered but set aside. Governance theory is better suited to studies of multi-actor coordination. Systems theory, while analytically powerful, lacks the institutional specificity needed here. Critical security studies raise important questions about who defines security and in whose interest, but these fall outside this study's scope. This study focuses on institutional performance: why Nigeria's security institutions are failing to deploy available technologies effectively, and what a corrective would look like.

Structural functionalism, which derives from Parsons (1951), views society as a system of interconnected institutions, each with specific functions to maintain social stability and order. When institutions perform those functions, the system achieves equilibrium. When they fail due to dysfunction, under-resourcing, poor coordination, or corruption, the result is systemic breakdown (Gad, 2003). Within this study, the framework is operationalised along three interlinked dimensions.

First, Nigeria's security agencies, including the Nigeria Police Force, the Armed Forces, the Department of State Services, and various paramilitary bodies, are understood as institutional actors whose core societal function is to maintain public order and protect citizens. Their persistent failure to contain insecurity is treated not as an isolated administrative problem but as evidence of systemic dysfunction.

Second, the inadequate deployment of surveillance technologies is examined as both a symptom and a compounding cause of that dysfunction. It represents a failure mode that leaves security agencies operationally blind in environments where criminal actors operate with relative sophistication.

Third, surveillance technologies such as CCTV systems, biometric databases, facial recognition tools, predictive analytics, data mining, and satellite monitoring are analysed for their potential as stabilising mechanisms. If properly institutionalised, they can restore functional capacity to security agencies and contribute to systemic equilibrium. Where deployment gaps exist, dysfunction persists. Where technology is successfully institutionalised, institutional recovery becomes possible.

Methodology

This study employs qualitative document analysis, an approach established in security studies and the broader social sciences for studies whose evidence base consists of policy texts, institutional reports, and scholarly literature (Bowen, 2009). The study focuses on institutional governance: why Nigerian security agencies have failed to deploy surveillance technologies effectively, and what conditions would need to change. Examining the documentary record through which governance intentions, failures, and outcomes are recorded is appropriate for this purpose. No primary quantitative data were collected; all evidence derives from purposively selected secondary sources subjected to systematic thematic analysis.

Search Strategy and Document Identification

A systematic search of four electronic databases was conducted between March and July 2023, including Google Scholar, Scopus, JSTOR, and the African Journals Online (AJOL) repository. The following search strings were applied across all databases:

- "surveillance technology AND Nigeria";
- "ICT AND security governance AND Nigeria";
- "CCTV AND crime AND Africa";
- "biometric surveillance AND sub-Saharan Africa";
- "insecurity AND Nigeria AND technology";
- "predictive policing AND developing countries"; and lastly
- "structural functionalism AND security institutions"

Searches were done only in English-language sources published between 2005 and 2023. This temporal boundary was selected because it captures both the intensification of Nigeria's contemporary security crisis (marked by the emergence of Boko Haram around 2009) and the rapid worldwide expansion of digital surveillance tools and their governance frameworks over the same period. In addition to database searches, supplementary hand-searching was conducted of key journals, including the African Security Review, the Journal of Modern African Studies, and the International Journal of Computer Science Trends and Technology, as well as the reference lists of all retained sources (backward citation tracking). Official documents were sourced directly from Nigerian government repositories, the UNODC, ACLED, the Global Terrorism Index, and SIPRI.

Inclusion and Exclusion Criteria

The initial database searches returned a combined 214 potentially relevant sources. Following the removal of 38 duplicates, 176 unique sources were screened at the title and abstract level. Of these, 103 were excluded at this stage for the following reasons: the source addressed surveillance technologies in contexts with no analytical relevance to the Nigerian or sub-Saharan African setting (n = 41); the source focused on surveillance from a purely technical or engineering perspective without engaging the governance or social science dimensions (n = 29); the source predated the study's temporal boundary of 2005 (n = 18); or the source was not retrievable in full text (n = 15). The 73 remaining sources were then subjected to a

full-text review, from which 21 more were excluded because, upon closer reading, they did not adequately address the study's core subjects: surveillance technology utilisation, institutional governance capacity, or Nigeria's security architecture. A final total of 52 sources was therefore retained for analysis, supplemented by 11 official documents, including legislative texts, government policy papers, and international institutional reports, identified through targeted governmental and organisational searches. The total analytical corpus, therefore, comprised 63 documents.

