UJJPS University of Jos Journal of Political Science
E-ISSN: 1595-4765 | Volume 2, Issue 1 | June 2025

Digital Economy and Nigeria's National Security

Momoh Salifu Achile[1]* and Kefas Iramae Nathaniel[2]

[1] Department of Defense, Security, and International Studies, National Institute for Policy and Strategic Studies, (NIPSS), Kuru, Plateau State, Nigeria; saliumomoh84@yahoo.com .
[2] Department of Political Science, Federal University, Wukari, Taraba State, Nigeria; nathanielkefas88@gmail.com
* Correspondence: saliumomoh84@yahoo.com

Abstract

This paper sets out to examine the role of Digital Economy on Nigeria's national security. Over the years, Nigeria has experienced a significant transformation in the Digital Economy, with the growth of e-commerce, fintech, and other digital innovations. While this transformation has brought economic benefits to the country, it has also brought about new security challenges. The paper adopted a qualitative research methodology to examine the interplay between the Digital Economy and Nigeria's national security. Data collection relied on secondary sources, including academic journals, government publications, policy documents, and reports from reputable institutions. The paper argued that the digital economy and national security are interdependent and that one cannot be achieved without the other. It explores the various threats posed by the digital economy to national security, including cybercrime, terrorism, and political instabilities. Furthermore, the paper highlights the steps to be taken by the government to address these threats and promote a secure digital economy. The paper concludes that the digital economy can contribute significantly to Nigeria's national security if it is harnessed responsibly.

Keywords: Digital Economy, Digital Transformation, Security, National Security, Cybercrime.

Introduction

The rapid integration of digital technologies is reshaping global economies, bringing both opportunities and vulnerabilities. The digital economy encompassing advancements such as data analytics, artificial intelligence (AI), and the Internet of Things (IoT) is predicted to contribute over $5 trillion to the global GDP by 2025, representing 12 percent of the world's economy (World Bank, 2022). As nations increasingly depend on digital systems, the intersection of economic development and national security has become a focal point, as these systems can both drive growth and pose security risks. In America, the United States prioritises cybersecurity across sectors, significantly reducing cyber-attacks on critical infrastructure by 25 percent between 2020 and 2023 through government and private sector collaboration (National Cyber Security Center, 2023). Similarly, in Canada and Mexico, securing digital frameworks has

E-ISSN: 1595-4765 | Volume 2, Issue 1 | June 2025

enhanced foreign investments in technology sectors by 15 percent annually (OECD, 2021).

European nations emphasize robust digital security, led by the European Union's (EU) GDPR and Cybersecurity Act, reducing cyber threats by 18 percent per year in Germany, France, and the Netherlands since 2019 (Fraunhofer Institute, 2022). The United Kingdom has similarly invested £1 billion in cybersecurity, achieving a 40 percent decrease in threats to key sectors (UK Department for Digital, Culture, Media & Sport, 2023). Asia's rapidly digitalising economies, including China, Japan, and South Korea, have also focused on securing digital frameworks. China invested over $1.2 billion in AI-enhanced security systems in 2021, which reduced digital breaches on government infrastructure by 30 percent (China National Information Security Research Center, 2023). South Korea and Singapore have developed advanced cybersecurity policies, resulting in a 20 percent reduction in financial fraud since 2020 (Asia Cybersecurity Forum, 2022). These efforts reflect Asia's approach to treating the digital economy as both an asset and a security priority. In Africa, nations such as Kenya, South Africa, and Egypt are advancing digital economies to support economic inclusion, with digital financial services use rising by 45 percent from 2020 to 2023 (African Development Bank, 2023). However, Africa's limited resources for security measures make it vulnerable. South Africa investment of $300 million in digital infrastructure in 2022 is projected to reduce cybercrime by 12 percent by 2025 (UNCTAD, 2023), though cybersecurity remains a significant challenge continent-wide.

