
POLITICAL ECONOMY OF DIGITAL IDENTITY SYSTEMS AND NATIONAL SECURITY GOVERNANCE IN NIGERIA

Mark, Kingsley Chinonso, PhD

Department of Political Science, Faculty of Social Sciences,
Nnamdi Azikiwe University Awka,
Anambra State-Nigeria

Patrick Onochie Nezianya

Department of Political Science, Faculty of Social Sciences,
Nnamdi Azikiwe University Awka,
Anambra State-Nigeria

Abstract

Over the past decade, digital identity systems have become central instruments of governance in developing countries, promoted by international institutions as tools for financial inclusion, service delivery, and national security. Nigeria's National Identification Number (NIN) programme, backed by over \$430 million in World Bank financing, represents one of Africa's most ambitious biometric identity projects, enrolling over 121 million citizens by June 2025 and enforcing mandatory NIN-SIM card linkage across the study period. Despite this substantial infrastructure expansion, national security outcomes remained poor during the same period. Kidnapping for ransom and armed banditry intensified, with independent monitoring organizations documenting thousands of victims during peak enforcement. Existing scholarship has not adequately examined why expanded state capacity for citizen data collection failed to translate into improved security governance, nor has it applied an integrated political economy framework to analyze the distributional and institutional dimensions of Nigeria's digital identity project. This study investigates the political economy of Nigeria's digital identity expansion, examining how resource allocation decisions, institutional incentives, bureaucratic competition, and elite interests shaped both implementation and outcomes between 2019 and 2025. The study employs a descriptive research design, drawing on systematic content analysis of government policy documents, World Bank project reports, security incident data from independent monitoring organizations, and digital rights publications. Michael Mann's theory of infrastructural power and the Political Economy Approach provide the analytical framework. While Nigeria expanded digital identity infrastructure, achieving enhanced data collection capacity as one dimension of infrastructural power, this expansion did not produce corresponding improvements in institutional coordination or operational effectiveness. Security agencies gained unprecedented surveillance capacity but lacked training, inter-agency cooperation, and analytical infrastructure to convert data into actionable intelligence. Implementation served the interests of technology vendors, state agencies, and political elites more than citizens, producing systematic exclusion among rural and marginalized populations. Nigeria's digital identity project exemplifies isomorphic mimicry, building the outward form of modern state capacity without developing its substance. Genuine security improvement requires institutional reform, anti-corruption measures, and coordinated governance, not technological investment alone. These findings have significant implications for digital identity policy across sub-Saharan Africa.

Keywords: Digital Identity Systems, Security, Surveillance, National Security, Governance

Introduction

Over the past two decades, digital identity systems have become central tools for modern governance. Governments worldwide have adopted biometric technologies including fingerprints, facial recognition, and iris scans, to create unique digital records for their populations. International development institutions have been key drivers of this trend. The World Bank, through its Identification for Development (ID4D) initiative, has promoted digital identity as essential for achieving Sustainable Development Goal 16.9, which calls for legal identity for all by 2030 (World Bank, 2016). The institution argues that robust identification systems can improve access to services, enhance financial inclusion, and strengthen state capacity to deliver public goods (Gelb and Clark, 2013).

However, the rapid expansion of digital identity systems has also raised significant concerns. Scholars such as Lyon (2018) argue that these systems represent a fundamental transformation in state-citizen relations, turning individuals into “data subjects” whose every interaction becomes a potential point of surveillance. In contexts where democratic institutions are fragile, digital identity can become an instrument of control rather than empowerment (Jacobsen, 2021). Breckenridge (2014), in his study of South Africa’s biometric state, demonstrates how identification systems originally designed for administrative purposes can be repurposed for surveillance and political control, particularly affecting marginalized populations. African governments have been particularly enthusiastic adopters of digital identity systems, often with substantial support from international donors. Countries including Kenya, Ghana, and Uganda have implemented national biometric identification programs over the past decade (Manby, 2018). These initiatives are typically justified through twin objectives: improving service delivery and enhancing national security (Donovan and Park, 2019).

Nigeria presents a particularly complex case for understanding digital identity and security governance. With a population exceeding 200 million and significant ethnic, religious, and regional diversity, the Nigerian state has historically struggled with what Scott (1998) describes as “legibility,” the administrative capacity to see, categorize, and govern its population effectively. Before 2019, Nigeria’s identity management was highly fragmented. The National Population Commission handled birth registration and census activities, the Central Bank of Nigeria managed the Bank Verification Number (BVN) for banking customers, the Independent National Electoral Commission maintained voter registration databases, and various agencies issued travel documents and professional licenses (Eke, 2020). This fragmentation created inefficiencies, enabled fraud, and limited the government’s capacity to deliver services or enforce policies consistently.

Simultaneously, Nigeria has faced severe and multifaceted security challenges. The Boko Haram insurgency in the Northeast, which began in 2009, has killed tens of thousands and displaced millions (Zenn, 2020). Kidnapping for ransom has become increasingly common across multiple regions, affecting students, travelers, and entire communities (Campbell and McCaslin, 2018). Armed banditry in the Northwest has disrupted agriculture and forced thousands from their homes (International Crisis Group, 2020). These security threats impose enormous economic costs and undermine state legitimacy. In 2019, the Nigerian government launched a comprehensive National Security Strategy that identified the harmonization of identity databases as a strategic priority (Office of the National Security Adviser, 2019). The strategy explicitly framed digital identity as a critical infrastructure for intelligence gathering, border control, and counter-terrorism operations. This policy vision was operationalized through aggressive enforcement of the National Identification Number (NIN) and the

mandatory NIN-SIM linkage policy. Beginning in December 2020, the Nigerian Communications Commission required all telecommunications subscribers to link their Subscriber Identity Module (SIM) cards to their NIN, with the explicit goal of enabling security agencies to track criminals who use mobile phones to coordinate kidnappings and other crimes (Nigerian Communications Commission, 2020). The policy was enforced through the disconnection of unlinked phone lines, affecting millions of Nigerians.

