

DNS Policy as Driver and Barrier: Investigating the Intersection of Security, Governance, and Innovation in Nigeria's Digital Economy

NURAINI USMAN¹, BABAWURO USMAN²

^{1,2}Department of International Programmes, Jigawa State Polytechnic for Information and Communication Technology (JSP ICT), Kazaure, Nigeria.

Abstract- The DNS stands as a backbone of the internet infrastructure that drives the digital economy globally. Its policies profile governance structures, impact cybersecurity resilience, and govern innovation potentials. In Nigeria, the digital economy contributed approximately 18.44 percent to the nation's GDP in 2022, yet DNS policy integration with digital development strategies remains fragmented. The aim of the study is to investigate how DNS policy acts instantaneously as a meaningful driver and a barrier across three intersecting dimensions: security, governance, and innovation of the digital economy in Nigeria. The methodology uses a qualitative resource, policy-analytics for DNS. The insights vividly highlighted the five dominant dynamics that define this driver-barrier division. (i) policy disintegration among the NCC, the NITDA, and the NiRA creates government barriers through overlapping mandates but can also drive distributed investigation. (ii) insufficient DNSSEC adoption and DDoS resilience will constitute a security barrier that leaves the DNS infrastructure vulnerable, although fast-tracked deployment would transform a driver of trust. (iii) limited multi-stakeholder coordination acts as a governance barrier that prevents meaningful accountability. Participating in organized coordination drives legitimacy. (iv) DNS-determined digital identity and innovation integration powerfully drive startup and home-grown content growth through .ng namespace, uniformly though expensive registration and renewal costs which lead to the continuity of a persistent barrier to new entry. (v) Universal and Local Policy models offer driver lessons, for instance DNSSEC lower fees and mandates whereas exposing barrier risks comprising of over-regulation and consolidated surveillance. Hence, DNS policy is neither purely beneficial nor harmful in Nigeria, meaningful DNS governance serves as a tactical enabler intended for digital transformation, simply only if the essential barriers of the DNS are systematically addressed. This paper recommends reorganization of the DNS policy to effectively align with the NCC, NITDA, and NiRA directives with the NDEPS through launching meaningful multi-stakeholder governance, accelerating DNSSEC deployment, integrating and implementing an

evidence-based policy monitoring frameworks to effectively strengthen drivers and minimize barriers.

Keywords: Domain Name System, DSN Policy, Digital Economy, Internet Governance, Regulatory Frameworks, NDEPS, DNSSEC, Driver-Barriers Analysis, Innovations

I. INTRODUCTION

The domain name system (DNS) served as a critical and most sophisticated component of the global internet infrastructure, more precisely operating as the internet's address book that is used in translating human-readable domain names also known as uniform resource locator (URL) into machine-readable internet protocol (IP) addresses. It supports worldwide digital infrastructures enabling digital resources and web services accessible from just a click using digital platforms like browsers etc. It is determined as a distributed and hierarchical system supported through international cooperations by the regional registries of the Internet Corporation for Assigned Names and Numbers (ICANN), and national Country Code Top-Level Domain (ccTLD) administrators. The ecosystem of DNS involves multiple layers known as: root nameservers, top-level domain (TLD) operators, registrars, domain registries, and recursive resolvers in this hierarchy are duly functioned by the public DNS services and the internet service providers (ISPs) [1], [2], [3], [4]. The criticality of the DNS infrastructures to digital economy goes beyond technical functionality to institutional magnitudes. The DNS policy frameworks establish governance mechanisms through revealing dispute resolutions, security standards, innovative environments, and stakeholder involvement models [5], [6], [7], [8]. The global institutions such as the internet society (ISOC), the international telecommunication unit (ITU), the organization for economic co-operation and

development (OECD) have progressively recognized the DNS governance as vital to digital transformation strategies, more particularly in the developing economies [9], [10], [11]. DNS policies involve registration rules, security protocols, data access frameworks, and governance formations which have profound propositions for exactly how countries develop their digital economies. Nigeria is the Africa's largest and most populous country, the digital economy demonstrated meaningful exponential growth, contributing 18.44 percent to national global domestic products (GDP) in the second quarter of 2022, surpassing the oil sector's contributing 6.33 percent during the same period [12], [13].

The Information and Communications Technology (ICT) sector's GDP contribution has remains consistently strong with leading tactical strategies reaching 17.34 percent in 2023 [14]. Despite federal government targets of 21 percent by 2027 and 25 percent by 20230 [15], the tactical strategic integration of DNS policy with national digital expansion frameworks remains fragmented and under-examined. Digital economy in Nigeria demonstrated exceptional vitality, based on the information and communication technology (ICT) sector which has grown at multiple annual evolution rates exceedingly over 250,000 direct technology workforces [12], [13], [14], [15], [16]. The Nigerian population is over 200 million, with median age of 18 years in the population, and over 40% broadband penetration offer infrastructural and demographic functions for digital transformation and inclusion [18], [20]. The DNS governance fragmentation in Nigeria is not simply an administrative embarrassment but an operational challenge with measurable penalties. In 2024, a Nigerian record has shown over 4,000 cyber-attacks weekly with an estimated financial loss exceeding N12 billion (approximately USD 15.6 million) [21], [22]. Also, a survey in 2021 found that 71 percent of the domestic organizations encountered cyber-attacks with approximately 44 percent paying ransoms averaging N2.64 billion (approximately USD 3.43 million) [23]. These figures underscore the urgency of examining how DNS policy particularly the security of the .ng namespace which affects national cyberspace resilience. Simultaneously, the .ng domain remained relatively low, with 80 percent of Nigeria's online identity reportedly hosted on foreign domains [24].

This paper addresses a critical gap in the literature through analyzing how DNS policy acts simultaneously as a driver and a barrier across three intersectional dimensions which includes; security, governance, and innovation in the Nigeria's digital economy. A systematic conducting a systematic review, this study adopts a conceptual and policy analytic methodology approach, to conduct intensive research on publicly available policy documents, regulatory reports, industry data, and international case comparison. The central research question is *"In what ways does DNS policy in Nigeria instantaneously enable and constrain digital economy development across the dimension of security, governance, and innovation?"*

This paper makes three principal research contributions. Firstly, it provides an organized mapping of the driver-barrier dynamics with Nigeria's DNS policy framework, offering a conceptual model that could be formed using both scholarly analysis and policy practice. Secondly, it incorporates evidence across five influential themes to present merged assessments. Thirdly, it improves actionable recommendations, depending on comparative analysis and empirical evidence.

The journal consists of seven major sections. As the page numbers may vary based on the topic of research work.

These sections are as follows:

- 1) *Abstract*
- 2) *Introduction*
- 3) *Conceptual Framework*
- 4) *Methodology*
- 5) *Analysis*
- 6) *Discussion and Recommendations*
- 7) *Conclusion*

II. CONCEPTUAL FRAMEWORK

This study is secured in three intersecting conceptual domains: cyber security resilience frameworks, internet governance theory, and innovation systems theory. The DNS policy surroundings are placed at the correlation of these domains, where policy protects security, governance, and innovation outcomes.