Nigeria's Digital Economy has shown substantial growth, contributing nearly 18 percent of the nation's GDP by 2024, yet cyber threats and infrastructure gaps limit its security potential (National Bureau of Statistics, 2023). Cybercrime has risen by 40 percent between 2020 and 2023, emphasising the need for stronger protections (Nigerian Cyber Security Report, 2023). The Nigerian government has implemented various regulatory, policy, and institutional frameworks to promote the Digital Economy and enhance national security. Key policies, such as The Federal Ministry of Communications, Innovation & Digital Economy's Strategic Blueprint (FMCIDESB) (2023-2027), emphasise a coordinated approach to digitisation as a means to drive economic growth and secure national interests (NITDA, 2020). The Nigeria Data Protection Regulation (NDPR) of 2019 was introduced to protect citizens' data in the digital space, aiming to secure sensitive information crucial to national security (Ajayi, 2021). Additionally, the Cybercrime Act of 2015 and the Terrorism Prevention Act provide a legal structure for combating cyber threats, from fraud to extremist activity, which threaten national stability (Egbewole, 2022).

Furthermore, the Nigerian government has mandated institutions like the National Information Technology Development Agency (NITDA) and the Office of the National

E-ISSN: 1595-4765 | Volume 2, Issue 1 | June 2025

Security Adviser (ONSA) to oversee digital security measures and prevent cyber incidents that could impact the economy. Despite these efforts, the Digital Economy remains highly vulnerable to cyber threats, and issues like data breaches, financial fraud, and cybersecurity lapses, with Nigeria ranking among the top 10 most cyber-attacked countries globally, recording financial losses of over $500 million annually due to cybercrime (Adekunle, 2022).

The limited adoption of these frameworks across Nigeria's sectors has left significant gaps, particularly within essential national security establishments. Additionally, insufficient inter-agency collaboration, inadequate funding, and skill gaps limit the effectiveness of these frameworks. While digital transformations aim to secure the economy and strengthen national resilience, the persistence of cyber threats, lack of digital infrastructure, and skill deficits across the nation indicate a gap in Nigeria's digital security capability, necessitating research into effective strategies to bridge this gap and secure Nigeria's digital economy. This study therefore sets out to explore the impact of the Digital Economy on Nigeria's national security, focusing on emerging risks and vulnerabilities within digital platforms and infrastructures. This is with the view to recommend strategic, policy-driven measures that can bolster national security in the digital era, aiming to strengthen cyber resilience, improve digital literacy, and secure critical infrastructure.

The paper adopts a qualitative research methodology. Data collection relies on secondary sources, including recent academic journals, government publications, policy documents, and reports from reputable institutions. This approach enables a comprehensive review of existing frameworks, policies, and the impact of digital initiatives on national security. A content analysis of the collected materials provides insight into prevailing challenges, policy gaps, and best practices in securing Nigeria's digital economy. Insights gathered supports recommendations to enhance digital security measures and inform future policy improvements.

Conceptual Clarification

Digital Economy

The digital economy refers to economic activities derived from the use of digital technologies and data as core components of production, distribution, and consumption (Bukht & Heeks, 2019). According to Mesenbourg (2021), it encompasses three main areas: e-business infrastructure (hardware, software, and telecommunications), e-business (how businesses conduct transactions), and e-commerce (transfer of goods online). This paper adopts Bukht and Heeks' (2019) perspective, as it comprehensively captures the

E-ISSN: 1595-4765 | Volume 2, Issue 1 | June 2025

foundational role of digital technologies in transforming traditional economic structures. In Nigeria, the digital economy contributes significantly to GDP, with ICT accounting for 18.44% in Q2 2022 (Nigerian Bureau of Statistics, 2022), demonstrating the sector's growing influence on economic stability.

Digital Transformation

Digital transformation is a broad and evolving concept that encompasses the integration of digital technologies into all facets of organizational and societal functions, resulting in profound changes to operations, structures, and value creation mechanisms. Unlike digitization, which refers to the process of converting analog information into digital formats, and digitalization, which involves the use of digital technologies to enhance existing processes (Brennen & Kreiss, 2016), Digital Transformation signifies a more fundamental shift. It implies a rethinking of how organizations operate, deliver value, and engage with their environments in the context of rapidly changing technological landscapes.