The World Bank provided substantial financial and technical support through its ID4D project, committing \$430 million officially designated for development objectives, including financial inclusion, service delivery improvement, and poverty reduction, to help Nigeria achieve 148 million NIN enrolments by June 2024 (World Bank, 2020). Nigeria failed to meet this target, prompting the World Bank to extend the project deadline to December 2026 and revise the enrolment target upward to 180 million (Biometric Update, 2024). This World Bank investment created a significant tension within Nigeria's digital identity project. While international donor funding was officially justified through development objectives aligned with Sustainable Development Goals, the Nigerian government's implementation and enforcement during 2019-2025 increasingly emphasized security rationales. Despite the successful expansion of the NIN-SIM linkage policy and the enrolment of over 121 million citizens in the biometric database by June 2025 (NIMC, 2025), Nigeria's security situation has not improved as anticipated. Kidnapping for ransom has intensified rather than diminished. SBM Intelligence (2025) documented 4,722 kidnapping victims across 997 incidents between July 2024 and June 2025, with at least 762 people killed, representing a significant escalation beyond the figures recorded during earlier enforcement years. Armed groups in the Northwest and Northeast have maintained their operational capacity, continuing to launch attacks, control territory, and extract resources from local populations (International Crisis Group, 2020).

This persistence of insecurity despite expanded digital identity infrastructure reveals a fundamental disconnect between technological capacity and governance outcomes. The Nigerian state has achieved unprecedented ability to collect and store citizen data, yet this capacity has not translated into the expected improvements in security provision. Security agencies possess extensive biometric databases and telecommunications data, but these resources appear to contribute little to preventing crimes or apprehending criminals. Moreover, the implementation of mandatory digital identity requirements has created new challenges. Millions of Nigerians, particularly in rural areas and among marginalized populations, face barriers to obtaining NINs due to distance from enrollment centers, lack of prerequisite documentation, and cost constraints (Paradigm Initiative, 2021). The enforcement of NIN-SIM linkage has resulted in service disconnections that disrupt livelihoods and cut people off from essential communications. Meanwhile, concerns have emerged about surveillance overreach, with digital rights organizations documenting instances where digital identity infrastructure has allegedly been used to target political opponents and civil society activists (Paradigm Initiative, 2022).

This study addresses this gap by examining Nigeria's digital identity project through an explicitly political economy lens, analyzing how resource allocation decisions, institutional incentives, bureaucratic competition, and distributional politics have shaped both the implementation and the limited effectiveness of digital identity systems for security governance. Employing the descriptive research design content analytical tool to provide empirical evidence on the relationship between digital infrastructure investment and actual security governance outcomes in Nigeria.

Operational Definitions

Digital Identity System:

Technological framework that uses biometric data (fingerprints, facial recognition, iris scans) and demographic information to create unique, verifiable digital records for individuals, managed through centralized databases and accessible to authorized government agencies (Gelb and Metz, 2018). In Nigeria's context, this specifically refers to the National Identity Management System administered by NIMC.

National Security Governance:

The institutional structures, legal frameworks, policy processes, and operational mechanisms through which the state identifies threats, allocates resources, coordinates agencies, and implements security measures to protect sovereignty, territorial integrity, and citizen safety (Omand, 2010). This encompasses both the formal architecture of security institutions and the actual practices of security provision.

Infrastructural Power:

As conceptualized by Mann (1984), the capacity of the state to penetrate civil society and implement political decisions throughout its territory through administrative, logistical, and technological means, rather than through coercive force alone. This concept emphasizes the state's reach and coordination capacity rather than its repressive capabilities.

Political Economy:

The study of how political institutions, power relations, and policy decisions interact with economic structures, resource allocation, and distributional outcomes (North, 1990). In this research, political economy analysis examines who benefits from digital identity investment, how institutional incentives shape implementation, and what consequences result for different social groups.

NIN-SIM Linkage:

The mandatory policy requiring all telecommunications subscribers in Nigeria to register their National Identification Number with mobile network operators and link it to their SIM cards, enforced through threats of service disconnection, with the stated purpose of enabling security agencies to identify phone users (Nigerian Communications Commission, 2020).

State Capacity:

The ability of government institutions to effectively implement policies, provide public goods including security, extract resources through taxation, and maintain authority throughout their territory (Besley and Persson, 2011). State capacity has multiple dimensions including administrative, fiscal, and coercive capacity.

Surveillance:

The systematic monitoring, collection, storage, and analysis of citizens' communications, movements, transactions, and personal data by government agencies, typically justified through national security or law enforcement objectives but potentially affecting privacy rights and civil liberties (Lyon, 2018).

Digital Exclusion:

The condition whereby individuals or groups are unable to access essential services, economic opportunities, or exercise their rights due to lack of digital identity documentation, often resulting from barriers including geographic distance from registration centers, lack of

prerequisite documentation, cost constraints, or technological infrastructure deficits (Donovan and Park, 2019).

Review of Related Literature

Digital Identity and State Capacity in Developing Countries

The relationship between digital identity systems and state capacity has emerged as a major theme in development studies and political economy scholarship. Gelb and Clark (2013) argue that robust identification systems are foundational for effective governance, enabling states to deliver targeted services, reduce leakages in social programs, and improve revenue collection. Their analysis of identification systems across multiple countries suggests that successful digital identity projects can significantly enhance state administrative capacity and development outcomes.

However, this optimistic view has been challenged by scholars who emphasize implementation challenges and unintended consequences. Szreter (2007) demonstrates historically that civil registration systems often failed to achieve their stated objectives due to weak state capacity, resistance from populations wary of taxation and conscription, and competing institutional interests. Similarly, Pritchett, Woolcock, and Andrews (2013) argue that development interventions in weak governance environments frequently produce “isomorphic mimicry,” the appearance of institutional reform without substantive capacity improvement. Their framework suggests that digital identity systems may expand bureaucratic infrastructure while failing to address underlying governance challenges. Breckenridge (2014), in his study of South Africa’s biometric state, shows how identification systems originally designed for apartheid-era population control were repurposed in democratic South Africa, but continued to reflect and reinforce social inequalities. Manby (2018) examines identification and citizenship in Africa more broadly, highlighting how digital identity systems intersect with contested questions of belonging, citizenship rights, and access to resources. Her work emphasizes that technical identification systems cannot resolve fundamentally political questions about who belongs to the nation and who deserves state protection.

Donovan and Park (2019) introduce the concept of “perpetual debt” in their study of mobile money and digital identity in Kenya, arguing that digital financial inclusion creates new forms of indebtedness and vulnerability rather than straightforward empowerment. Their political economy analysis reveals how digital systems promoted as development interventions may primarily serve commercial and state surveillance interests rather than citizen welfare.

