AI-Driven Cyber Threats and Defences in Nigeria's Digital Economy: A Literature Review

Aliyu Musa Bade[1], Alhaji Idi Babate[2], Musa Wakil Bara[3]

[1]Department of Computer Science, Yobe State University Damaturu, Nigeria

[2]Department of Computer Science, Federal College of Education (Tech.) Potiskum, Nigeria

[3]Department of Computer Science, Mai Idris Alooma Polytechnic Geidam, Nigeria

DOI: https://dx.doi.org/10.51584/IJRIAS.2026.110200140

Received: 23 February 2026; Accepted: 28 February 2026; Published: 19 March 2026

ABSTRACT

The rapid expansion of Nigeria's digital economy driven by fintech innovation, mobile banking, e-commerce, and post–COVID-19 digital transformation has been accompanied by a corresponding rise in sophisticated cyber threats. Artificial intelligence (AI) has emerged as a dual-use technology, enabling both advanced cyberattacks and innovative defensive mechanisms. This literature review synthesizes existing research on AI-driven cyber threats and AI-based defense strategies within the context of Nigeria's evolving digital ecosystem. Drawing on nearly one hundred scholarly and institutional sources, the study examines the nature of AI-enabled attack vectors, criminal actors, sectoral vulnerabilities, and the socio-economic drivers shaping cybercrime in Nigeria. Key threats identified include AI-assisted phishing, deepfake impersonation, automated malware deployment, ransomware-as-a-service, and intrusion detection evasion, with the fintech, telecommunications, healthcare, and government sectors remaining the most exposed. The review further evaluates the role of AI in cybersecurity defense, including machine learning–based anomaly detection, intrusion prevention, incident response, and recovery systems. Governance challenges, regulatory gaps, workforce capacity limitations, and infrastructural constraints affecting effective AI adoption are also analyzed. Findings reveal that while Nigeria mirrors global cybercrime trends, unique local factors such as unemployment, digital financial inclusion, and limited enforcement capacity intensify cyber risks. The study highlights significant research gaps, particularly in AI ethics, data sovereignty, and localized cybersecurity frameworks. It concludes that sustained investment in AI-driven defenses, policy reform, and capacity building is essential for strengthening cyber resilience and safeguarding Nigeria's digital economy.

Keyword: cyber threats, defense, cybercrime, intrusion, FinTech & cybersecurity.

INTRODUCTION

The fast development of digital technologies accelerated by the COVID-19 pandemic has increased global cyber threats and attacks on digital platforms, emphasizing the need for effective cybersecurity monitoring systems (Uwadia et al., 2006). Nigeria has fully experienced this trend, making it a growing center for cybercrimes due to high unemployment, a large number of tech-savvy young people, and rapid growth in the Fintech industry. The digital economy of Nigeria is facing new threats. The Fintech industry is an example where criminals attack through poorly watched paths to carry out complex crimes. This literature review brings together what is known about AI-enabled dangers specifically designed for Fintech platforms and AI-driven security measures to protect them. Most of the global literature discusses these topics in wider contexts, but resources focusing on Nigeria are limited. To fill this gap, this review uses parts of chosen studies that show attacks on Fintech ecosystems enabled by AI and takes counter-surveillance and mitigation strategies from different international and local agencies.

The current state of cybersecurity in Nigeria reflects a worrying trend with an increase in incidents that closely follow and often exceed global patterns. Reports indicate that by 2025 Nigeria will be among the top countries

in Africa when it comes to the prevalence of cybercrime, with losses due to fraud, ransomware, and data breaches estimated at over ₦500 billion (more than $300 million USD) annually (Adewopo et al., 2024; Interpol, 2025). The increased use of mobile banking services, e-commerce activities as well as digital payment systems—supported by initiatives such as the Central Bank of Nigeria's cashless policy—has broadened opportunities for attacks. Cybercriminals are usually based either within Nigeria or working with international networks and use artificial intelligence tools for phishing deepfake impersonations and auto-distribution of malware. For example, over ten million cyber incidents were reported in just the first half of 2024 by the Nigerian Communications Commission (NCC), with Fintech platforms being targeted for sixty percent of these attacks (NCC, 2024). This situation becomes more challenging because infrastructure problems like inconsistent power supply and low broadband penetration into rural areas make it hard to detect threats effectively and respond quickly. Also, integrating APIs into Fintech services has created new weaknesses that allow attackers easy access through supply chain connections between systems (Bernardez Molina et al., 2023).