2.1 DNS Governance

The DNS is position of disputed governance authority, not basically a technical protocol. The internet governance literature identifies that control over the DNS root zone, ccTLD administration, and registration policies constitutes a form of digital sovereignty [25], [26]. The ICANN's multistakeholder model, that connects the governments and its Ministries, Departments, and Agencies (MDAs), the private sector, civil societies, and the technical communities, has been promoted as the most appropriate and meaningful framework for DNS governance. In African context, ICANN has worked significantly to strengthen regional participation, with the African Engagement Forum and the Africa Regional Plan of 2026 to 2030 straightly emphasizing bottom-up, multistakeholderism to safeguard digital sovereignty [27], [28]. Yet, the translation of this

regional to national contexts in the case of Nigeria remains irregular. The Nigeria Internet Registration Association (NiRA) is playing a significant role in providing ccTLD with the authority of the NITDA [29]. The .ng ccTLD coordinated and maintained by the NiRA successfully registered over 200,000 domains in 2024, with expansion and fast-tracking through commercial registration and government domain policies growth [30], [31], [32]. The .ng registration establishes measurable economic value through domain-driven business formalization, e-commerce platforms, and digital identity incorporation [30], [31], [32]. Though DNS infrastructural advancement remains inhibited by fragmented policy oversight, partial DNSSEC deployment with estimated <10% adoption, and harmonization gaps between NCC, NITDA, and NiRA [33], [34], [35].



Figure 1. Country Code Top-Level Domain (ccTLD) for Nigeria

Figure 1 shows the disaggregation of the second level domain based on .ng standard using institutional disaggregation's. This gives businesses a trust visibility in Nigeria, it improves local trust, strengthens brands and supports long-term digital exponential growth locally [36].

2.2 DNS Security and Cyber security

DNS security remains critical to general cyber security posture. The DNSSEC cryptographically authenticates DNS responses, spoofing, protecting users cache poisoning, and man-in-the-middle

attacks. In the absence of DNSSEC in the .ng domain potential becomes more vulnerable to any kind of malicious phishing and redirection. Recent reports have indicated that Nigeria has experienced countless DNS-related threats, with DNS intensification attacks being a dominant vector in West Africa [37]. The Distributed Denial-of-Service (DDoS) threat landscape concerning Nigeria have been reported as approximately 3,600 intensive attacks between July 2025 to December 2025 alone [38].

2.3 DNS Digital Identity and Innovation

The DNS policy shapes the cost of entry for digital entrepreneurship, from an innovative perspective, the fidelity of online transactions, and the visibility of local contents. The .ng ccTLD serves as a marker of Nigerian digital identity and local economic participation, not only as a technical identifier. The value of Nigeria's digital economy industry estimates approximately 10 to 18 billion dollars, with projections reaching 27 billion dollars by 2030 [39]. The DNS policy openly affects the exponential progress trajectory through meaningful registration pricing, security features, and regulatory clarity.

2.4 The Driver-Barrier Duality

This study has a vital conceptual innovation concentrating on the driver-barrier duality framework. Moderately than treating DNS policy as explicitly beneficial or harmful, the framework identifies that the same policy instrument can rapidly fast-track digital transformation crosswise in one dimension though obstructing it along another. For instance, consolidated DNS governance may improve security oversights and however, it can create barriers to innovation over bureaucratic interruption. Also, low registration fees may initiate domain adoptions deprived of adequate security investment led to a barrier to trust and reliability. Highlighting dual visible across the Nigerian DNS policy landscape.

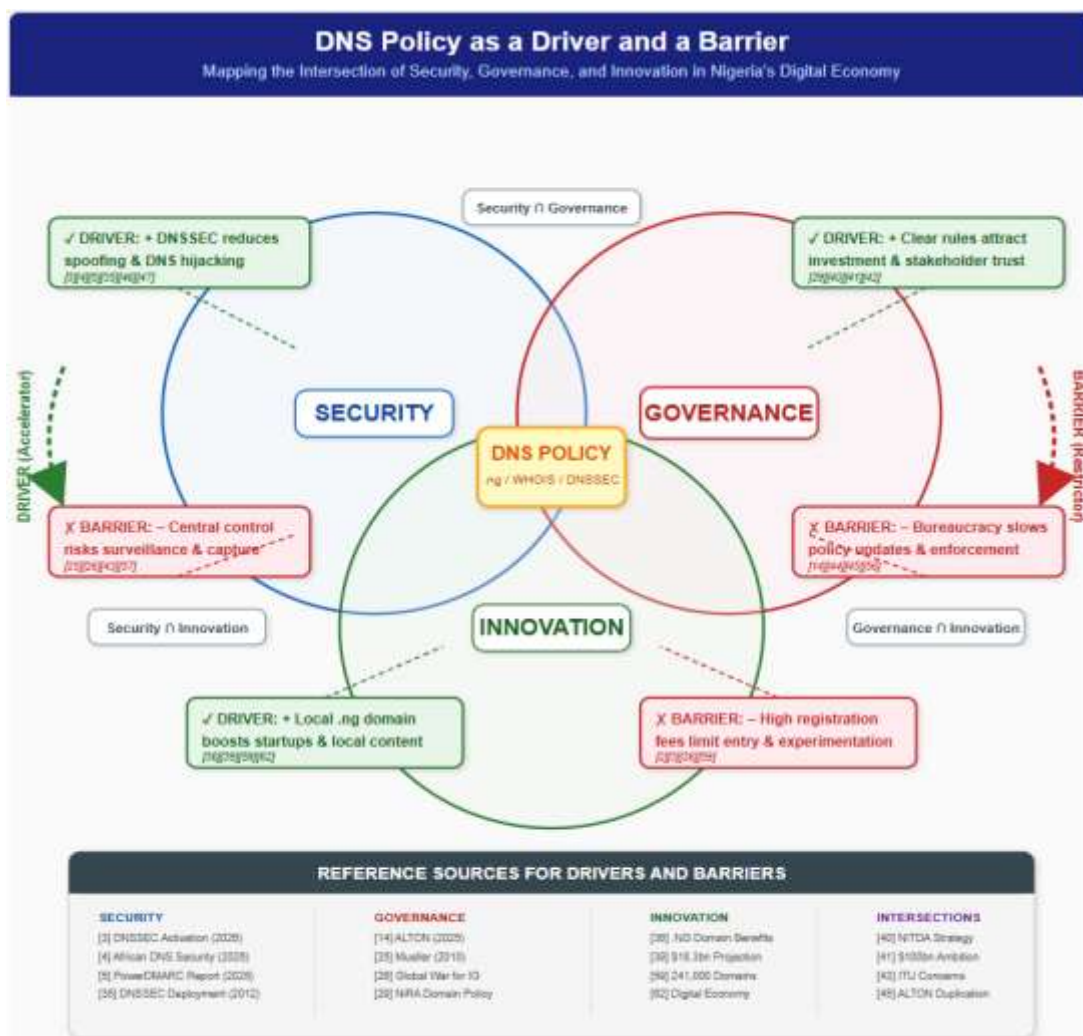


Figure 2. Domain Name Server Policy as a Driver and Barrier with Set Intersections

Figure 2 offers a visual illustration of the Conceptual Framework highlighted for this study focusing on the three intersecting circles representing the beautiful dimensions of Security, Governance, and

Innovation. The center ground lies DNS Policy that operates as both drivers also known as the accelerator and barrier also known as the restrictor. The callout frames identify specific driver and

barrier manifestations, also intersection classifications denote where combined effects occur.