Surveillance, Security, and Digital Technologies

The securitization of digital identity systems raises important questions examined in surveillance studies scholarship. Lyon (2018) argues that modern societies have become “surveillance societies” where data collection pervades everyday life, fundamentally altering the relationship between individuals and both state and corporate actors. His work emphasizes that surveillance is not merely about security provision but constitutes a form of social ordering that distributes power unequally, with vulnerable populations experiencing disproportionate monitoring and control.

Zuboff (2019) extends this analysis through her concept of “surveillance capitalism,” demonstrating how data extraction has become central to contemporary economic systems. While her focus is primarily on corporate surveillance, the framework illuminates how

governments and technology companies share interests in expanding data collection infrastructure, creating convergence between commercial profit motives and state control objectives. In the African context, Magnet (2011) examines how biometric technologies are deployed in ways that reinforce racial and economic inequalities, subjecting marginalized populations to intensive monitoring while privileged groups experience less intrusive identification systems. Jacobsen (2021) analyzes the “rush to register” refugees and displaced populations through biometric systems, arguing that humanitarian claims about improving service delivery often mask surveillance and control objectives that serve state and international organization interests more than those of affected populations. The relationship between surveillance and security effectiveness remains contested. Hosein and Whitley (2002) examine identity cards and surveillance in the United Kingdom, finding that expanded identification requirements and monitoring capacity produced limited security benefits while imposing substantial costs on civil liberties and creating new vulnerabilities through centralized data systems. Their analysis questions the assumption that more identification automatically yields better security outcomes.

Political Economy of Technology and Development

Understanding digital identity requires examining the political economy of technology adoption in developing countries. Unsworth (2015) provides a framework for analyzing the political economy of development projects, emphasizing the importance of institutional incentives, power relations among stakeholders, and how official objectives may diverge from actual implementation driven by rent-seeking and bureaucratic interests. In technology specifically, Wade (2002) demonstrates how technology transfer in developing countries often serves the interests of technology vendors and domestic elites more than developmental objectives. His analysis highlights asymmetric power relations between international technology providers and recipient countries, with developing states often adopting expensive systems that generate limited local benefit while enriching foreign contractors. Gelb and Metz (2018) examine the political economy of identification systems in Africa, noting that substantial donor funding creates particular incentive structures. They observe that when international organizations finance digital identity projects, implementing agencies may prioritize meeting donor-defined metrics (such as enrollment numbers) rather than achieving operational outcomes (such as improved service delivery or security). This principal-agent dynamic helps explain gaps between stated objectives and actual results. Khan (2010) provides theoretical grounding for understanding how political settlements shape institutional development. His framework suggests that state capacity emerges not from technical interventions alone but from underlying political agreements about how power and resources are distributed. Applied to digital identity, this implies that technological infrastructure cannot compensate for absence of political will or coordination among competing power centers.

Digital Rights, Exclusion, and Inequality

Critical scholarship has increasingly examined how mandatory digital identity systems affect rights, inclusion, and inequality. Madianou (2019) introduces the concept of “technocolonialism” to describe how digital technologies promoted by Western institutions may reproduce colonial patterns in their design, implementation, and effects, often prioritizing control and data extraction over genuine empowerment of populations in the Global South.

Research on digital exclusion reveals systematic patterns. Taylor (2016) documents how biometric identification requirements disproportionately exclude women, minorities, and

economically marginalized populations who lack prerequisite documentation or face cultural barriers to registration. Masiero (2018), studying India's Aadhaar biometric identification system, shows that mandatory identity requirements create new gatekeepers and exclusion mechanisms, with technical failures and enrollment barriers preventing vulnerable populations from accessing essential services and benefits they are legally entitled to receive. Eubanks (2018) examines digital technologies in social policy more broadly, arguing that automated systems often deepen poverty and inequality by subjecting poor populations to intensive surveillance and algorithmic decision-making while affluent populations experience more discretionary, less intrusive services. Her framework is relevant for understanding how Nigeria's mandatory NIN requirements may affect different socioeconomic groups differently.

Empirical Review

Digital Identity Implementation in Africa

Several empirical studies examine digital identity systems in African contexts, providing comparative insights relevant to Nigeria. Kenya's Huduma Namba system offers important parallels. Gelb and Diofasi (2016) analyze Kenya's earlier implementation of biometric identification for SIM card registration, finding that while enrollment was successful, the system produced limited security improvements and created significant exclusion problems for nomadic populations and urban poor residents. Their findings suggest that technological implementation success does not automatically translate to governance outcomes.

Ghana's National Identification Authority implementation has been examined by Manby (2018), who documents persistent challenges in achieving universal enrollment despite substantial investment, with rural populations and marginalized ethnic groups remaining disproportionately excluded. The Ghanaian case illustrates institutional coordination difficulties when multiple agencies claim authority over aspects of identification policy. Uganda's mandatory SIM card registration program provides a direct parallel to Nigeria's NIN-SIM linkage. Donovan (2012) analyzed Uganda's implementation, finding that while the stated objective was combating terrorism and crime, actual effects included enabling government surveillance of opposition figures and creating new corruption opportunities in the registration process, while producing no measurable improvements in security outcomes. This empirical precedent is directly relevant to evaluating Nigeria's similar policy.

Nigeria's Digital Identity and Security Outcomes

Empirical research specifically examining Nigeria's digital identity project remains limited, creating the research gap this study addresses. Eke (2020) provides a technical description of Nigeria's digital identification management program but does not engage deeply with political economy analysis or security outcomes. His work documents implementation progress but offers a limited critical assessment of effectiveness or distributional consequences. Eyikorogha and Chigozie (2021) examine NIMC's performance, identifying institutional challenges including inadequate funding, infrastructure deficits, and coordination failures with other government agencies. However, their analysis remains primarily descriptive without a systematic political economy framework. On security outcomes specifically, empirical evidence comes primarily from independent monitoring organizations. SBM Intelligence (2022) provides systematic tracking of kidnapping incidents in Nigeria, documenting over 3,400 kidnapping victims between July 2021 and June 2022, the period of active NIN-SIM linkage enforcement. Their data reveals that kidnapping has intensified in several regions despite the identification requirements, directly contradicting the policy's stated security objectives. International Crisis Group (2020) similarly documents the

continued expansion of armed banditry in Northwest Nigeria throughout the period when digital identity infrastructure was being built and enforced.