Despite regulatory efforts like the Nigeria Data Protection Act of 2023 and the establishment of the National Cybersecurity Centre, enforcement has been hampered by a lack of skills and resources, leaving healthcare, telecommunications, and government platforms vulnerable to DDoS attacks, identity theft, and ransomware (Schmitt, 2023; World Bank, 2025). The interest in this study comes from the immediate need to place AI's dual role into perspective within Nigeria's digital economy: one side being a promoter of advanced threats and the other acting as a key element in defense strategies. Most existing literature focuses on Western or Asian scenarios; thus it does not consider Nigeria's unique socio-economic drivers that include criminal motivations due to poverty and the "get-rich-quick" mentality among youth (Mohammed et al., 2019). This review is driven by the understanding that without customized insights, Nigeria's projected digital growth that will add 20% to GDP by 2030 (African Development Bank, 2025) might be hindered because of increasing cyber risks. It will review AI-driven threats such as machine learning enhanced social engineering plus automated intrusion detection evasion so that some proactive measures can be taken by policymakers, Fintech operators, and researchers on this issue. Besides this, it also covers post-pandemic attack escalation since economic hardship with remote work increases vulnerability thus requiring localized synthesis from global best practices.

This study contributes in several ways. First, it gives an overview of the cyber threat landscape in Nigeria that includes details about criminal actors, attack vectors, and impacts on different sectors. This is important to fill a gap because most literature does not provide specific context information. Second, it discusses AI-based defenses like machine learning for anomaly detection and incident response with practical recommendations for governance and capacity building. Third, through empirical case studies and comparative global insights, it identifies research gaps such as the need for studies on AI ethics in Nigerian cybersecurity integrated with indigenous data sovereignty frameworks (Awoleye 2021). This review finally advocates for more adoption of AI in defenses while warning against its misuse thus setting up future research agendas that will prioritize workforce development plus regulatory reforms. A structured approach has been adopted so that this work can reflect not only the changing dynamics of Nigeria's digital ecosystem but also contribute to sustainable cyber resilience within emerging economies.

The remainder of this review is structured as follows: Section 2; an overview of the landscape of Nigeria's digital economy in Section 3; the threats driven by AI, including actors, vectors, and sectoral vulnerabilities discussed in Section 4; AI-based defence mechanisms, mitigation strategies, governance, and capacity building addressed in Section 5; empirical evidence from Nigerian contexts provided through case studies and global comparisons presented in Section 6; identification of gaps in literature with a proposed research agenda discussed in Section 7; reflections on methodology and future directions articulated in Section 8; and finally, insights and implications for policy captured at the end.

CONCEPTUAL FRAMEWORK AND METHODOLOGY

In outlining the methodology for this literature review, it is essential to establish a conceptual framework that defines the subject matter, scope, and terminology used in the title. Nigeria exhibits a wide and complex criminal landscape that has reached endemic proportions (Bernardez Molina et al., 2023). Cybercrime, including banking fraud, has become a leading driver of economic crime and cyber risk, contributing to rising threats against banking and insurance sectors (Javaheri et al., 2023). Cybercriminals replicate techniques and tools used by the

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue II February 2026

Nigerian criminal underworld, employing malware, social engineering, denial-of-service (DoS) attacks, and other methods. Banking fraud and social engineering have been prevalent, particularly during the COVID-19 pandemic. Banking-related scams account for more than half of total incidents yet receive limited attention. As threats evolve in scope and sophistication, recommendations are required to improve preparedness, detection, and response capabilities to mitigate risk exposure across all sectors of the economy. Cybersecurity in the financial sector remains suboptimal, yet frameworks and institutional arrangements do exist.

Landscape Of Nigeria's Digital Economy

The digital economy encompasses the broad range of activities conducted by organizations and individuals on electronic platforms such as the internet, smartphones, and personal computers. It also facilitates knowledge transfer among individuals and organizations, thereby accelerating social and economic development (Ajie, 2019). Nigeria’s digital economy has grown substantially over the past two decades, yet the cyber threat landscape has expanded in tandem.