Thematic Analysis and Coding Procedure

Thematic analysis followed a six-phase process outlined by Braun and Clarke (2006), which includes;

- Familiarisation with the data
- Generation of initial codes
- searching for themes
- Reviewing themes
- Defining and naming themes
- Producing the report.

In the familiarisation phase, all 63 documents were read in full, with preliminary annotations recorded. In the initial coding phase, open codes were applied to relevant passages using a combination of deductive codes derived from the structural functionalist framework (e.g., "institutional dysfunction", "functional deficit", "systemic equilibrium") and inductive codes emerging directly from the data (e.g., "power supply failure", "inter-agency mandate confusion", "budget asymmetry"). A total of 47 initial codes were generated. In the theme development phase, related codes were clustered into candidate themes, which were then reviewed for internal coherence and distinctiveness. Four main themes were identified as both analytically robust and directly significant to the study's research questions: (i) institutional capacity deficits, (ii) technology deployment barriers, (iii) legal and policy framework gaps and (iv) governance and accountability failures. These themes, once defined, were applied consistently across the entire corpus during a second reading to ensure their fit and completeness. Where a document contributed evidence relevant to more than one theme, it was then coded to all applicable themes. Analytical memos were maintained throughout this process to document interpretive decisions and trace the progression from data to theme to finding.

Reflexivity

Reflexivity in qualitative research requires transparency about the values, experiences, and positions the researchers bring to the interpretive process (Braun & Clarke, 2006; Bowen, 2009). All three authors are Nigerian-based sociologists with research and professional backgrounds in governance, security, and public policy. This provides contextual familiarity with the interagency dynamics of Nigerian security institutions and public-sector procurement, both of which inform document selection and interpretation. It also carries a risk of confirmation bias, which a researcher familiar with the governance failures of Nigerian security institutions may read evidence in ways that reinforce prior views. To

address this, the authors maintained analytical memos that documented instances in which evidence did not fit prevailing interpretations and resolved interpretive disagreements through team discussion. The structural functionalist framework served as an additional check, anchoring analysis in institutional function rather than political attribution.

Methodological Limitations

Three methodological limitations apply. First is the documentary analysis, which depends on the quality and completeness of available literature. Where deployments have failed to generate audit reports, journalistic or academic attention, this study cannot capture them. Documented failures are said to be better represented than undocumented ones. Secondly, without primary fieldwork, such as interviews with security agency personnel, procurement officials, or technology vendors, the study cannot capture the informal dynamics and personal incentives that often shape governance outcomes. Future research combining documentary analysis with key informant interviews would strengthen these findings. Thirdly, restricting the search to English-language sources may have excluded relevant scholarship from francophone West African contexts. These limitations define the study's scope. They do not undermine the validity of the analysis within it.

Findings

Thematic analysis of the documentary evidence, which is interpreted through the structural functionalist framework, produced three principal findings, each addressing a distinct dimension of Nigeria's surveillance technology governance failure.

The international evidence base is substantial, but Nigeria is not using it.

The international evidence that surveillance technologies can reduce insecurity is well established. Welsh and Farrington's (2009) systematic review recorded an average of 16% reduction in crime with the use of surveillance areas across 44 UK and US studies. Ratcliffe et al. (2019) reported about 20% reductions in violent crime from predictive policing pilots in Philadelphia. In Kenya and South Africa, despite implementation difficulties, both recorded measurable improvements in security agencies' responsiveness following investments in surveillance technology. For Nigeria, the relevant question is not whether these tools work but whether the institutional conditions required for effective deployment exist or can be created.