Surveillance, Rights, and Exclusion in Nigeria

Empirical research on digital rights in Nigeria provides important evidence on surveillance and exclusion dimensions. Paradigm Initiative (2021, 2022), Nigeria's leading digital rights organization, has documented multiple concerns through its annual LONDA reports. Their 2021 report identifies significant barriers to NIN enrollment, including geographic distance from enrollment centers, cost burdens, and bureaucratic obstacles that disproportionately affect rural populations and women in northern Nigeria. Their 2022 report documents instances of alleged surveillance overreach, including claims that digital identity infrastructure has been used to track journalists, monitor activists, and target political opponents. While these allegations are difficult to verify independently, given the classified nature of surveillance operations, the pattern of reports raises concerns about accountability mechanisms for how digital identity data is accessed and utilized by security agencies.

Iwuoha and Doevenspeck (2021) provide a critical empirical analysis of what they term "biometric coloniality" in Nigeria and other African states. Their research examines how biometric identification systems reflect and reproduce power asymmetries, serving elite interests in control and surveillance rather than genuinely empowering citizens. They document patterns whereby digital identity implementation prioritizes enrollment speed and donor metrics over ensuring universal access or protecting citizen rights. On exclusion specifically, anecdotal evidence reported in Nigerian media throughout 2021-2022 documented widespread service disruptions when millions of SIM cards were disconnected for failure to complete NIN linkage. While comprehensive quantitative data on economic impacts remains unavailable, journalistic investigations documented cases of market traders losing customer contact, rural residents being cut off from families, and low-income workers unable to access mobile banking services due to disconnection (Premium Times, 2021; The Guardian Nigeria, 2021).

Political Economy of Digital Identity in Nigeria

The political economy dimensions of Nigeria's digital identity project remain significantly underexplored in existing empirical literature. Limited research examines resource flows, beneficiaries, or institutional incentives driving implementation. World Bank (2020, 2023) implementation status reports on the ID4D project provide official accounts of spending and progress, documenting the \$430 million commitment and enrollment achievements. However, these reports do not provide a critical analysis of contract allocations, technology vendor selection processes, or an assessment of whether resources were deployed efficiently. Detailed information about which companies received major contracts, their profit margins, and their connections to political elites remains largely unavailable in public documentation.

On institutional dynamics, fragmented evidence suggests coordination challenges among Nigerian agencies. Nigeria's 2019 National Security Strategy acknowledges that multiple agencies maintain separate databases with limited interoperability, but does not examine the political economy reasons why agencies resist integration or sharing of resources and authority (Office of the National Security Adviser, 2019). This empirical gap, the absence of systematic political economy analysis examining resource allocation, beneficiaries, institutional incentives, and distributional consequences, represents the core contribution this study will make. By analyzing available evidence on investments, security outcomes, exclusion patterns, and institutional behavior through an integrated political economy

framework, this research provides a needed empirical assessment of how and why Nigeria's digital identity project has produced the outcomes observed between 2019 and 2025.

Methodology

This study adopts a descriptive research design, which is appropriate for investigating complex governance phenomena where the objective is systematic description and analysis of patterns, relationships, and institutional behaviour rather than experimental manipulation. The design allows for rigorous examination of how digital identity systems have functioned within Nigeria's political economy context between 2019 and 2025, a period encompassing the active enforcement of the National Identification Number programme and the mandatory NIN-SIM linkage policy.

Data for this study were generated entirely from secondary sources. Primary documentary sources include Nigeria's National Security Strategy (2019), Nigerian Communications Commission guidelines on the NIN-SIM linkage policy, National Identity Management Commission enrolment statistics, and World Bank project appraisal and implementation status reports for the Nigeria Digital Identification for Development (ID4D) Project. These official documents provide the formal policy record against which implementation outcomes are evaluated.

Secondary analytical sources include security incident data from SBM Intelligence and the International Crisis Group, digital rights monitoring reports from Paradigm Initiative's annual LONDA series, peer-reviewed scholarship on digital identity, surveillance, and state capacity in Africa, and investigative journalism from Nigerian outlets including Premium Times and The Guardian Nigeria. These sources provide independent empirical evidence on security outcomes, exclusion patterns, and institutional behaviour that official documents alone cannot supply.

The analytical method is qualitative content analysis, applied within the dual theoretical framework of Michael Mann's infrastructural power theory and the Political Economy Approach. Content analysis was employed to identify, categorise, and interpret patterns across the documentary record, particularly the relationships among stated policy objectives, resource allocation decisions, implementation outcomes, and distributional consequences. This approach is consistent with established practice in qualitative political economy research examining governance institutions in developing country contexts (Unsworth, 2015; Khan, 2010). The study does not make causal claims beyond what the available evidence supports; rather, it offers a theoretically grounded analytical interpretation of observed patterns across the 2019-2025 period.

Theoretical Framework

This study employs Michael Mann's Theory of infrastructural power, propounded in 1984, "*The Autonomous Power of the State*," as its analytical framework, supplemented by the Political Economy Approach.

Mann's Theory of Infrastructural Power

According to Michael Mann (1984), Infrastructural power refers to the institutional capacity of the state to penetrate civil society and logistically implement political decisions throughout its territory. Michael Mann (1984, 1993) argues that infrastructural power operates through what he calls the "logistics of control," which is the administrative systems, information

networks, communication infrastructure, and coordination mechanisms that enable states to make their populations legible and governable.

According to Mann (1993), modern effective states rely less on despotic capacity and more on infrastructural power. This form of power depends on administrative penetration (the ability to reach all parts of the territory and population), information systems (mechanisms for collecting, storing, and analyzing data about the population), coordination capacity (the ability to synchronize actions across different agencies and geographic spaces), and logistical implementation (the capability to turn decisions into actions consistently). Mann's framework is particularly valuable for analyzing Nigeria's digital identity systems for several reasons.

First, it helps explain what the state is attempting to achieve. Nigeria's National Identification Number, Bank Verification Number, and NIN-SIM linkage policy can be understood as efforts to build infrastructural power, to make the Nigerian population more visible and governable, to extend state administrative reach into domains (like mobile telecommunications) where anonymity previously prevailed, and to create the informational foundation for coordinated governance.

Second, Mann's theory illuminates the challenges of implementation. Infrastructural power requires more than just technology or data collection. It demands well-functioning institutions capable of coordinating with each other, trained personnel able to analyze and act on information, standardized procedures for accessing and utilizing data, and sustained political commitment to make the systems work operationally. Mann (1993) emphasizes that infrastructural power is built through decades of institutional development, not through rapid technology adoption alone.