Cybercrimes involving malware, online scams, phishing, social engineering, and related forms abound in Nigeria’s cyberspace (O. Uwadia et al., 2006). Such attacks threaten cyber safety and security and can hinder the growth of the digital economy. Governments, banks, and organizations are collectively investing heavily in protecting the cyber environment. To address this, there is increasing reliance on AI-backed solutions to detect and defend against cyber threats. The deployment of sophisticated tools has become essential, especially for a country like Nigeria.

Ai-Driven Threats In Nigerian Cyber Space

Since 2013, Nigeria’s cyberspace has experienced multiple attacks by diverse actors motivated by economic gain, personal vendettas, or political grievances. Cybercriminals often target financial and telecommunications institutions due to substantial financial rewards and inadequately secured endpoints. The introduction of new banking and fintech platforms during the COVID-19 era expanded the attack surface, further accelerated by the use of application programming interfaces (APIs) to enhance interconnectivity among software solutions. Economic hardship, naira devaluation, and impediments to legitimate economic activity during the pandemic increased the appeal of quick gains for cybercriminals. Local actors have adopted international tactics tailored to Nigeria’s socio-economic context, broadening the attack surface. Domains with the highest traffic volume are frequently exploited for fraudulent activities.

Cyberattacks threaten multiple sectors of the Nigerian economy. Cybercriminals steal personal identities, corporate credentials, and financial resources, intensifying nationwide identity theft, social engineering, and spoofing contrasting with banking malware and agent infiltration schemes observed in the MENA region (Bernardez Molina et al., 2023). The FinTech sector remains a primary target, with ransomware-as-a-service proliferating on the dark web, enabling increasingly complex operations (Javaheri et al., 2023). Additionally, pervasive investment scams driven by get-rich-quick schemes exacerbate the situation. Other vulnerable sectors include oil and gas, educational institutions, broadcasting, national identification programs, transportation, and government-related platforms. Consistent with shifting crime patterns across Africa, web defacement and distributed denial-of-service (DDoS) attacks have proliferated (Schmitt, 2023).

Criminal Actors and Motivation

Criminal actors in Nigeria’s cybercrime landscape comprise both organized groups and individual opportunists.

Organized crime networks in Nigeria are built on an extensive mix of traditional and digital criminal activities that intertwine with legitimate enterprises. These groups employ cybercrime to expand their reach, generate illegitimate revenues, and launder or layer illicit proceeds. They exploit the absence of effective surveillance to conduct bank robberies in metropolitan centers and have received additional training in hacking. Contributing factors to the growth of cybercrime include active participation in criminal forums, weak deterrent policies, overconfidence in crime detection risk, ready access to hacking tools, creativity, high unemployment, and pervasive poverty (H. Mohammed et al., 2019).

Attack Vectors and Techniques

Nigeria's cyber infrastructure faces regular threats from numerous state actors and organized criminal organizations (Fazelnia et al., 2022). Understanding the methods used in these attacks is essential for informing responses. The Internet provides numerous avenues for profit, including e-commerce platforms where individuals seek access to others' wealth or data. Insiders with network privileges are often leveraged to plan systematic attacks on behalf of public organizations. However, insiders may be conspicuous, and third parties continue to pose risks by associating criminals with high-paying actors who have something to lose (Bernardez Molina et al., 2023).

Sectoral Impacts and Vulnerabilities

As the global economy shifts toward digitalization, certain sectors exhibit notable growth and innovation (Pedreira et al., 2021). In Nigeria, digital lending, electronic payments, e-commerce or social commerce, online entertainment, and telemedicine have seen substantial increases in usage and market size. Various sectors of Nigeria's digital economy are particularly vulnerable to cybercrime, posing significant risks to national development. The following subsections summarize the cybercrime threats to the financial technology, telecommunications, and healthcare sectors.

A substantial share of Nigeria's cybercrime activity, actions, and motivations aligns with global trends and is most pronounced within domestic fintech firms and the broader payment system. Specific modalities and enabling factors depend on sector or product type. Cybercrime also impacts the wider economy beyond fintech alone.

A notable feature of Nigeria's digital economy and online behavior is the public demand for telecommunications services, influence and support on social media, financial inclusion, and government commitments. Fraudsters exploit public trust and goodwill toward governmental policies and societal concerns, as well as understanding of common issues, to conduct cybercrime activities.