Nigeria's actual deployment is inadequate.

Nigeria's surveillance technology deployments fall well short of what effective security governance requires. Oghorodi (2014) documented approximately 700 CCTV cameras installed in Lagos under the Public Security Communications System, a figure that represents negligible coverage for a metropolitan area of over 20 million people, let alone a country of over 220 million people. The N30 billion National Identity Management System (NIMS) biometric database project, appropriated in the 2012 national budget, had still not delivered a functional national system year after its estimated completion date. This is a major failure, given how central identity verification is to modern crime investigation and counterterrorism. At the sub-national level, the Bayelsa State Safe City, Safe State initiative, contracted to Wawin Technology for N1.7 billion, was broadly welcomed as a proactive state-level response to rising crime in the Niger Delta. However, reported challenges, including an unstable power supply, limited technical capacity among local operating personnel, and the

absence of independently verified outcome data on crime reduction, have prevented a rigorous assessment of its effectiveness and raised questions about long-term sustainability (Adams, 2016; Oghorodi, 2014). Across these cases, a consistent pattern occurs: technology is procured, installed, and then inadequately maintained, operated, or appraised. The primary deficit is institutional rather than technological.

The Barriers are interconnected and mutually reinforcing.

At the institutional level, unclear interagency mandates and bureaucratic inertia mean that even when technology is procured, it is rarely integrated into coherent operational frameworks. At the technical level, Nigeria's chronic power supply deficits and the finding that fewer than 35 per cent of Army Signal Corps personnel can operate ICT tools without assistance (Oghorodi, 2014) point to a fundamental readiness gap. Financially, the gap between conventional military spending and technology-specific budget allocations is substantial; a country spending over US$3.5 billion annually on defence (SIPRI, 2023) has not ring-fenced meaningful resources for the surveillance and intelligence tools that could make that defence more effective. At the socio-political level, the pattern of announced projects, appropriated funds, and absent accountability suggests that political will, rather than the availability of money or technology, is the binding constraint.

Challenges to ICT Deployment for Security Governance in Nigeria

Several interconnected challenges impede the effective deployment of ICT for security governance in Nigeria. These fall into four categories: institutional challenges, including weak governance structures, unclear agency mandates, and bureaucratic inertia; technical challenges, arising from inadequate infrastructure, power supply deficits, and skills shortages; financial challenges, encompassing insufficient budgetary allocations and unsustainable funding models; and socio-political challenges, including corruption, limited political will, and the reluctance of successive governments to prioritise technology-led security reforms.

Low Level of ICT Skills among Security Personnel

The low level of ICT skills among security personnel constitutes a critical technical challenge. The International Telecommunication Union (ITU) ICT Development Index ranked Nigeria 122nd out of 155 economies in 2011, with a growth rate of just 0.18 per cent (Oghorodi, 2014). A comparative analysis across security agencies reveals the depth of the problem: in the Nigerian Army Signal Corps, only approximately 35 per cent of personnel could operate ICT tools without assistance (Oghorodi, 2014). The National Institute of Policy and Strategic Studies noted that fewer than 20 per cent of frontline police officers received any ICT-related training in the previous three years (Abubakar, 2005). Uchenna et al. (2018) report that digital competency among Nigerian Security and Civil Defence Corps (NSCDC) personnel is largely confined to basic computer literacy, with negligible capacity for operating advanced surveillance systems or performing data analytics.

Hardware is not the primary constraint; institutional capacity is. Deploying and sustaining surveillance tools requires human capital, governance structures, and training systems that are currently inadequate. Addressing these gaps requires standardised, mandatory ICT training curricula across all security agencies, inter-agency knowledge-sharing platforms, and sustained investment in digital literacy within the security sector.