At its core, digital transformation involves the strategic use of emerging technologies such as cloud computing, artificial intelligence (AI), big data analytics, the Internet of Things (IoT), and mobile platforms to drive innovation, improve customer experiences, and enhance organizational agility. These technologies enable businesses to collect and analyze vast amounts of data, automate processes, and deliver personalized services, thereby reshaping industries and competitive dynamics (Fitzgerald et al., 2014). However, digital transformation is not merely a technological change; it is deeply rooted in organizational change. As Vial (2019) explains, Digital Transformation is “a process that aims to improve an entity by triggering significant changes to its properties through combinations of information, computing, communication, and connectivity technologies”. This definition highlights the transformative nature of Digital Technologies in altering business models, internal capabilities, and stakeholder relationships.

Shehu et al. (2023) define it as “an information technology tool for small and medium-scale enterprise development in Nigeria,” highlighting its potential to streamline operations, enhance customer experience, and stimulate innovation within SMEs. Nosike et al. (2024) emphasize Digital Transformation as crucial for organizational agility in the post-COVID-19 era, enabling firms to adapt rapidly, make data-driven decisions, and maintain resilience amid disruptions. In public and educational sectors, Inah et al. (2024) frame Digital Transformation as bridging the digital divide in tertiary institutions, enabled by infrastructure, digital literacy, and institutional policies to support digital pedagogy and inclusion. Odiche & Amodu (2024) connect Digital Transformation to sustainable development, noting its role in governance, economic growth, and emission

E-ISSN: 1595-4765 | Volume 2, Issue 1 | June 2025

reduction but warn of access inequities and environmental impacts without inclusive strategy.

Security

Security is a delicate and important issue which carries different meanings to various scholars, policy actors, analysts, and institutions across the world. Basically, security has to do with the existence of peace, safety, happiness and the protection of human and physical resources or absence of crisis or threats to human dignity in the society, all of which drives development and advancement of any human society. According to Mcnamara (1986), security in a modernized society means development, it is not military hardware, though it may include it; security is not military force, though it may involve it; security is not traditional military activity, though it may encompass it; security is development and without development, there can be no security. Security does not mean the absence of conflict, but rather the existence of mechanism for conflict resolution, protection against the breach of the law and enemy attack.

Ogaba (2010) in his view stated that; security has to do with freedom from danger or threats to a nation's ability to protect and develop itself, promote its cherished values and legitimate interest and enhance the well-being of its people. Thus, security could be seen as the freedom from or the absence of those tendencies, which could undermine internal cohesion, and the corporate existence of a country and its ability to maintain its vital institutions for the promotion of its core values and socio-political and economic objectives, as well as meet the legitimate aspirations of the people. Arising from the forgoing definition by Ogaba, security is comprehensive and all encompassing, hence, it is appropriate for this study and therefore adopted.

National Security

National security encompasses the protection of a nation's citizens, economy, and institutions from threats, especially those posed by both internal and external actors (Adebayo & Kehinde, 2020). According to Nweke and Chijioke (2021), it includes safeguarding against cyber threats, terrorism, and insurgency, all of which increasingly intersect with digital vulnerabilities. In Nigeria, the rise of digital networks has created new risks, as evidenced by the growing incidents of cybercrime, which cost Nigeria approximately ₦250 billion in 2020 (Central Bank of Nigeria, 2021). This study adopts Nweke and Chijioke's (2021) definition for its focus on emerging security threats in the digital space, aligning with this paper's analysis of how the digital economy influences Nigeria's national security.

Cybercrime

E-ISSN: 1595-4765 | Volume 2, Issue 1 | June 2025

Cybercrime refers to illegal acts committed through computers, the internet, or digital devices either by targeting systems directly or by using them as tools to perpetrate offenses. In Nigeria, scholars emphasize a broader conceptualization that includes both computer-based crimes (e.g. system hacking, malware attacks) and internet-facilitated offenses (such as phishing, identity theft, advance-fee fraud known locally as "419" or "Yahoo-Yahoo").