Third, the framework helps analyze the gap between capacity and outcomes. A state can possess extensive surveillance and data collection infrastructure without having genuine infrastructural power if it lacks the institutional coordination and operational capacity to convert information into effective governance. In Nigeria's case, Mann's theory predicts that simply building biometric databases will not automatically improve security governance unless complementary institutional development occurs.

Political Economy Approach

The Political Economy Approach, as associated with the foundational work of Gilpin (1970), examines how political factors shape economic outcomes. In this context, the approach examines how resources, interests, and power relations shape digital identity implementation and effectiveness. Besley and Persson (2011), argued that state capacity emerges not merely from technical infrastructure but from political settlements that determine which institutions receive resources and whose interests they serve. As such, digital identity projects involve substantial resource flows. In Nigeria, for instance, over \$430 million in funding from government budgets and donor agencies. Khan (2010) argues that in developing country contexts, institutional design often reflects political settlements among powerful groups rather than optimal governance arrangements. Applied to digital identity, this suggests that how systems are structured, which agencies control data, what access protocols exist, and how coordination is organized may reflect bureaucratic competition and power relations rather than rational security planning. The political economy approach examines not just aggregate outcomes but distributive consequences like who benefits and who bears costs. Digital identity systems create winners (technology vendors who profit from equipment and services contracts, state agencies that gain expanded budgets, authority, and surveillance capacity, political elites who control procurement and resource allocation, and citizens with

education and resources to navigate enrollment easily) and losers (rural populations distant from enrollment centers bearing travel costs and time burdens, marginalized groups lacking prerequisite documentation, those excluded from services due to non-enrollment, and populations subjected to surveillance risks without corresponding security benefits).

Together, infrastructural power and political economy provide complementary analytical lenses. Infrastructural power explains what digital identity systems are meant to build and what institutional capabilities effective governance requires. Political economy explains why implementation often diverges from intentions, whose interests shape how systems function, and what distributional consequences result. The synthesis predicts that digital identity will expand state surveillance capacity (one dimension of infrastructural power) without necessarily improving security governance if institutional coordination remains weak, bureaucratic incentives reward resource capture over operational effectiveness, political settlements do not prioritize genuine security provision, and implementation serves elite interests more than public welfare.

Political Economy of the Digital Identification System and National Security in Nigeria

Nigeria's digital identity project was characterized by a fundamental misalignment between the rationale for international funding and the justification for domestic implementation. The World Bank's \$430 million ID4D investment was officially designated for development objectives aligned with Sustainable Development Goal 16.9, specifically financial inclusion, improved service delivery, and poverty reduction (World Bank, 2020). The project established targets for enrolling 148 million Nigerians by 2024, with success measured through quantifiable outputs such as enrollment coverage and system interoperability.

However, the Nigerian government's implementation and enforcement of digital identity systems were increasingly justified through security imperatives rather than development objectives. The 2019 National Security Strategy explicitly identified the harmonization of identity databases as a strategic national security priority, framing digital identity as critical infrastructure for intelligence gathering, border control, and counter-terrorism operations (Office of the National Security Adviser, 2019). Government officials repeatedly presented the mandatory NIN-SIM linkage policy, which required all telecommunications subscribers to link their phone numbers to their National Identification Number, as essential for combating kidnapping and insurgency.

This dual narrative created space for what can be characterized as strategic ambiguity in implementation. When questioned by international development partners about progress toward development objectives, implementing agencies could point to enrollment statistics showing over 100 million NINs issued by mid-2024. When questioned by domestic constituencies about persistent insecurity, the same agencies could cite the technical challenges of building surveillance infrastructure and the need for continued investment in security systems. Neither accountability structure, to donors for development outcomes nor to citizens for security provision, was fully satisfied, yet the dual justification enabled continued resource flows and bureaucratic expansion. The political economy implications of this dual narrative are significant. First, it enabled resource capture by multiple elite actors who could justify their benefits through either development or security rationales, depending on the audience. International technology vendors supplying biometric equipment, software platforms, and consulting services received lucrative contracts framed as development assistance to donors and as security investment to domestic stakeholders. State agencies, particularly the National Identity Management Commission, gained expanded budgets and

personnel justified through both development mandates and security imperatives. Political elites controlling procurement processes benefited from the substantial resource flows regardless of whether development or security outcomes actually improved.

Second, the dual narrative created perverse incentives for implementing agencies. Success for donors was measured through enrollment numbers and system functionality, neither of which required actual improvement in citizen access to services or reduction in insecurity. Agencies could therefore satisfy donor metrics while failing to achieve substantive development or security objectives. Moreover, the persistence of both exclusion (development failure) and insecurity (security failure) justified continued investment and bureaucratic expansion, creating institutional interests in maintaining the problems that digital identity was ostensibly designed to solve.

Third, the divergence between funding rationale and implementation justification reveals underlying power asymmetries in international development cooperation. The World Bank and other donors funded digital identity infrastructure based on assumptions about how such systems would be used, developed, and implemented, without sufficient political economy analysis of how domestic institutional interests and power relations would shape actual implementation. The Nigerian government, as agent rather than principal in this relationship, faced incentives to adopt the outward form of development-oriented digital identity systems while pursuing domestic political and security objectives that diverged from donor intentions. The dual failure, neither development nor security outcomes significantly improved during 2019-2025, suggests that this dual narrative served elite capture more effectively than it served either public welfare or genuine state capacity building. Development-oriented enrollment targets were achieved, but excluded populations remained marginalized. Security-justified surveillance infrastructure was built, but kidnapping and insecurity persisted. Meanwhile, technology vendors profited, agencies expanded, and political elites controlled substantial resource flows. This pattern exemplifies what Pritchett, Woolcock, and Andrews (2013) describe as “isomorphic mimicry,” where institutions build the appearance of modern state capacity without developing the substance of effective governance.

Implementation of Nigeria’s digital identity systems

The Implementation of Nigeria’s digital identity systems revealed deep institutional fragmentation that undermined both development and security objectives. Multiple government agencies maintained overlapping authority over different aspects of identification and security: the National Identity Management Commission controlled the NIN database, the Nigerian Communications Commission regulated telecommunications and enforced the NIN-SIM linkage, the Central Bank of Nigeria managed the Bank Verification Number system, various security agencies claimed intelligence and enforcement responsibilities, and state-level apparatus operated parallel identification systems. Rather than coordinating effectively toward shared objectives, these agencies often competed for resources, authority, and political influence.