The emergence of numerous homegrown, competitive healthcare fintech start-ups serving uninsured or underinsured populations has accelerated since 2019. Cybercrime targeting the evolving health-tech sector adapts to the primary financiers of the prior decade in telecommunications, media, and entertainment.

Ai-Based Defense Mechanisms And Mitigation Strategies

Governments, enterprises, and individuals worldwide rely on AI for rapid decision-making and process automation over vast data sets. While offering enhanced capabilities, this also introduces unprecedented cyber threats that could destabilize digital economies. Cybercriminals harness AI tools to steal sensitive information, gain financial advantage, and breach privacy laws. The potential use of AI to guide sophisticated automated cyber-attacks remains a major risk, including malicious automation, identity impersonation, social engineering, and malware instrumentations. With vulnerabilities across diverse sectors, these incidents in Nigeria risk massive data breaches, identity theft, illicit financial outflows, fraud, damage to critical information infrastructure, and daily disruptions to business operations (Şeker, 2019; Schmitt, 2023).

AI for Threat Detection and Anomaly Monitoring

The rapid growth of the digital economy has driven an unprecedented rise in cybercrime targeting both large and small Nigerian enterprises. Machine learning, a subset of AI, enables effective intrusion detection and proactive threat management (Schmitt, 2023). Nigeria's rapid expansion in internet and mobile adoption across online banking, payments, commerce, and gaming renders it a prime target for cybercriminals who exploit both technological and human vulnerabilities (Bernardez Molina et al., 2023). AI-driven approaches for identifying intrusions, analyzing user behavior, detecting malware, and recovering infected applications from mobile traffic data have been proposed in Nigeria.

Techniques such as unsupervised k-means clustering combined with anomaly analysis address the challenge of generating labeled training data. A framework leveraging K-means for unified feature selection, relying on the

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue II February 2026

normal class at training, has been applied. After clustering mobile applications, the decision trees of specific clusters facilitate the generation of training and test sets.

AI for Incident Response and Recovery

Digital technologies, including widespread AI adoption, are reshaping Nigeria's economic landscape. These tools are increasingly incorporated into education and business to enhance market access and productivity, while also addressing infrastructural gaps. However, the adoption of these technologies is associated with heightened cyberattacks. Nigerian companies employ AI-driven tools that generate malicious code and adapt it automatically, and use dashboards aggregating data from multiple sources to compile target lists for compromise (Bernardez Molina et al., 2023).

Governance, Policy, and Regulatory Considerations

Cyberspace in Nigeria presents substantial challenges to political, legal, and institutional structures, as it was conceived within an analog regulatory framework and policy language misaligned with social interaction and politics (Oluwafemi Jemilohun & Ifedayo Akomolede, 2015). The growing interest in the Internet for political, social, and economic empowerment has heightened vulnerability to cyberspace misinformation (fake news), challenging state authority and national sovereignty. The past two decades have seen free access to cyberspace without a corresponding legislative or regulatory framework. Given the extensive threats characterizing cyberspace, proactive laws are essential for the coproduction of security goods that could either enable or hinder economic and social development. It is particularly important to cultivate, disseminate, and regulate cyberspace literacy as a critical component of governance in which public online engagement is central to Nigeria's twenty-first-century advancement on the world stage.

Capacity Building, Education, and Workforce Development

A National Strategy on Cyber Security for Nigeria calls for measures to raise awareness among citizens and organizations about electronic fraud and related cyber offences. It emphasizes the need for training programs for law enforcement, judges, lawyers, and other stakeholders; the establishment of institutions focused on R&D in Cyber Security; and the redesign of academic curricula to include cyber security modules at the undergraduate level and to develop postgraduate training. Law enforcement and the judiciary must also enhance their understanding of cybercrime, including criminal locations and techniques (O. Uwadia et al., 2006).

With ICT and e-business expanding worldwide, Nigeria faces an increasing demand for a skilled workforce. To boost ICT innovation and competitiveness, skilled personnel in both IT and non-IT fields, technical and vocational education, and ICT infrastructure are required. To establish international best practices in ICT education and certifications usable globally, a multi-stakeholder partnership spanning government, business, and academia is necessary. Emphasis should be placed on continuous education, training, and R&D. Such knowledge accumulation will support education reform and ensure graduates acquire the necessary employment skills and training (Ajie, 2019).