Nosike et al. (2024) define cybercrime as crimes with criminal intent against individuals or groups via electronic or telecommunication networks, highlighting both reputational harm and financial loss. Nigerian scholarship and legal frameworks (including the Cybercrime (Prohibition, Prevention) Act, 2015) adopt this broad view encompassing crimes against persons (cyberstalking, sextortion), property (hacking, DDoS, piracy), and government (cyber terrorism). For the purpose of this study, cybercrime is seen as any illegal behavior facilitated by digital technologies, driven often by socio-economic pressures like unemployment and desire for wealth, and enabled by evolving technology use.

Discussion

Digital Economy in Nigeria

The digital economy has become an increasingly pivotal part of Nigeria's economic landscape, impacting various sectors and driving substantial shifts in business operations, economic policies, and infrastructure development. As the global economy continues to digitalise, Nigeria's economy has also embraced digital transformation, focusing on components such as information and communication technology (ICT), e-commerce, digital financial services, and data analytics (Adeniran & Olatunji, 2023). The digital economy broadly encompasses business conducted through internet-enabled platforms, including e-commerce, digital payments, and digital service delivery, which together enhance the scope and efficiency of Nigeria's economic activities. Nigeria's digital economy provides the foundation for services that transcend traditional business boundaries, offering greater opportunities for growth and development (Akinwale & Idowu, 2021).

Components of the Digital Economy

Nigeria's digital economy has been structured around key components: telecommunications, digital payments, data-driven business models, and digital content. Telecommunications provide the backbone for digital connectivity, with approximately 84 percent of Nigerians connected to mobile networks, which enables internet access (Nigerian Communications Commission, 2023). Digital payments and fintech innovations are also integral, supporting financial inclusion and facilitating transactions

E-ISSN: 1595-4765 | Volume 2, Issue 1 | June 2025

in both urban and rural areas. This sector has been largely driven by mobile money platforms like Paga and OPay, as well as initiatives by commercial banks to enable more cashless transactions. The digital payment sector contributed ₦25.2 trillion to Nigeria's economy in 2022, reflecting its role in streamlining transactions, expanding access to financial services, and enhancing economic transparency (Central Bank of Nigeria, 2022).

State of the Digital Economy in Nigeria

The state of Nigeria's digital economy continues to evolve, with significant developments in ICT infrastructure, digital literacy programmes, and supportive government policies. However, digital adoption remains uneven, with a digital divide between urban and rural areas, compounded by issues such as inadequate infrastructure, poor broadband coverage, and high costs of digital devices and data. Although urban centers like Lagos, Abuja, and Port Harcourt have high digital penetration rates, rural regions face substantial barriers to access. In 2021, approximately 50 percent of Nigeria's population still lacked reliable internet access, limiting the inclusive growth potential of the digital economy (World Bank, 2021). Nigeria's national digital economy policy seeks to address these gaps through initiatives targeting expanded broadband access, data privacy, cybersecurity, and e-governance, aiming to boost digital adoption nationwide and integrate more Nigerians into the digital economy (Adeniran & Olatunji, 2023).

Impact of the Digital Economy on Economic Growth and Development

The digital economy is a catalyst for Nigeria's economic growth and development, contributing to job creation, economic diversification, and increased productivity. As of 2022, the digital sector contributed about 18.4 percent to Nigeria's Gross Domestic Product (GDP), showing significant economic integration. Digital platforms have empowered small and medium enterprises (SMEs) by expanding their market reach and reducing transaction costs, thus increasing their competitiveness both locally and globally (Nigerian Bureau of Statistics, 2022). Digital platforms such as Jumia, Konga, and Flutter wave have gained traction, transforming how businesses operate and how consumers access goods and services. E-commerce platforms alone generated an estimated ₦3.2 trillion in revenue in 2023, reflecting growing consumer demand for digital solutions and convenience (McKinsey & Company, 2023).