Lack of Government Commitment

Nigeria's governance record shows persistent underinvestment in technology-led security solutions relative to conventional military expenditure. Military spending reached approximately US$3.5 billion in 2022 (SIPRI, 2023), yet allocations for ICT-based security infrastructure and surveillance technology remained marginal and poorly tracked. The pattern is consistent: despite N30 billion appropriated for NIMS in the 2012 national budget, the Commission did not deliver a functional biometric database within its projected timeline; the National Cybersecurity Policy, first drafted in 2014, was not formally enacted until 2021; and successive national security budgets have not earmarked dedicated funding for surveillance technology procurement, maintenance, or operator training. Nigeria has yet to establish a national surveillance technology oversight body responsible for setting deployment standards, auditing performance, and ensuring public accountability.

Infrastructure Deficits

Nigeria's severe infrastructure deficits, particularly persistent electricity supply shortfalls, make uninterrupted CCTV and digital surveillance operation difficult without substantial investment in alternative power systems (Adams, 2016). Maintenance costs represent a recurring challenge. Surveillance networks require continuous technical upkeep, software updates, and hardware replacement. These are commitments that have historically been neglected in Nigeria's public sector, as evidenced by the deteriorating condition of many installed cameras.

Corruption and Governance Challenges

Corruption within security institutions poses a systemic risk. The integrity of surveillance systems depends on the personnel who manage and review footage; without accountability mechanisms, even well-installed systems can cease to function as intended. Additional governance challenges compound these operational difficulties: unclear jurisdictional mandates between the Nigeria Police Force, the DSS, and state security agencies; the absence of a dedicated legal surveillance framework; and limited data protection provisions. None of these barriers rules out the deployment of surveillance. However, they do require that any national rollout be phased, carefully governed, and supported by clear institutional mandates, dedicated maintenance budgets, and credible anti-corruption safeguards.

Discussion

The findings show that Nigeria's failure to use surveillance technologies more effectively is primarily an institutional governance problem, not a technology access problem. Cameras are procured and installed, and biometric databases have been funded. Policy frameworks have also been drafted. What has failed is the institutional infrastructure needed to make these investments work, including adequate training, inter-agency coordination, maintenance budgets, and accountability mechanisms. Applied here is Parsons' (1951) structural functionalist framework, which identifies why, in a stable social system, institutions perform their designated roles in coordination with one another. Nigeria's security system is failing because coordination has broken down across multiple institutions simultaneously. The police, the military, the intelligence services, and the agencies responsible for this technology governance are each underperforming in ways that compound rather than compensate each other's weaknesses.

The pattern identified in Nigeria is not unique, but it is especially pronounced. The experiences of Kenya and South Africa documented by Amara (2016) and Kariuki (2020) show the same dynamic: technology deployed in institutional environments that are inadequately trained, insufficiently funded, and poorly governed does not deliver the expected security outcomes. Nigeria's situation differs in scale and complexity. Its security challenges are larger than those Kenya or South Africa faced in their surveillance technology initiatives. Governance deficits span multiple agencies simultaneously, making coordination correspondingly harder. The range of non-state armed actors, including Boko Haram, ISWAP, bandits, criminal kidnap networks, and secessionist movements, also requires a more comprehensive and adaptable surveillance architecture than any single state-level initiative has so far attempted.

The policy and legal framework analysis reinforces this diagnosis. Nigeria's existing legislative instruments, including the Cybercrimes Act, the NDPR, the National Security Strategy, and the National Cyber Security Policy, each have some merit but collectively fall short of what effective surveillance governance requires. There is no dedicated national surveillance technology framework. Inter-agency mandates remain contested. Enforcement of existing provisions is weak. No accountability exists with the mandate and resources to hold government surveillance actors to transparent performance standards.