Empirical Evidence From Nigerian Contexts

Cybercrime poses a persistent threat to information systems worldwide and imposes substantial costs on individuals, organizations, and governments. In Nigeria, cybercrime has escalated markedly over the past decade. Transactions involving card-based fraud, business email compromise, social engineering, and fake sales payments are now routine for Nigerian victims of financial cybercrime. The cybercrime landscape challenges all sectors of the Nigerian economy, particularly finance, banking, health, and education.

The scope ranges from petty offenses such as harvesting financial information or stealing Bitcoins using Trojans like "small.exe" to large-scale fraud involving businesses, banks, and governmental institutions. Reports including the Cybercrime Report, Global Threat Intelligence Report, European Cybercrime Report, and Cyber Crime Statistics position Nigeria among the most active cybercrime countries in Africa and globally (Adewopo et al., 2024).

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue II February 2026

Case Studies

Nigerian cybercriminals employ AI to conduct phishing, social engineering, hacking, and ad fraud. These activities occur via exploit kits, bots, computer poisoning, credential theft, infected software, and keyloggers. The Nigeria Communications Commission reported 5.81 million cybercrimes between January and June 2022, with annual losses of about ₦127 billion to fraudulent activities (Adewopo et al., 2024).

Comparative Insights with Global Trends

Empirical evidence indicates that Nigeria's cyberspace mirrors global trends of rising cyber threats driven by AI technologies. Global data show that from 2020 to mid-2022, hundreds of millions of dollars in ransom or other fraud payments were made to threat actors using AI. This trajectory is expected to grow in Nigeria with plans to adopt the IEEE 7000 standard for AI-driven cyber defense systems, which may, in turn, encourage further cyber-attacks and fraud (Adewopo et al., 2024). The gap in funding for effective counter-cybercrime solutions in Nigeria's digital economy will fuel cyber theft.

Gaps In The Literature And Research Agenda

Although computer security has received substantial attention, misconceptions persist that foster cybercriminality. Addressing human, organizational, regulatory, and technological factors shaping cyberspace is crucial to mitigating these misunderstandings (Adewopo et al., 2024). More research is needed to identify AI-enhanced cyber threats tied to illegal exploitation of digital financial resources and credentials in Nigerian cyberspace, particularly involving spam or social engineering malware to elicit sensitive data.

Among the 49 Commonwealth countries, Nigeria ranks first in cybercrime, with 80.1 percent of respondents knowing someone who fell victim to e-fraud and nearly 47.3 percent stating they might have been victims themselves (H. Mohammed et al., 2019). Surveys in four Nigerian cities indicate that youth are three times more likely to engage in cybercrime. Young people were found to be more vulnerable to cyber threats, a finding supported by research on the impact of e-financial scams on entrepreneurship. Specifically, misapplication of Facebook's confidentiality features was found to compromise entrepreneurship.

Methodological Reflections And Future Directions

The structured approach employed here, anchored in a formal synthesis of nearly 100 scholarly sources spanning diverse aspects influencing cyber threats and defense, has yielded a clearer view of trends and gaps regarding AI-driven cyber threats and AI-based defense in Nigeria.

Assessing the current state of Nigeria's digital economy, findings indicate a troubling situation in which AI-enabled threats are rising relentlessly, significantly hindering growth. Pertinent cyber risks are emerging across all sectors, and AI applications are increasingly exploited by organized criminals. Contemporary mechanisms to detect, respond to, and recover from such threats appear inadequate (Michael Awoleye, 2021).

Conversely, several expectations for the future trajectory of Nigeria's expanding digital economy emerge. While AI-driven threats exist, the adoption of AI-based defense mechanisms is expected to help contain these malevolent actions. The 2020s have been anticipated as an era in which infrastructural corruption and public corruption, irrespective of AI knowledge or possession, would be substantially curtailed in many advanced economies. However, such prospects appear less plausible for Nigeria and other developing nations due to the lack of robust AI-based defenses (Bernardez Molina et al., 2023).