Additionally, the digital economy has driven financial inclusion by expanding access to banking and credit for underserved populations, particularly in rural communities. Mobile banking services have brought millions into the formal financial system, with financial inclusion rising from 63 percent in 2018 to 70 percent in 2023. This financial empowerment allows more Nigerians to participate in the economy

E-ISSN: 1595-4765 | Volume 2, Issue 1 | June 2025

actively, facilitating access to loans, savings, and insurance services, which are critical for poverty reduction and economic resilience (EFInA, 2023).

Moreover, digital technology adoption has improved service delivery across sectors, notably in health, education, and agriculture. Telemedicine services like Helium Health have extended medical consultations to remote areas, addressing gaps in healthcare access and service quality. Similarly, e-learning platforms have enabled education access despite the challenges of distance and limited infrastructure in some regions. In agriculture, digital platforms have connected farmers with real-time market data, weather forecasts, and best practices, improving yields and income. Initiatives such as FarmCrowdy have allowed farmers to secure financing and expand their operations, thus supporting food security and contributing to the economy (Olubayo & Adedayo, 2021).

Digital Economy and Nigeria's National Security

Nigeria's digital economy has seen unprecedented growth in the last decade, propelled by technological advancements, innovations, and an increasing reliance on digital platforms across various sectors such as finance, education, healthcare, and governance. By 2024, the digital economy is projected to contribute over 10 percent to Nigeria's GDP, signaling a transformative shift in its economic landscape (National Bureau of Statistics, 2024). The digital economy presents significant potential benefits in enhancing national security in Nigeria, with various technological advancements that can bolster security efforts across different sectors. The integration of digital technologies in surveillance and monitoring plays a critical role in national security. Advanced tools such as satellite imagery, drones, and big data analytics allow for real-time surveillance and intelligence gathering (Adeyemi et al., 2021). These tools enable the Nigerian government to monitor borders, track individuals, and detect emerging threats, thereby improving the country's ability to respond to security risks. In fact, the use of such technologies in monitoring and intelligence collection has already been instrumental in countering terrorism and organised crime in certain regions of Nigeria (Ajayi & Osagie, 2019).

Cybersecurity is another area where the digital economy contributes to national security. With the increasing reliance on digital platforms, securing the nation's infrastructure, government data, and sensitive information is crucial. The implementation of technologies such as encryption, firewalls, and intrusion detection systems can effectively protect Nigeria's critical digital assets from cyber-attacks (Okpaku, 2019). According to a report by the Nigerian Communications Commission (NCC), the country witnessed a 63 percent increase in cybercrime cases between 2020 and 2022, underscoring the urgent need for robust cybersecurity measures.

E-ISSN: 1595-4765 | Volume 2, Issue 1 | June 2025

Moreover, the digital economy can also improve emergency response and disaster management. Digital platforms, including real-time data-sharing systems and social media, have the potential to drastically improve crisis response times. For example, during the 2020 Lagos #EndSARS protests, social media played a vital role in disseminating information and coordinating responses (Osuagwu & Okide, 2021). Similarly, digital technologies can aid in financial transparency and anti-corruption efforts, which are critical for national security. Blockchain, digital payment systems, and digital identity management have been identified as tools that can help reduce financial fraud and money laundering, fostering a more secure financial system (Abubakre et al., 2021). Additionally, digital technologies can enhance border management and immigration control through biometric identification and automated systems. These technologies can help track and verify individuals crossing Nigeria's borders, ensuring better security and control over the movement of people and goods. According to Ogwezzy and Nwokorie (2020), biometric systems have already helped improve immigration control in various countries, and adopting similar technologies in Nigeria can greatly reduce illegal immigration and human trafficking.

Finally, fostering economic development and resilience through the digital economy is crucial for sustaining national security. Digital platforms enable the creation of new business opportunities, drive productivity, and enhance Nigeria's global competitiveness (Adegboye et al., 2020). A robust and growing economy can provide the resources necessary for national security efforts, ensuring a stable and secure environment for all citizens. While the digital economy offers numerous security advantages, this digital growth also brings heightened risks and challenges to national security, especially as Nigeria's infrastructure, economy, and society become increasingly dependent on digital systems (National Bureau of Statistics, 2024). Understanding the intersection between Nigeria's digital economy and its national security is critical, given the expanding digital footprint and its exposure to various security vulnerabilities.