Conclusion

This study assessed the role of modern surveillance technologies in tackling insecurity in Nigeria. International and African studies confirm that these technologies produce measurable security improvements when properly deployed, and Nigeria has access to many of them. Even as such, the country remains among the world's most terrorism affected nations, with over 5,000 conflict-related fatalities recorded in 2022 alone. The structural functionalist analysis was used to explain this gap; the problem lies not in technology but in the institutions responsible for deploying and sustaining it. Security agencies that cannot coordinate with one another, a legal framework that does not clearly authorise surveillance operations, budget allocations that favour hardware procurement over training and maintenance, and a political culture in which policy announcements routinely outpace implementation are the binding constraints. They are addressable, but only through a governance-centred response rather than a procurement-centred one.

Recommendations

The following recommendations are derived directly from the study's findings:

i. The government should establish a National Surveillance Technology Coordination Committee (NSTCC) under the National Security Adviser to audit existing infrastructures, harmonise agency mandates and also develop a National surveillance technology master plan.
ii. There should be a mandated standardised ICT competency training across Nigeria's Armed Forces with a curriculum developed in partnership with NITDA, to ensure that fewer than 35 per cent of Signal Corps personnel can operate the tools.
iii. Complete and activate the NIMS biometric database with transparent procurement processes and independent auditing, addressing the long-standing N30 billion implementation failure.
iv. Enact a National Surveillance and Data Protection Act to fill the regulatory void identified in this study.

v. Implement a phased, nationally coordinated CCTV deployment program with mandatory power backup systems and built-in independent performance evaluation mechanisms.
vi. Develop inter-agency data-sharing platforms connecting police, military, DSS, and immigration systems.
vii. Ring-fence a minimum of 15 per cent of the national security budget for ICT security infrastructure.
viii. Pilot predictive policing systems in Lagos, Abuja, and Kano with independent ethical oversight and public accountability mechanisms.

Longer Term recommendation (5 Years plus)

i. Invest in indigenous surveillance technology research through a dedicated national centre of excellence.
ii. Develop a STEM security track in military and police academies to build a sustainable talent pipeline.
iii. Centralise biometric and criminal databases under the NSTCC with robust data protection controls.
iv. Pursue a regional surveillance cooperation framework with Chad, Cameroon, Niger, and Benin to address the cross-border dimensions of terrorism and organised crime.
v. Institutionalise continuous ICT retraining as a mandatory annual obligation across all security agencies.

References

Abdulkabir, O. S. (2017). Causes and incisive solutions to the widespread kidnapping in Nigeria's current administration: Under scholarly scrutiny. Journal of Political Science & Public Affairs: 5, 258. https://doi.org/10.4172/2332-0761.1000258

Abubakar, A. (2005). The challenges of security in Nigeria: Paper presented at the Public Lecture Organised by the National Institute for Policy and Strategic Studies (NIPSS), Kuru, Jos.

ACLED (Armed Conflict Location and Event Data Project): (2023). Nigeria: Conflict data overview 2022. ACLED, https://acleddata.com

Adams, O. K. (2016). The role of information technology in national security: A case study of Nigeria. Global Journal of Computer Science and Technology, 16(3), 6–14.

Afrifa, J., Ishaya, B., & Lami, D. S. (2016). The role of information and communication technology (ICT) and early warning systems in school security in North-Eastern Nigeria. International Journal of Scientific and Research Publications, 6(10), 55–59.

Ajibola, O. (2012). The role of ICT deployment for national security: In ICT and Security Studies (Vol. 1, pp. 39–55). Nigerian Defence Academy Press

Amara, J. (2016). Technology and security sector reform in Africa: Lessons from Kenya's biometric surveillance initiative. African Security Review, 25(3), 210–228.

Bowen, G. A. (2009). Document analysis as a qualitative research method: Qualitative Research Journal, 9(2), 27–40.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology: Qualitative Research in Psychology: 3(2), 77–101.

Chainey, S., & Ratcliffe, J. (2005). GIS and crime mapping: John Wiley & Sons

Eke, C. (2020). Data protection in Nigeria: Assessing the NDPR and its enforcement gaps. Journal of Information Law and Technology, 12(1), 45–62.