III. METHODOLOGY

This study exercises a qualitative, policy-analytic methodology proposed to map and explore the driver-barrier dynamics of Nigeria's DNS policy. The methodology comprises of three components including: (i) DNS Strategy documents analysis and DNS regulatory apparatuses (ii) Combination of secondary data sourced from cybersecurity metrics, and industry intelligence; and (iii) Proportional investigation with district and intercontinental DNS policy models.

3.1 Data Sources

The DNS resources were drawn from four repositories. (i) DNS regulatory frameworks and policy documents directly sourced from the NCC, NITDA, NiRA, and National Digital Economy Policy and Strategy (NDEPS), part of which the recommended Digital Economy and Electronic Governance Bill were highlighted, and related constitutional apparatus. (ii) The discovery of DNS performance documents from NiRA's annual and business reports between 2024 to 2026, entailing of DNSSEC implementation status, domain name registration statistics, and domain renewal rates. (iii) Cybersecurity threat data reports from the NETSCOUT, Radware, Nigerian Data Protection Commission (NDPC), international cybersecurity organizations, conducting empirical grounding for security background analysis. (iv) Reasonable records from the intercontinental DNS policy frameworks, African ccTLD registries are drawing reports from the Africa Top Level Domains Organization (AfTLD), ICANN, the Internet Society (ISOC) Chapters, and the Coalition for digital Africa.

3.2 Analytical Approach

The analysis was conducted through five iterative phases. Phase 1: involved systematic document gathering, and thematic identification, portraying on the five themes previously known through preliminary policy scanning. Phase 2: encompassed drive-barrier coding for each theme, uniquely segregating between positive drivers and negative driver efforts across security, governance and innovation dimensions. Phase 3: involved in complex intersectional analysis to effectively identify where drivers in one dimension create barriers in another, and contrariwise. Phase 4: involved in comparative analysis, positioning Nigeria's DNS policy within international and broader African contexts to identify transferable lessons. Phase 5: synthesized insights into an integrated assessment and policy recommendations.

3.3 Limitations

The arising limitations need to be taken into consideration. (i) The analysis depends on public available documents on publicly available primarily, which may not eventually capture informal policy practices. (ii) qualitative data aggregated from multiple sources with dynamic methodological guidelines. (iii) the absence of primary interview data means stakeholder viewpoints are reconciled through secondary repositories. (iv) the rapidly dynamic policy landscape means some findings may require updating.

IV. ANALYSIS: DNS FIVE DOMINANT DYNAMICS OF DRIVER-BARRIER DUALITY

The five dominant dynamics that define the driver-barrier duality of DNS policy in Nigeria's digital economy. In each dynamic, the investigation identifies both driver and barrier manifestations across the three intersecting dimensions.

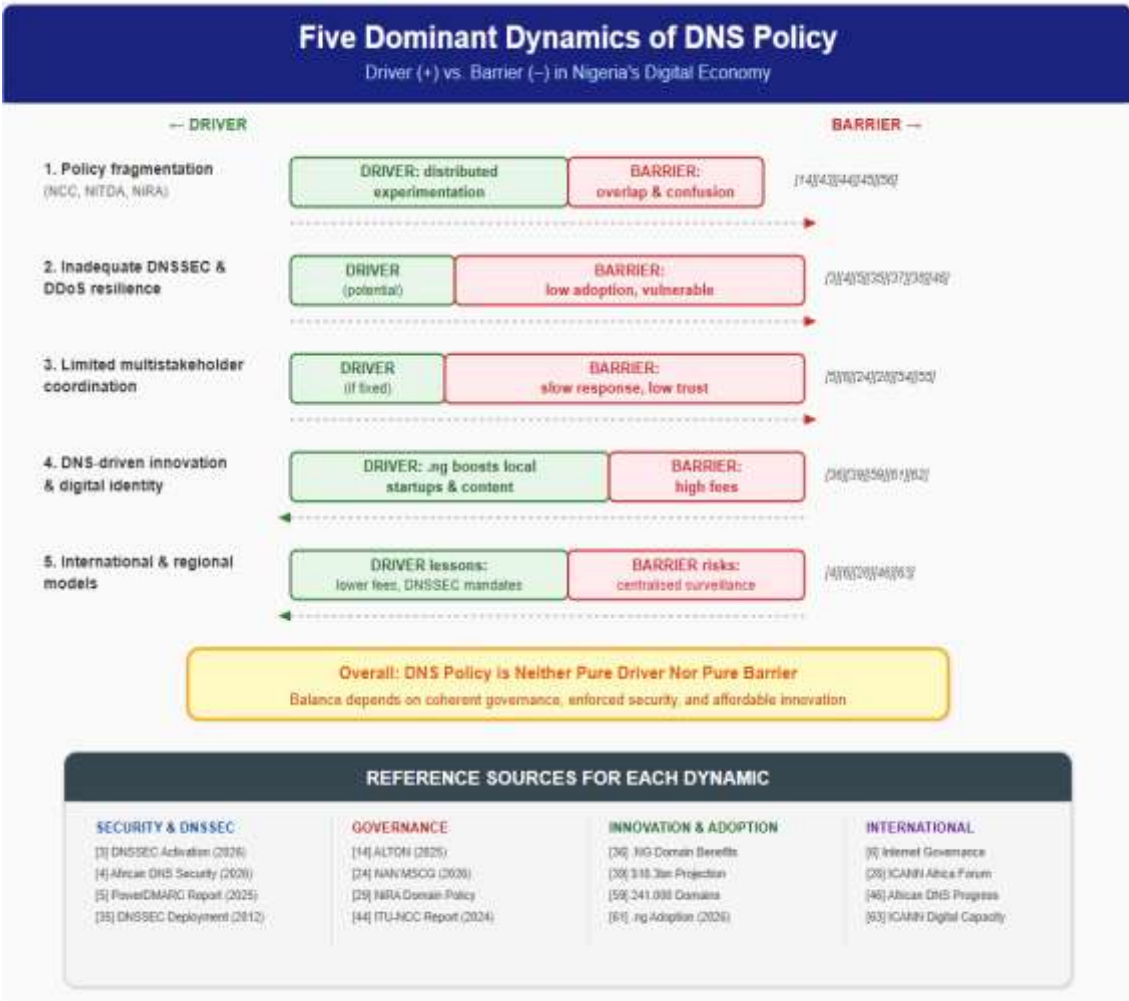


Figure 3. Five Dynamics of Driver-Barrier Duality

Figure 3 offers an illustration summary of the five dynamics highlighted in this study, representing the comparative balance between driver and barrier influences for each theme. The diagram solely highlighted that no dynamic is completely biased; respectively involves both accelerators and restrictors whose continuing effects depends on policy implementation adoptions.