This institutional fragmentation reflected rational bureaucratic behavior within Nigeria’s political economy context. As predicted by North, Wallis, and Weingast (2009), institutions in limited-access orders prioritize distributing rents among elite coalitions over efficiently providing public goods. Each agency had interests in maintaining autonomous control over its portion of the identity ecosystem. Integration would require ceding authority and resources to coordinating mechanisms, reducing agencies’ independent power and potentially threatening patronage networks and budget allocations. The result was persistent coordination

failures despite the theoretical benefits of integration for both development and security outcomes.

Evidence of these coordination failures appeared throughout the 2019-2025 period. Security agencies could not access NIMC databases in real-time during operations due to bureaucratic procedures and technical incompatibilities. Inter-agency information sharing required lengthy authorization processes that undermined operational effectiveness during active security incidents. Different agencies maintained separate databases with limited interoperability, preventing comprehensive analysis that would require combining identity, telecommunications, financial, and security data. Jurisdictional disputes delayed responses when multiple agencies claimed authority over particular aspects of digital identity or security operations (Eyikoro and Chigozie, 2021). Beyond institutional fragmentation, capacity constraints within security agencies limited their ability to utilize available digital identity data, even when technically accessible. Many agencies lacked personnel trained in digital forensics, telecommunications analysis, and data-driven intelligence methods. Technical infrastructure for analyzing large datasets and extracting actionable intelligence remained underdeveloped. Operational procedures for how to effectively use digital identity information during investigations had not been standardized across agencies. These capacity gaps meant that even when surveillance capacity existed, agencies could not convert it into operational intelligence that prevented crimes or enabled successful prosecutions.

Criminal networks demonstrated adaptive capacity that further limited the effectiveness of digital identity systems for security purposes. Available evidence suggests that armed groups and kidnapping syndicates adapted to NIN-SIM linkage requirements through several strategies. They obtained unregistered or improperly registered SIM cards through black markets or corruption. They deployed foreign telecommunications services beyond Nigerian regulatory reach. They coerced civilians to register SIM cards in their names for criminal use. They adopted operational security measures, reducing reliance on traceable communications for sensitive activities. The persistence of kidnapping at over 3,400 victims during July 2021 to June 2022 (SBM Intelligence, 2022), and the further escalation to 4,722 victims across 997 incidents between July 2024 and June 2025, with at least 762 people killed (SBM Intelligence, 2025), demonstrates that these adaptation strategies have effectively and persistently circumvented the digital identity infrastructure. Far from diminishing as the NIN database expanded, kidnapping has grown into what SBM Intelligence (2025) describes as a structured, profit-seeking industry.

The political economy of digital exclusion created additional challenges. Mandatory NIN requirements for accessing telecommunications, banking, and other essential services created systematic barriers for vulnerable populations. Rural residents faced substantial costs, including travel to distant enrollment centers, lost work time, and difficulty obtaining prerequisite documentation. Many lacked birth certificates or other documents required for enrollment, creating impossible catch-22 situations. Women in northern Nigeria encountered cultural barriers to biometric registration and travel without male relatives. Nomadic pastoral communities struggled with systems requiring fixed addresses. Poor urban residents lacked resources for enrollment fees or time away from daily labor (Paradigm Initiative, 2021). The enforcement of NIN-SIM linkage through service disconnection imposed severe costs on those unable to obtain NINs. Millions of Nigerians were cut off from mobile banking, family communications, business contacts, and emergency services when their phone lines were disconnected. For many, particularly in informal economic sectors, mobile phones are essential economic tools. Service disruption directly harmed livelihoods. These exclusion

patterns followed existing lines of inequality. Those already marginalized by poverty, geographic isolation, gender, or ethnic identity faced the highest barriers to enrollment and bore the greatest costs from enforcement. Rather than promoting inclusion as development rhetoric suggested digital identity should do, mandatory requirements deepened existing divides.

Weak oversight of surveillance practices created risks of abuse that further undermined the legitimacy of digital identity systems. Throughout 2019-2025, security agencies operated with broad authority to access citizen information without requiring judicial warrants, demonstrating specific investigative necessity, or facing meaningful oversight. While Nigeria enacted the Nigeria Data Protection Act in 2023, implementation and enforcement remained limited. Digital rights organizations documented concerns about surveillance infrastructure being used for political purposes, including alleged monitoring of opposition figures, tracking of civil society activists, and intimidation of journalists (Paradigm Initiative, 2022). The scale of the security failure was further quantified by the Nigeria National Bureau of Statistics, whose Crime Experience and Security Perception Survey revealed that approximately 2.2 million Nigerians were kidnapped between May 2023 and April 2024, with victims paying approximately N2.23 trillion in ransom during that period alone (NBS, 2024). These figures, released in December 2024, expose the profound gap between the state's expanding surveillance infrastructure and its actual capacity to protect citizens. The absence of robust oversight mechanisms meant safeguards against abuse were minimal, while those controlling surveillance infrastructure had limited incentive to accept constraints. Ultimately, the limited effectiveness of digital identity for both development and security governance reflects deeper political economy realities. Security challenges in Nigeria stem from complex factors, including extreme poverty providing recruitment pools for armed groups, youth unemployment creating vulnerability to criminal networks, environmental degradation generating resource competition between farming and pastoral communities, political manipulation of ethnic and religious tensions, corruption within security agencies undermining enforcement, and governance failures alienating peripheral populations from the state. Digital identity systems cannot address these underlying drivers. They offer technological solutions to fundamental political and economic problems.

The political settlement in Nigeria proved easier to achieve around visible technological investments creating concrete benefits for powerful actors, agencies, contractors, and politicians than around difficult institutional reforms threatening existing power arrangements. Digital identity thus became a form of what can be characterized as Security Theater and development theater simultaneously. It projected state action and modernity to international donors and domestic audiences while avoiding the fundamental changes, anti-corruption measures, institutional coordination, addressing poverty, and marginalization that would genuinely improve either development outcomes or security provision but would require disrupting established elite interests. This pattern reveals the limits of technological solutions in contexts where political economy structures prioritize elite capture over public welfare.

Findings

Nigeria achieved significant expansion of digital identity infrastructure between 2019 and 2025, representing growth in one dimension of state infrastructural power: the capacity to collect and store information about the population. NIN enrolment increased from approximately 40 million in 2019 to 121 million by June 2025 and 123.9 million by October 2025, covering well over half the population (NIMC, 2025; TechCabal, 2025). The World

Bank, having extended its project deadline to December 2026 and revised the enrolment target upward to 180 million after Nigeria missed the original June 2024 milestone of 148 million, acknowledged that monthly enrolment rates of approximately 1.08 million fell far short of the 3.3 million per month required to meet the new target (TechCabal, 2025).