Ezemenaka, K. E. (2018). Kidnapping: A security challenge in Nigeria Journal of Security and Sustainability Issues: 8(2), 233–246.

Federal Republic of Nigeria (2015), Cybercrimes (Prohibition, Prevention, Etc. Act, 2015 (as amended 2024). Federal Government of Nigeria Official Gazette

Gad, B. (2003). Communities and law: Politics and cultures of legal identities. University of Michigan Press

Global Terrorism Index, 2023 Global Terrorism Index (2023): Institute for Economics and Peace.

Hobbes, T.(1951). Leviathan, Andrew Crooke.

Kariuki, M. (2020). CCTV surveillance and urban security governance in Johannesburg and Cape Town: An assessment. South African Journal of Criminal Justice, 33(2), 178–196.

Krahmann, E. (2003). Conceptualising security governance: Cooperation and Conflict: Journal of the Nordic International Studies Association, 38(1), 5–26.

Locke, J. (1689). Two treatises of government: Awnsham Churchill.

Lyon, D. (2007). Surveillance studies: An overview. Polity Press

Nwagboso, C. I. (2016). The nature of internal security problems in African states: The Nigerian experience. International Journal of Academic Research in Business and Social Sciences, 6(4), 38–71.

Nwanegbo, C. J., & Odigbo, J. (2013). Security and national development in Nigeria: The threat of Boko Haram. International Journal of Humanities and Social Science, 3(4), 285–291.

Odeh, A. M., & Umoh, N. (2015). State policing and national security in Nigeria. Mediterranean Journal of Social Sciences, 6(1), 412–422.

Oghorodi, D. U. (2014). Deployment of information and communication technology tools to combat national insecurity in Nigeria. International Journal of Computer Science Trends and Technology (IJCST), 2(4), 142–147.

Okauru, A. B. (2012). Information communication technology and national security in Nigeria: Punch Newspaper, 28 July 2013. Retrieved April 8, 2020, from http://www.punchng.com/business/ict-clinic/security-challengeswhat-can-ict-do

Okonkwo, U. (2018). Cybercrime legislation and civil liberties in Nigeria: An appraisal of the Cybercrimes Act 2015. Journal of African Law, 62(2), 311–336.

Oludare, A. I., Omolara, E. O., Umar, A. M., & Kemi, D. V. (2015). The use of ICT tools in tackling insecurity and terrorism in Nigeria. Network and Complex Systems, 5(5), 21–29.

Parsons, T. (1951). The social system: Free Press

Ratcliffe, J., Groff, E., Haberman, C., & Taniguchi, T.(2019). A randomised controlled trial of a hot spots policing intervention in Philadelphia: Translating theory into empirical test. Journal of Experimental Criminology, 15(3), 1–26.

SIPRI (Stockholm International Peace Research Institute). (2023). SIPRI Military Expenditure Database 2023: SIPRI. https://www.sipri.org/databases/milex

Stan, F. (2004). The security–development nexus: Conflict, peace and development in the 21st century. International Peace Academy

Uchenna, C. P., Chukwuemeka, O., & Chukwuka, O. (2018). The impact of ICT on national security: A case of the Nigerian Security and Civil Defence Corps. International and Public Affairs, 2(3), 48–61.

UNDP (United Nations Development Program) (1994). Human Development Report 1994: New dimensions of human security. Oxford University Press

UNODC (United Nations Office on Drugs and Crime), (2021): The use of the internet for terrorist purposes: Updated guidance. United Nations

Welsh, B. C., & Farrington, D. P. (2009). Public area CCTV and crime prevention: An updated systematic review and meta-analysis. Justice Quarterly, 26(4), 716–745.

Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. Public Affairs

Zureik, E., & Salter, M. B. (Eds.). (2013). Global surveillance and policing: Borders, security, identity. Willan Publisher