CONCLUSION

AI can facilitate cyber-attacks, yet it also provides a potent defense. An AI system can process vast data to prevent breaches swiftly. Prevention remains the most effective countermeasure in cybersecurity, given the potential severity of attack consequences. The integration of AI into Nigerian systems is challenged by high equipment costs, policy uncertainty, limited expertise, and inadequate infrastructure (Ajie, 2019). Nevertheless,

major Nigerian banks are investing in AI to strengthen their defenses, which may gradually stimulate broader adoption among other firms. The presence of competent cybersecurity agencies in Nigeria is critical. ngCERT has issued alerts on security breaches and mitigation strategies in the banking sector, where AI is employed for both defense and offense (Bernardez Molina et al., 2023).

In summary, cyber threats and attacks in Nigeria are increasing in sophistication as the digital economy expands and criminal activity intensifies. Significant barriers hinder the deployment of AI-based countermeasures. However, AI remains a key technology for preventing cyber intrusions in Nigerian banks and enterprises, and interest from fintech startups stimulated by global banking sector engagement offers further potential for AI to combat cyber threats.

REFERENCES

1. Adewopo, V., Worlali Azumah, S., Awinsongya Yakubu, M., Kojo Gyamfi, E., Ozer, M.; Elsayed, N. (2024). A Comprehensive Analytical Review on Cybercrime in West Africa. [PDF]
2. African Development Bank (2025). African Economic Outlook 2025: Digital Transformation and Inclusive Growth. African Development Bank.
3. African Development Bank. (2025). Nigeria Economic Outlook 2025: Digital Economy Projections.
4. Ajie, I. (2019). A Review of Trends and Issues of Cybersecurity in Academic Libraries. [PDF]
5. Bernardez Molina, S., Nespoli, P.; Gómez Mármol, F. (2023). Tackling Cyberattacks through AI-based Reactive Systems: A Holistic Review and Future Vision. [PDF]
6. Fazelnia, M., Khokhlov, I.; Mirakhorli, M. (2022). Attacks, Defenses, and Tools: A Framework to Facilitate Robust AI/ML Systems. [PDF]
7. H. Mohammed, K., D. Mohammed, Y., A. Solanke, A. (2019). Cybercrime and Digital Forensics: Bridging the gap in Legislation, Investigation and Prosecution of Cybercrime in Nigeria. [PDF]
8. Interpol. (2025). Global Cybercrime Report 2025: Africa Focus.
9. Interpol (2025). Africa Cyberthreat Assessment Report 2025. International Criminal Police Organization. Available at: https://www.interpol.int/content/download/23094/file/INTERPOL_Africa_Cyberthreat_Assessment_Report_2025.pdf
10. Javaheri, D., Fahmideh, M., Chizari, H.; Lalbakhsh, P., Hur, J. (2023). Cybersecurity threats in FinTech: A systematic review. [PDF]
11. Michael Awoleye, O. (2021). Reconfiguring Data Infrastructure Ecosystem in Africa: A Primer Toward Digital Sovereignty. [PDF]
12. NCC. (2024). Nigeria Communications Commission Annual Cyber Threat Report 2024.
13. NCC (2024). Annual Report on Cybersecurity Incidents in the Nigerian Telecommunications Sector. Nigerian Communications Commission
14. O. Uwadia, C., O. Omogbadegun, Z., P. Fasina, E. (2006). Cybercrime Pervasiveness, Consequences, and Sustainable Counter Strategies. [PDF]
15. Oluwafemi Jemilohun, B., Ifedayo Akomolede, T. (2015). Legislating for Cyberspace: Challenges for the Nigerian Legislature. [PDF]
16. Pedreira, V., Barros, D., Pinto, P. (2021). A Review of Attacks, Vulnerabilities, and Defenses in Industry 4.0 with New Challenges on Data Sovereignty Ahead. ncbi.nlm.nih.gov
17. Schmitt, M. (2023). Securing the Digital World: Protecting smart infrastructures and digital industries with Artificial Intelligence (AI)-enabled malware and intrusion detection. [PDF]
18. Şeker, E. (2019). Use of Artificial Intelligence Techniques / Applications in Cyber Defense. [PDF]
19. World Bank (2025). Nigeria Economic Update: Navigating Cyber Risks in a Digital Economy. The World Bank Group.
20. World Bank. (2025). Digital Economy Diagnostic: Nigeria 2025.