4.1 Dynamic 1: Policy Fragmentation (NCC, NITDA, NiRA)

4.1.1 Driver Effect

The existence of numerous regulatory bodies with overlapping mandates creates more opportunities for regulatory arbitrage and policy experimentation. The expanded mandate of NITDA in 2019 to encompass the digital economy, has enabled the agency to develop strategic frameworks consisting of the National Digital Literacy Framework targeting 95 percent literacy by 2030, and the

Strategic Roadmap and Action Plan of 2024 to 2027, the E-Governance Bill and the National Digital Economy [40], [41]. NiRA with a status of a non-governmental and not-for-profit institute managing the .ng domain delivers operational flexibility that honestly governmental registry might lack [42]. The decentralized governance structure allows different policy methodologies to be experimented across different domains, with potential learning effects.

4.1.2 Barrier Effects

The ITU has openly warned that overlapping functions of NCC and NITDA create regulatory doubt, opening the possibility for licenses, fees, duplication of roles, and forum shopping [43], [44]. The ITU report demonstrated overlapping functions in ICT policy formulation, content regulation, and data protection. Proposed legislation aligning NITDA as a lead-regulator with powers to efficiently classify Artificial Intelligence (AI)

systems could further confuse jurisdictional boundaries [45]. For digital entrepreneurs that are navigating through multiple regulatory requirements, they experience an exponential increase in compliance burden and transactional costs.

4.1.3 Intersectional Effects

Governance decentralization most directly affects innovation through compliance costs, but also has security implications, as known overlapping mandates can form huge gaps in DNSSEC enforcement responsibility. Equally, the distributed governance structure might drive security innovation by allowing NiRA to implement DNSSEC directly without waiting for legislative processes from NITDA or NCC.

4.2 Dynamic 2: Inadequate DNSSEC and DDoS Resilience

4.2.1 Driver Effect

The DNSSEC has made a significant progress in Nigeria. NiRA formally signed the .ng zone and published DNSSEC evidence in the root zone on 15th February 2026 which makes Nigeria one of the most recent African ccTLDs to accomplish full DNSSEC deployment [46]. At the official inauguration in April 2026, the current President of NiRA stated that DNSSEC deployment signifies a defining instant of internet ecosystem for Nigeria through providing most secure atmosphere for businesses, government, and citizens [47], [48], [49]. Once fully implemented in the digital infrastructure DNSSEC will eventually protect users from spoofing, phishing, and traffic redirection, effectively positioning .ng as a more trustworthy namespace for both local and international businesses.

4.2.2 Barrier Effects

Notwithstanding registry-level deployment, DNSSEC adoption at the domain level remains tremendously limited. From a report of 2025 only 8.2 percent of Nigerian domains have DNSSEC enabled, indicating media sector at only 2.63 percent and the banking sector, even though highest is at 27.59 percent [50]. This gap between registry authentication and domain-level activation characterizes a significant security problem. Moreover, Nigeria faces extensive DDoS threats uninterruptedly with visible analysis showing over 1,716 DDoS attacks in the latter half of 2024, with DNS amplification outstanding the dominant attack

vector [37], [51]. The cyber-attack rate recorded 71 percent among Nigerian organizations [52], and over 4,000 weekly cyber-attacks [53]. This clearly highlighted the scale of the challenge.

4.2.3 Intersectional Effects

The driver potential of DNSSEC is perfect, a secure .ng namespace boosts trust in Nigerian digital space through attracting investment and supporting of e-commerce growth. Yet, low adoption changes a potential security driver into a persistent security barrier. Highlighting the government failures as inadequate enforcement mechanisms, unclear accountability, and insufficient registrar training for DNSSEC implementation are the root causes leading to a persistent security barrier.

4.3 Dynamic 3: Limited Multistakeholder Coordination

4.3.1 Driver Effect

In response to the coordination scarcity, Nigeria has taken steps to institutionalize multistakeholder governance. NITDA inaugurated a Multi-Stakeholder Coordinating Group (MSCG) on Digital Governance on April 2026 with a mandate of deepen accountability, transparency, and inclusion in Nigeria's digital space [24]. The Nigeria Internet Governance Forum (NIGF) operates through a Multi-Stakeholder Advisory Group (MAG) consisting of private and public sector representative [54]. The NCC correspondingly supports a multistakeholder model of engagement together with proposed codes of practice for an open internet [55]. This institutional apparatus when functioning effectively can positively drive policy responsiveness and legitimacy.

4.3.2 Barrier Effects

Regardless of the institutional frameworks, coordination failures continue dynamically. NIGF's efficacy remains limited by irregular meetings and unreliable stakeholder participation. The ITU's 2024 warning about regulatory disintegration directly implicates coordination failures [56], [57]. The DigitalSENSE Forum 2026 focused on driving Sustaining World Summit on the Information Society (WSIS) Vision with Multistakeholder Synergy in Nigeria, this frame implicitly acknowledges recent synergy gaps. For DNS policy to be specifically lack coordination between regulators including NCC; known to be the telecommunication regulator, NITDA; known to be

the digital economy agency, and NiRA; known to be the technical operator, these issues extensively create government resistance and friction, making resolutions more challenging.

4.3.3 Intersectional Effects

The coordination barrier most directly distresses governance legitimacy but also has sophisticated security implications of coordination failures which slows incident response and DNSSEC rollouts, and innovation implications also makes doubt about which body has authority over DNS-related matters which creates investment hesitation. The fractional existence of coordination mechanisms for both MSCG and NIGF significantly demonstrate driver potential, but their inconsistent operation and limited authority represent a governance barrier that requires systemic transformation.

4.4 Dynamic 4: DNS-Driven Innovation and Digital Identity Incorporation

4.4.1 Driver Effect

The .ng ccTLD serves as a Nigerian digital identity and sophisticated platform for innovation. Based on statistics NiRA have recorded 241,000 actives .ng domains under management, 71,470 renewals, 98,285 new registration as of 2025 [58], [59]. The .ng namespace has been explicitly positioned as Nigeria's digital identity in cyberspace, the suffix of official email address originating within Nigeria [60], [61]. The Nigeria First Policy Agenda that was initiated and accepted by the Federal Executive Council in May 2025; the mandates enforced all federal ministries, departments, and agencies (MDAs) to significantly prioritize on domesticated produced goods and services with the extension .ng adoption, also recognized as a strategic tool for digital sovereignty [61].