The mandatory NIN-SIM linkage policy was enforced nationwide, resulting in millions of SIM card disconnections and eventual compliance by most telecommunications subscribers. The Bank Verification Number system is integrated with NIMC databases to create cross-referenced financial and identity information. This expansion demonstrates the state's enhanced ability to penetrate civil society through data collection, moving from fragmented, incomplete identity databases managed by separate agencies to a more centralized system with substantially broader coverage.

However, this technological infrastructure did not translate into operational security effectiveness. Despite successful data collection, effective coordination among agencies for operational use of digital identity information remained weak. Evidence from government reports and media accounts reveals persistent challenges, including inadequate real-time data-sharing mechanisms between NIMC and security agencies, bureaucratic procedures slowing information access during active investigations, technical incompatibilities between different agencies' systems limiting interoperability, and insufficient personnel training in digital forensics and data analysis within security agencies (Eyikorooha and Chigozie, 2021).

Security agencies gained unprecedented surveillance capacity through the linkage of phone numbers to verified identities and biometric databases for identity verification, yet this capacity did not produce measurable security improvements.

The expansion of infrastructural power therefore, remained largely latent rather than operational. The state gained the capacity to collect data, but did not develop corresponding institutional coordination or analytical capability to utilize that data effectively for security purposes. This represents what Mann (1993) would characterize as incomplete infrastructural power, where administrative reach expands without corresponding improvement in implementation capacity.

Conclusion

Nigeria's digital identity expansion between 2019 and 2025 reveals a fundamental paradox at the heart of technology-driven governance reform: substantial investment in surveillance infrastructure failed to improve security outcomes despite over 100 million NIN enrolments, while simultaneously deepening exclusion among the most vulnerable segments of the population it claimed to empower. The World Bank funded digital identity for development objectives aligned with Sustainable Development Goal 16.9, yet Nigerian government implementation prioritized security enforcement, producing neither development nor security dividends in any meaningful measure. This dual failure is not accidental. It reflects what Pritchett, Woolcock, and Andrews (2013) describe as isomorphic mimicry, where states and institutions build the outward appearance of modern governance capacity without developing its operational substance. Nigeria expanded its data collection infrastructure, satisfying one dimension of Mann's (1984) infrastructural power, but the complementary requirements of institutional coordination, trained personnel, inter-agency information sharing, and accountability mechanisms were absent. Biometric databases were built; the institutional architecture to utilize them effectively was not. The political economy analysis further reveals that this outcome was not a failure of implementation but a predictable consequence

of the incentive structures surrounding Nigeria's digital identity project. Technology vendors, state agencies, and political elites controlling procurement benefited substantially from the resource flows the project generated. Accountability to donors was met through enrolment statistics rather than governance outcomes. Accountability to citizens was diffused by the dual development-security narrative. Meanwhile, rural populations, women in northern Nigeria, nomadic communities, and urban poor faced the highest costs of mandatory enrolment requirements while receiving the least benefit from the infrastructure created. Theoretically, this study contributes to the growing scholarship on the limits of digital state capacity building in weak governance environments. It demonstrates that Mann's infrastructural power framework, while analytically powerful, must be supplemented with political economy analysis that examines whose interests shape how infrastructure is built and governed. Technological capacity without institutional reform, political accountability, and distributional equity cannot produce effective governance outcomes. This finding holds important implications for digital identity policy across sub-Saharan Africa, where similar programmes are underway in Kenya, Ghana, Uganda, and other states receiving substantial international financing for biometric identification systems. Policymakers, donors, and civil society organizations should resist the assumption that enrolment numbers constitute governance success. The quality of institutional coordination, the robustness of data protection frameworks, the accessibility of enrolment systems to marginalized populations, and the accountability mechanisms governing surveillance must all be addressed if digital identity is to fulfil its development promise rather than serve primarily as an instrument of elite resource capture and social control. This study is not without limitations. The reliance on secondary sources means that some dimensions of implementation, particularly the internal decision-making of security agencies and procurement processes, remain opaque. Future research employing primary fieldwork with security officials, NIMC administrators, and affected communities would significantly deepen understanding of the mechanisms identified here. Additionally, the analysis covers the period 2019-2025; a longer-term assessment, as institutional reforms potentially take hold, will be necessary to evaluate whether current trajectories change.

Recommendations

From the discourses above, the paper recommends;

1. Relevant security agencies should establish specialized digital intelligence units, properly staffed, analytically trained, and equipped with modern tools. Training programmes should cover digital forensics, telecommunications analysis, data-driven intelligence methods, and investigative techniques appropriate for addressing technologically sophisticated criminal networks.
2. Budget allocation processes should be restructured to reward agencies that demonstrate effective inter-agency collaboration. Joint task forces with clear authority and dedicated resources should be established for specific security challenges. Institutional cultures that value collective effectiveness over bureaucratic competition must be deliberately cultivated. Without these complementary human capital investments and institutional reforms, digital identity infrastructure will remain underutilized regardless of its technical capabilities.