For Small and Medium-sized Enterprises (SMEs), and startups, the .ng registration offers local trust and legitimacy that foreign domains cannot contest. The Tech Career Outlook and NiRA's .ng Academy programmes aims to bridge skills gaps in the DNS ecosystem and to continue driving human capacity development. The growth of Nigeria's digital economy from 5.09 billion dollars in 2019 to 9.97 billion dollars in 2021 has been moderately credited to the enabling role of local digital infrastructure including the .ng namespace [62].

4.4.2 Barrier Effects

Despite these driver effects, substantial barriers persist including high cost of registration and renewal which are the most cited barriers to .ng adoption more especially for micro-enterprises and informal sector businesses with a statistical index of about 96.9 percent of Nigerian Micro, Small, and Medium Enterprises (MSMEs). With so many years of advocacy, adoption of the .ng ccTLD has stayed relatively low with a statistics showing 80 percent of Nigeria's digital identity hosted outside the .ng domain [61]. The adoption of foreign domains directly breaches the Nigeria First Policy and sidelines the homeland's own online identity. Stakeholders have cautioned that slow adoption of .ng could limit digital economy growth, with an argument that the country cannot claim digital leadership while 80 percent of its online identity is hosted around the globe [61].

4.4.3 Intersectional Effects

The driver-barrier pressure in this dynamic is severe as the same .ng infrastructure that could serve as a national innovation framework is constrained by expensive fees and awareness barriers that exclude most potential end users. Innovation is most strongly driven when .ng adoption is well-understood and affordable; it is majors' barrier when costs exclude micro-enterprises and start-ups.

4.5 Dynamic 5: International and Regional Models

4.5.1 Driver Effect

Nigeria has benefited from international and regional capacity-building initiatives. The Alliance from Digital Africa's ccTLD capacity development program specifically supported by ICANN has worked to improve the sustainability and effectiveness of African ccTLDs [63] [27]. The deployment of the highest level of DNS (L-Root server) clusters in Africa improves DNS resilience and reduce latency [27]. Regional leaders such as South Africa (.za) and Kenya (.ke), offer driver lessons as the former through liberalized pricing that drives domain adoption, the latter through recognized DNSSEC implementation. A researcher has argued that Africa's digital resilience pivots a technically competent workforce of managing modern DNS technologies. Nigeria has participated in DNSSEC capacity-building and roadshows efforts through the Internet Society (ISoC) and the Coalition for Digital Africa [64].

4.5.2 Barrier Effects

International models also portray barrier risks. Having a centralized DNS governance as accompanied by some non-African authorities produces scrutiny risks and potential challenges for political control over namespace access. Over-regulation in the guidelines that was introduced from the models was designed for larger, and more efficient and mature digital economies can effectively stifle local innovation by magnificent compliance burdens, which is unsuitable for market's structure of Nigeria. The ITU's call for regulatory reconstruction in Nigeria indirectly acknowledges that intercontinentally recommend regulatory configuration many not directly translate to some national dimension without variations and adaptations. Nearly 35 percent of the African ccTLDs obligated began DNSSEC implementation in early 2025 demonstrating that the local driver landscape remains unbalanced, with experience from leaders not yet adopted by followers.

4.5.3 Intersectional Effects

Driver lessons from local leaders suggest actionable pathways for Nigeria to expand the DNSSEC deployment, consolidate corporate governance expertise and make registration fees more

affordable. Barrier risks starting from over-regulatory models warn compared to wholesale implementation of foreign frameworks excluding careful background analysis. Nigeria's Digital economy is valued ranging from 10 to 18 billion dollars with targets of 25 percent additional input by 2030, has reasonably scale to require domesticated policy resolutions rather than constraint of foreign models.

V. DISCUSSION AND RECOMMENDATIONS

5.1 Synthesis of Key Findings

The analysis uncovers that DNS policy in Nigeria managed as a complicated two-edged weapon. The insights across all five dynamics emphasized the same policies that meaningfully drive digital transformation instantaneously create broad barriers that constrain it. Obviously, this duality is not a sign of significant policy failure in isolation but a dynamic characteristic of DNS policy in contexts where regulatory frameworks are exponentially growing, institutional capacities are unstable, and stakeholder coordination remains imperfect. Table 1 summarizes the driver-barrier balance based on the insights.

Table 1: Summary of Driver-Barrier Dynamics in DNS Policy of Nigeria

S/N	Dynamic	Primary Driver Effect	Primary Barrier Effect	Net Direction
1	Policy Fragmentation (Dynamic 1)	Distributed investigation at NCC, NITDA, and NiRA	Forum shopping, regulatory confusion, duplication fees	Barrier-dominant
2	DNSSEC Adoption (Dynamic 2)	Registry-level deployment of 2026, enhanced trust	Domain-level adoption only 8.2 percent, DDoS vulnerability	Barrier-dominant
3	Multistakeholder Coordination (Dynamic 3)	Institutional frameworks (NIGF, Multi-Stakeholder Coordinating Group (MSCG), and NCC codes)	Limited authority, inconsistent operation	Barrier-dominant
4	DNS-Driven Innovation (Dynamic 4)	Local identity value, .ng growth with 241,000 domains	High fees, low adoption of 80 percent identity outside .ng	Balanced
5	International Models (Dynamic 5)	L-Root deployment, capacity building	Uneven regional adoption, Imported over-regulation	Balanced

The Table 1 Governance-related barriers are dynamics 1, 2, and 3 which are currently stronger than their driver complements, while innovation (4) and international (5) dynamics demonstrate more balanced trade-offs. This suggests that governance reform should be the priority intervention opinion.

5.2 Recommendations

Based on the analysis, four integrated as represented from A-D recommendations are advanced, each effectively addressing specific driver-barrier imbalances identified in the five dynamics.

5.2.1 Recommendation A: DNS Policy

Reconstruction to Align with NCC, NITDA, and NiRA Mandates based on the National Digital Economy Policy and Strategy (NDEPS)

In 2024 the ITU's call for regulatory reorganization must be operationalized through a formal Memorandum of Understanding (MoU) among the three bodies (NCC, NITDA, NiRA) should be negotiated and exchanged, specifying principal responsibility for: (i) DNSSEC enforcement and incident response lead by NiRA as the technical operator, followed by NCC as a security regulator; (ii) digital economy-general policy coordination lead by NITDA; and (iii) connectivity and telecommunications oversight lead by NCC. The MoU should be carefully reviewed by the Multi-Stakeholder Coordination Group. Without clear role description, the barrier of regulatory overlap will continue, undermining investment confidence within the Nigeria's digital economy.

5.2.2 Recommendation B: Unveiling Structured Multistakeholder Governance with the Appropriate Decision-Making Authority

The existing MSCG, NCC, and NIGF multistakeholder mechanisms provide useful platforms but lack requisite decision-making authority. A statutory *Nigeria DNS Policy Council (Nig-DNS-PoC)* is proposed to be established, grouping experts from NiRA as the technical operator, NCC as the regulator, NITDA as the digital economy agency, industry consisting of registrars, Internet Service Providers (ISPs), civil society as the digital rights organizations, and the start-up ecosystem. The established council should have the power and authority to effectively coordinate the following: (i) The council is responsible for agreeing and approving any changes to .ng registration policy; (ii) Have the power effectively establish DNSSEC enforcement timelines; (iii) Recommend any registration fee modifications to the NiRA board of trustees; and (iv) Facilitate jurisdictional discrepancies and disputes between the regulatory institutions. The barrier of unreliable management cannot be overcome without institutionalizing

decision-making authority meaningfully with excellent guidelines.

5.2.3 Recommendation C: DNSSEC Deployment

Speeding-up through Layered Policy Mechanisms Registry-level DNSSEC acquisition achieved in February 2026 is mandatory but inadequate. To successfully address the 8.2 percent domain-level barrier, the government DNS experts should implement the following three-tiered approach: (i) Implementation of compulsory enforcement for government domains .gov.ng with compliance deadlines; (ii) Also, create a financial incentives for private division adoption, covering reduced fees for DNSSEC-enabled domains; and (iii) Registrar capacity-building to guarantee technical capability to support customers with DNSSEC implementation. The ITU requires to be co-opted to present technical support for registrar training, forming the Coalition for Digital Africa DNSSEC roadshows.

5.2.4 Recommendation D: Implement Evidence-Based Policy Monitoring System

Currently, there is no existing evidence with systematic and or longitudinal data stored in a repository labeled as a DNS policy outcome in Nigeria. This highlighted the urgent need for DNS Policy Observatory and Tracking system that can evidently store DNS information for research and other evidenced-based interventions, proposed to be housed within NITDA and NiRA with intensive monitoring and support from the DNS expert group, responsible for annual reporting effectively on the following: (i) Establish .ng registration activities and fee elasticity; (ii) Setup a DNSSEC approval rates built on sectoral analysis; (iii) Establish a stakeholder satisfaction with intensive multistakeholder synchronization; (iv) Establish a professional cybersecurity events and incidents data correlated to DNS vulnerabilities; (v) Effectively set-up a comparative benchmarking guidelines against African peer ccTLDs comprising of Kenya (.ke), South Africa (.za), Rwanda (.rw) This recommended evidence-based monitoring would ultimately allow an iterative policy fine-tuning, guaranteeing that drivers are scaled and barriers addressed equally as condition change in dynamic circumstances toward improving the Nigeria's digital economy.

The recommendations A – D procedures provided a process of digital economy strengthening. Pilot for translation of the recommendations should be conducted by the NKF, using digital tracking systems to effectively examine and document the processes, doing this would become a positive and the most efficient method of tracking our research feedback. During the processes we would identify the challenges to become our solid evidence. The process is going to be expensive because of stakeholder engagement in the experiments, we also need the implementers to efficiently identify the best procedures that would be cost effective during the pilot implementation. The evidence would be a meaningful as the DNS intervention was done toward strengthening Nigeria's digital economy.

VI. CONCLUSION

The study has successfully investigated and analyzed how the DNS policy acts simultaneously as a drive and a barrier across the identified three intersecting dimensions including security, governance, and innovation in the Nigeria's digital economy. Even though effective mapping of the five dominant dynamics has been completed, the analysis has effectively demonstrated that DNS policy has been neither beneficial nor harm. It meaningfully facilitates digital transformation when governance is logical, security mandates are duly enforced, and innovation cost are low. It initially becomes a barrier when regulatory authorities overlap with each other, DNSSEC deployment lags, stakeholder coordination fails, and fees exclude new entrants.

The study offers driver to barrier duality frameworks effectively highlighting a conceptual instrument for efficient analysis of the internet governance policies in other emerging economy dimensions. Also understood that these same dynamics examined in Nigeria with massive digital security implementation gaps, innovation pricing barriers, policy fragmentations, coordination deficits, and very complex intercontinental scratch that are more likely to manifest, with extensive local discrepancies across other African and Global South digital economies. Conducting intensive a comparative studies using this framework to Ghana, Kenya, Rwanda, South Africa would productively produce a valuable insight to which the driver to barrier

trade-offs is generalizable and are practically framework specific.

The path forward is transparent but extensively demanding in the Nigerian context. Having a meaningful DNS governance is a strategic enabler for any digital transformation, only if its fundamental barriers are fully identified and progressively addressed. The digital economy's exponential growth route from 18 percent to a projected 25 percent of GDP as at 2030, which will substantially be affected by how well Nigeria coordinated the driver to barrier duality at the central zone if its DNS policy framework. The recommendations actively advanced in the study focused on regulatory orientations and alignments, accelerated DNSSEC deployment, evidence-based policy monitoring, and structured multistakeholderism governance. The study provides a tactical practical roadmap for effective rewarding of the balance for barrier-dominant to maximum ultimate driver. The status for decisive policy actions perfectly aligns with the digital economy's ambitions, as known delay will not eradicate barriers but only entrench them, which means at this level we need actions.

ACKNOWLEDGEMENT

The authors express their gratitude to the Ndukwe Kalu Foundation (NKF) an organization affiliated to the Nigeria Internet Registration Association (NiRA) for their invaluable support throughout this research, despite the challenges and limited resources encountered during the process. We appreciated the NKF team collaboration and support throughout the process of the research work.

FUNDING INFORMATION

This study was supported by the NKF an organization affiliated to the NiRA, under the grant support for the post-graduate research award with a title "The Impact of DNS Policy on the Development of the Digital Economy in Nigeria", awarded to Nuraini Usman under the full supervision of Prof. Babawuro Usman at the Jigawa State Polytechnic for Information and Communication Technology, (JSPICT), Kazaure, Nigeria. The grant was awarded on the 2nd of November 2024 by the NKF executive management.