References

- Besley, T., & Persson, T. (2011). *Pillars of prosperity: The political economics of development clusters*. Princeton University Press.
- Breckenridge, K. (2014). *Biometric state: The global politics of identification and surveillance in South Africa, 1850 to the present*. Cambridge University Press.
- Campbell, J., & McCaslin, N. (2018). Boko Haram's deadly impact. Council on Foreign Relations. <https://www.cfr.org/article/boko-harams-deadly-impact>
- Donovan, K. P. (2012). Mobile money, more freedom? The impact of M-PESA's network power on development as freedom. *International Journal of Communication*, 6, 2647-2669.
- Donovan, K. P., & Park, E. (2019). Perpetual debt in the Silicon Savannah. *Boston Review*, October 20, 2019. <https://www.bostonreview.net/articles/kevin-donovan-emma-park-perpetual-debt-silicon-savannah/>
- Eke, D. O. (2020). Nigeria's digital identification (ID) management program. *Digital Government: Research and Practice*, 1(4), 1-3. <https://doi.org/10.1145/3428093>
- Eubanks, V. (2018). *Automating inequality: How high-tech tools profile, police, and punish the poor*. St. Martin's Press.
- Eyikorogha, Q., & Chigozie, J. (2021). National identity management and security: An assessment of NIMS's performance in Nigeria. *International Journal of Public Administration and Development Studies*, 3(2), 45-67.
- Gelb, A., & Clark, J. (2013). *Identification for development: The biometrics revolution*. Center for Global Development Working Paper 315.
- Gelb, A., & Diofasi, A. (2016). Biometric elections in poor countries: Wasteful or a worthwhile investment? Center for Global Development Policy Paper 435.
- Gelb, A., & Metz, A. D. (2018). *Identification revolution: Can digital ID be harnessed for development?* Center for Global Development.
- Gilpin, R. (1970). The politics of transnational economic relations. *International Organization*, 25(3), 398-419.
- Hosein, G., & Whitley, E. A. (2002). *Assuming answers: Asking the right questions about identity cards and surveillance*. Working Paper, London School of Economics and Political Science.
- International Crisis Group. (2020). *Violence in Nigeria's North West: Rolling back the mayhem*. Africa Report No. 288.
- Iwuoha, V. C., & Doeverspeck, M. (2021). Biometric coloniality: Digital consensus and the biometric state in Africa. *Third World Quarterly*, 42(11), 2686-2704. <https://doi.org/10.1080/01436597.2021.1971305>
- Jacobsen, K. L. (2021). Biometric identity management, sovereignty and the rush to register in humanitarian contexts. In K. L. Jacobsen & A. Sandvik (Eds.), *UNHCR and the struggle for accountability* (pp. 165-186). Routledge.

- Khan, M. H. (2010). Political settlements and the governance of growth-enhancing institutions. SOAS Research Online. <https://eprints.soas.ac.uk/9968/>
- Lyon, D. (2018). The culture of surveillance: Watching as a way of life. Polity Press.
- Madianou, M. (2019). Technocolonialism: Digital innovation and data practices in the humanitarian response to refugee crises. *Social Media + Society*, 5(3), 1-13. <https://doi.org/10.1177/2056305119863146>
- Magnet, S. A. (2011). When biometrics fail: Gender, race, and the technology of identity. Duke University Press.
- Manby, B. (2018). Citizenship and identity in a changing Africa: A collection of essays. Africa Programme, Chatham House.
- Mann, M. (1984). The autonomous power of the state: Its origins, mechanisms and results. *European Journal of Sociology*, 25(2), 185-213.
- Mann, M. (1993). The sources of social power: Volume 2, The rise of classes and nation-states, 1760-1914. Cambridge University Press.
- Masiero, S. (2018). Explaining trust in large technological systems: Healthcare delivery in India. *Journal of Information Technology*, 33(2), 120-132. <https://doi.org/10.1057/s41265-017-0036-6>
- Nigerian Communications Commission. (2020). Guidelines on the linkage of subscriber identification module (SIM) with National Identification Number (NIN). NCC.
- National Identity Management Commission. (2024). Enrolment statistics. Retrieved from <https://www.nimc.gov.ng>
- North, D. C. (1990). Institutions, institutional change and economic performance. Cambridge University Press.
- North, D. C., Wallis, J. J., & Weingast, B. R. (2009). Violence and social orders: A conceptual framework for interpreting recorded human history. Cambridge University Press.
- Office of the National Security Adviser. (2019). National Security Strategy 2019. Federal Republic of Nigeria.
- Omand, D. (2010). Securing the state. Hurst & Company.
- Paradigm Initiative. (2021). LONDA: Nigeria digital rights and inclusion report 2020. Paradigm Initiative.
- Paradigm Initiative. (2022). LONDA: Nigeria digital rights and inclusion report 2021. Paradigm Initiative.

- Premium Times. (2021, April 6). Over 72 million phone lines blocked over NIN linkage. Premium Times Nigeria. <https://www.premiumtimesng.com>
- Pritchett, L., Woolcock, M., & Andrews, M. (2013). Looking like a state: Techniques of persistent failure in state capability for implementation. *The Journal of Development Studies*, 49(1), 1-18. <https://doi.org/10.1080/00220388.2012.709614>
- SBM Intelligence. (2022). Grim reaping: The economics of Nigeria's kidnap industry 2021-2022. A 12-month update. SBM Intelligence.
- Biometric Update. (2024, July 4). World Bank revises Nigeria's digital ID project as country fails to meet critical targets. Biometric Update. <https://www.biometricupdate.com/202407/world-bank-revises-nigerias-digital-id-project-as-country-fails-to-meet-critical-targets>
- National Bureau of Statistics. (2024). Crime experience and security perception survey (CESPS) 2024. Federal Republic of Nigeria.
- National Identity Management Commission. (2025). NIN enrolment report: June 2025. NIMC. <https://nimc.gov.ng/nin/enrolment-report/june-2025>
- SBM Intelligence. (2025). Grim reaping: The economics of Nigeria's kidnap industry 2024-2025. SBM Intelligence.
- TechCabal. (2025, August 22). NIMC must enroll 3.3 million Nigerians monthly to hit 2026 target. TechCabal. <https://techcabal.com/2025/08/22/nimc-nigeria-digital-identity-2026-deadline/>
- Scott, J. C. (1998). *Seeing like a state: How certain schemes to improve the human condition have failed*. Yale University Press.
- Szreter, S. (2007). The right of registration: Development, identity registration, and social security: A historical perspective. *World Development*, 35(1), 67-86.
- Taylor, L. (2016). No place to hide? The ethics and analytics of tracking mobility using mobile phone data. *Environment and Planning D: Society and Space*, 34(2), 319-336.
- The Guardian Nigeria. (2021, April 9). Telecoms: 73 million lines disconnected over NIN. The Guardian. <https://guardian.ng>
- Unsworth, S. (2015). It's the politics! Can donors rise to the challenge? Effective States and Inclusive Development Research Centre Working Paper No. 53.
- Wade, R. H. (2002). Bridging the digital divide: New route to development or new form of dependency? *Global Governance*, 8(4), 443-466.
- World Bank. (2016). Identification for development (ID4D): Strategic framework. World Bank Group.

- World Bank. (2020). Nigeria Digital Identification for Development Project. Project Appraisal Document, Report No. PAD3777. World Bank Group.
- World Bank. (2023). Implementation status and results report: Nigeria Digital Identification for Development Project. World Bank Group.
- Zenn, J. (2020). Unmasking Boko Haram: Exploring global jihad in Nigeria. Lynne Rienner Publishers.
- Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. Public Affairs.