REFERENCES

- [1] H. Arksey and L. O'Malley, "Scoping studies: Towards a methodological framework," *International Journal of Social Research Methodology: Theory and Practice*, vol. 8, no. 1, pp. 19–32, Feb. 2005, doi: 10.1080/1364557032000119616.
- [2] A. Shostack, J. Jacobs, and W. Baker www.globalcyberalliance.org, "The Economic Value of Dns Security", [Online]. Available: <https://www.globalcyberalliance.org/wp-content/uploads/GCA-DNS-Security-Report.pdf>
- [3] S. Jorge, A. Mangal, and E. Sarpong, "Affordability Report 2020 Acknowledgements," 2020, [Online]. Available: www.a4ai.org
- [4] M. Niestadt, "Internet governance Keeping the internet open, free and unfragmented," no. November, 2024.
- [5] O. Ikechukwu, C. Nweke, J. Chukwuemeka, and J. Igweike, "Leveraging Technology to Bridge the Policy Innovation Gap in Developing Countries: Enhancing Service Delivery and Public Engagement," *West African Journal of Interdisciplinary Research*, vol. 2, no. 2, p. 56, 2024.
- [6] Internet Society (b), "Internet Governance - An Internet Society Public Policy Briefing," *Internet Society*, no. October, pp. 1–5, 2015.
- [7] "Nigeria's ICT sector contribution to GDP increases in Q1 2025 - NBS." Accessed: Mar. 07, 2026. [Online]. Available: <https://www.premiumtimesng.com/business/business-news/808747-nigerias-ict-sector-contribution-to-gdp-increases-in-q1-2025-nbs.html>
- [8] R. Heeks and R. Bukht, "Digital Economy Policy: The Case Example of Thailand," *SSRN Electronic Journal*, vol. 9, no. 1, pp. 176–189, 2020, doi: 10.2139/ssrn.3540030.
- [9] S. Calder, "Internet Governance," *Encyclopedia of Cyber Warfare*, pp. 148–150, 2017, doi: 10.7551/mitpress/9780262012850.003.0010.
- [10] C. Perumal, N. Lyndon, and Z. Sakawi, "Evaluating ICT development: Indicators, digital progress, and societal impact for sustainable development," *International Journal of Advanced and Applied Sciences*, vol. 11, no. 9, pp. 36–47, 2024, doi: 10.21833/ijaas.2024.09.005.
- [11] *Measuring the digital economy*. 2023. doi: 10.30875/9789287073594c010.
- [12] "Nigeria's digital economy projected to hit \$18.3bn by 2026." Accessed: Jun. 14, 2026. [Online]. Available: <https://punchng.com/asset-managers-project-18-3bn-digital-economy-for-nigeria/>
- [13] "At The Launch of Two Policies on Digital Economy, President Buhari Says Diversification Has Been Most Successful In The Sector – The Statehouse, Abuja." Accessed: Jun. 14, 2026. [Online]. Available: <https://demo2.acresal.gov.ng/news/at-the-launch-of-two-policies-on-digital-economy-president-buhari-says-diversification-has-been-most-successful-in-the-sector/>
- [14] "ALTON slams \$1trn digital vision as 'House on Faulty Foundation' amid regulatory duplication - Businessday NG." Accessed: Jun. 14, 2026. [Online]. Available: <https://businessday.ng/technology/article/alton-slams-1trn-digital-vision-as-house-on-faulty-foundation-amid-regulatory-duplication/>
- [15] "FG eyes 25% GDP growth from ICT by 2030 - Businessday NG." Accessed: Jun. 14, 2026. [Online]. Available: <https://businessday.ng/news/article/fg-eyes-25-gdp-growth-from-ict-by-2030/>
- [16] Nigerian Communications Commission, "2024 Subscriber/Network Performance Report Policy, Competition And Economic Analysis Department," pp. 1–78, 2024.
- [17] "The cost of cyber insecurity: How it affects Nigeria's digital economy - Businessday NG." Accessed: Mar. 07, 2026. [Online]. Available: <https://businessday.ng/opinion/article/the-cost-of-cyber-insecurity-how-it-affects-nigerias-digital-economy/>
- [18] B. Egert, T. J. Kozluk, and D. Sutherland, "Infrastructure and Growth: Empirical Evidence," *SSRN Electronic Journal*, no. 685, 2021, doi: 10.2139/ssrn.1360784.
- [19] "(17) Stable and Secure DNS towards a prosperous Digital Economy in Africa | LinkedIn." Accessed: Mar. 07, 2026. [Online]. Available: <https://www.linkedin.com/pulse/stable-secure->

- dns-towards-prosperous-digital-economy-
olorundare-sbmtc/
- [20] “National_Digital_Economy_Policy_and_Strategy”.
- [21] “Nigeria loses N12bn to cyberattacks as FG, experts chart path for digital economy growth - Tribune Online.” Accessed: Jun. 14, 2026. [Online]. Available: <https://tribuneonlineng.com/nigeria-loses-n12bn-to-cyberattacks-as-fg-experts-chart-path-for-digital-economy-growth/>
- [22] “NDPC: 4,000 weekly cyberattacks push data localisation, stricter compliance - Vanguard News.” Accessed: Jun. 14, 2026. [Online]. Available: <https://www.vanguardngr.com/2026/05/ndpc-4000-weekly-cyberattacks-push-data-localisation-stricter-compliance/>
- [23] Sophos Ltd, “the State of Ransomware 2025,” no. April, p. 17 pages, 2025, [Online]. Available: www.sophos.com
- [24] “FG Moves To Strengthen Digital Governance, Inaugurates Coordination Group - News Agency Of Nigeria.” Accessed: Jun. 14, 2026. [Online]. Available: <https://nannews.ng/fg-moves-to-strengthen-digital-governance-inaugurates-coordination-group/>
- [25] M. L. Mueller, “Networks and States: The Global Politics of Internet Governance,” *Networks and States*, Sep. 2010, doi: 10.7551/MITPRESS/9780262014595.001.0001.
- [26] “t he globa l wa r f o r internet gove rna nc e”.
- [27] S. P. Collins *et al.*, “No Title 濟無No Title No Title No Title,” *Ilmu-ilmu keislaman dan kemasyarakatan*, vol. 2 No 1, no. 0, pp. 167–186, 2021.
- [28] “Press Release: Africa Engagement Forum Opens in Accra, Strengthening Regional Collaboration on Internet Governance - ICANN.” Accessed: Jun. 14, 2026. [Online]. Available: <https://www.icann.org/resources/press-material/release-2025-12-09-en>
- [29] “NiRA DOMAIN NAME POLICY.”
- [30] S. Sheng, “The Internet Ecosystem and ICANN !,” no. April, pp. 1–28, 2013.
- [31] I. T. Union and D. Sector, *Regional good practices*. 2021.
- [32] D. Sector, “Regional good practices: Accelerating innovation, entrepreneurship and digital transformation in the Africa region.”
- [33] ITU, “Digital Infrastructure Investment: Collaborative approaches and mechanisms to finance universal connectivity,” pp. 1–5, 2024.
- [34] A. G. Femi, M. O. Adenomon, I. O. Gilbert, and U. Ibrahim, “The Effects of Data Privacy Regulations on Cybersecurity Practices in Nigeria and Africa adopting data privacy laws inspired by international standards like the European Union ’ s General Data Protection Regulation (GDPR). The African Union ’ s Malabo C,” pp. 313–336, 2025.
- [35] D. York, “Challenges and Opportunities In Deploying DNSSEC A progress report on an investigation into DNSSEC deployment,” *Satin*, 2012, [Online]. Available: <http://conferences.npl.co.uk/satin/papers/satin-2012-York.pdf>
- [36] “Exploring the Significance and Benefits of Your .NG Domain.” Accessed: Jul. 02, 2026. [Online]. Available: <https://gitservers.com.ng/blog/benefits-of-ng-domain/>
- [37] D. Threat and I. Report, “UNMASKING THE SWARM: THE EVOLVING TACTICS OF BOTNET-DRIVEN DDoS,” no. 16.
- [38] “Nigeria - Latest Cyber Threat Intelligence Report.” Accessed: Jun. 14, 2026. [Online]. Available: <https://www.netscout.com/threatreport/country/nigeria/>
- [39] “Nigeria’s digital economy projected to hit \$18.3bn by 2026.” Accessed: Jun. 14, 2026. [Online]. Available: <https://punchng.com/asset-managers-project-18-3bn-digital-economy-for-nigeria/>
- [40] “NITDA Reaffirms Drive For A Digitally Inclusive, Innovation-Led Nigerian Economy – NITDA.” Accessed: Jun. 19, 2026. [Online]. Available: <https://nitda.gov.ng/nitda-reaffirms-drive-for-a-digitally-inclusive-innovation-led-nigerian-economy/8986/>
- [41] “Shaping Tomorrow: NITDA Outlines the Strategic Pillars of Nigeria’s \$100bn Digital Ambition – NITDA.” Accessed: Jun. 19, 2026. [Online]. Available:

- <https://nitda.gov.ng/shaping-tomorrow-nitda-outlines-the-strategic-pillars-of-nigerias-100bn-digital-ambition/9323/>
- [42] “NiRA DOMAIN NAME POLICY”.
- [43] “ITU Expresses Concerns Over Nigeria’s Multiple Regulations In Digital Space – Independent Newspaper Nigeria.” Accessed: Jun. 19, 2026. [Online]. Available: <https://independent.ng/itu-expresses-concerns-over-nigerias-multiple-regulations-in-digital-space/>
- [44] ITU & NCC, “National Launch of the Collaborative Regulation Report: Accelerating Nigeria’s Digital Transformation,” 2024, [Online]. Available: <https://www.itu.int/en/ITU-D/Regional->
- [45] “ALTON slams \$1trn digital vision as ‘House on Faulty Foundation’ amid regulatory duplication - Businessday NG.” Accessed: Jun. 19, 2026. [Online]. Available: <https://businessday.ng/technology/article/alton-slams-1trn-digital-vision-as-house-on-faulty-foundation-amid-regulatory-duplication/>
- [46] “Continued Progress in African DNS Security | ISOC Pulse.” Accessed: Jun. 19, 2026. [Online]. Available: <https://pulse.internetsociety.org/en/blog/2026/02/continued-progress-in-african-dns-security/>
- [47] “Nigeria activates DNSSEC on .ng domain to curb cyber fraud, boost digital trust - Businessday NG.” Accessed: Jun. 19, 2026. [Online]. Available: <https://businessday.ng/technology/article/nigeria-activates-dnssec-on-ng-domain-to-curb-cyber-fraud-boost-digital-trust/>
- [48] “Nigeria deploys DNSSEC to strengthen .ng domain security - Vanguard News.” Accessed: Jun. 19, 2026. [Online]. Available: https://www.vanguardngr.com/2026/04/nigeria-deploys-dnssec-to-strengthen-ng-domain-security/#google_vignette
- [49] “NiRA deploys DNSSEC to secure Nigeria’s .ng domain against cyber threats - Technology Times | Latest and Breaking Nigeria Tech News.” Accessed: Jun. 19, 2026. [Online]. Available: <https://technologytimes.ng/nira-deploys-dnssec-to-secure-nigeria-ng-domain/>
- [50] “Nigeria DMARC & MTA-STS Adoption Report 2025 Assessing the Threat Landscape,” 2025.
- [51] “REPORT: NETSCOUT Hints on Shifting DDoS Attack Patterns in West Africa | Tech | Business | Economy.” Accessed: Jun. 20, 2026. [Online]. Available: <https://techeconomy.ng/report-netscout-hints-on-shifting-ddos-attack-patterns-in-west-africa/>
- [52] “The State of Ransomware 2021 | SOPHOS.” Accessed: Jun. 20, 2026. [Online]. Available: <https://www.sophos.com/en-us/blog/the-state-of-ransomware-2021>
- [53] “Nigeria Records 4,000 Weekly Attacks amid \$10.5tn Global Cybercrime - Olatunji | Tech | Business | Economy.” Accessed: Jun. 20, 2026. [Online]. Available: <https://techeconomy.ng/nigeria-records-4000-weekly-attacks-amid-10-5tn-global-cybercrime-olatunji/>
- [54] “NIGF 2024 – Nigeria Internet Governance Forum.” Accessed: Jun. 20, 2026. [Online]. Available: <https://igf.ng/nigf-2024/>
- [55] “Stakeholder Consultation for Establishment of an Internet Industry Code of Practice | NCC.” Accessed: Jun. 20, 2026. [Online]. Available: <https://www.ncc.gov.ng/consumers/public-consultations/stakeholder-consultation-for-establishment-of-an-internet-industry-code-of-practice>
- [56] ITU-D, *Collaborative regulation: Accelerating Nigeria’s digital transformation*. 2023.
- [57] “ITU Expresses Concerns Over Nigeria’s Multiple Regulations In Digital Space – Independent Newspaper Nigeria.” Accessed: Jun. 20, 2026. [Online]. Available: <https://independent.ng/itu-expresses-concerns-over-nigerias-multiple-regulations-in-digital-space/>
- [58] F. W. Avenue and A. M. P. Wednesday, “NiRA ZOOM PLATFORM AND NiRA SECRETARIAT ,” 2025.
- [59] “NiRA records 241,000 active .ng domains, targets nationwide adoption - Nairametrics.” Accessed: Jun. 20, 2026. [Online]. Available: <https://nairametrics.com/2026/06/08/nira-records-241000-active-ng-domains-targets-nationwide-adoption/>
- [60] “Nigeria loses N12bn to cyberattacks as FG, experts chart path for digital economy growth

- Tribune Online.” Accessed: Jun. 20, 2026.
[Online]. Available:
https://tribuneonlineng.com/nigeria-loses-n12bn-to-cyberattacks-as-fg-experts-chart-path-for-digital-economy-growth/#google_vignette
- [61]. “ng adoption as pathway to digital sovereignty.” Accessed: Jun. 20, 2026.
[Online]. Available:
<https://guardian.ng/technology/tech/ng-adoption-as-pathway-to-digital-sovereignty/>
- [62] “Nigeria’s digital economy projected to hit \$18.3bn by 2026.” Accessed: Jun. 20, 2026.
[Online]. Available:
<https://punchng.com/asset-managers-project-18-3bn-digital-economy-for-nigeria/>
- [63] “Building on Long-Standing Cooperation to Strengthen Digital Capacity in Africa.” Accessed: Jun. 20, 2026. [Online]. Available:
<https://www.icann.org/en/blogs/details/building-on-long-standing-cooperation-to-strengthen-digital-capacity-in-africa-25-05-2026-en>
- [64] “Continued Progress in African DNS Security | ISOC Pulse.” Accessed: Jun. 20, 2026.
[Online]. Available:
<https://pulse.internetsociety.org/en/blog/2026/02/continued-progress-in-african-dns-security/>