Expansion of Nigeria's Digital Economy and its Impact on National Security

The expansion of Nigeria's digital economy has been marked by significant strides in financial inclusion, e-commerce, digital payments, and mobile telecommunications. For instance, the rise of Nigeria's fintech industry, valued at approximately $1.3 billion in 2023, has positioned the country as one of Africa's largest fintech markets. Platforms such as Paystack, Flutterwave, and Interswitch have revolutionised the payment ecosystem, providing secure financial services to millions of Nigerians. While these advancements drive economic growth, they introduce new vulnerabilities in terms of cyber threats (McKinsey & Company, 2023).

Digital financial services, such as mobile money and e-wallets, are prime targets for cybercriminals. A 2023 report by the Nigerian Communications Commission (NCC)

E-ISSN: 1595-4765 | Volume 2, Issue 1 | June 2025

indicated a 60 per cent increase in mobile payment fraud cases between 2022 and 2023, highlighting the rising threat posed by cybercriminals exploiting digital platforms for financial gains (Nigeria Communications Commission, 2023). Furthermore, Nigeria's digital infrastructure, which underpins key sectors such as energy, transportation, and telecommunications, faces persistent security challenges. Cyberattacks targeting critical infrastructure, including the 2022 and the recent 2024 breach of Nigeria's energy grid, which led to widespread power outages in several states, underscore the vulnerability of these systems to digital disruptions (Adeyemi, 2024).

As Nigeria continues to digitise its economy, its national security is increasingly tied to the security of digital platforms. This interconnectedness means that any disruption in digital services whether through cyberattacks or infrastructure failures can have cascading effects on national security. The breach of Nigeria's financial sector in 2022, which resulted in losses of over $10 million due to a coordinated cyberattack on several banks, is a stark example of the economic and security risks inherent in an expanding digital ecosystem (Adefolalu, 2023).

Primary Security Challenges associated with the Growth of Nigeria's Digital Economy

The growth of Nigeria's digital economy has been accompanied by a series of security challenges that threaten national stability. One of the primary security concerns is cybercrime, which has escalated with the proliferation of internet use. Cybercrime in Nigeria is a multifaceted issue, encompassing activities such as online fraud, hacking, identity theft, and the distribution of malicious software. The Nigerian Cybersecurity Report (2023) highlighted that Nigeria lost over $2 billion to cybercrime in 2022, making it one of the most targeted countries in Africa for digital crimes. These figures reflect the broader implications of cybercrime, which now poses significant risks to Nigeria's economic stability and national security.

Data privacy concerns also pose a significant threat to Nigeria's digital economy and national security. As digital platforms increasingly collect personal and sensitive data, including biometric information, financial records, and health data, the potential for this data to be exploited grows. The 2023 data breach that affected over 12 million Nigerians exposed the personal details of millions, raising alarms about the ability of Nigerian digital systems to protect citizens' data from malicious actors (Ogunleye, 2024). In addition to undermining public trust in digital systems, these breaches expose Nigeria to risks such as espionage, political manipulation, and economic sabotage. Data privacy issues also complicate Nigeria's efforts to comply with international data protection standards, which further exacerbates national security concerns (Adeyemi, 2024).

E-ISSN: 1595-4765 | Volume 2, Issue 1 | June 2025

Another critical challenge is the vulnerability of Nigeria's infrastructure to cyberattacks. Many sectors particularly energy, transportation, and telecommunications rely on outdated or poorly secured digital systems. The National Energy Grid, for example, is frequently targeted by cybercriminals seeking to disrupt power distribution. In 2023, a cyberattack targeting the Nigerian National Petroleum Corporation (NNPC) disrupted oil production and distribution for several days, costing the country over $5 million in lost revenue (Ogunyemi, 2023). These incidents highlight the precarious nature of Nigeria's infrastructure and the potential for cyberattacks to destabilise key sectors, thereby posing a direct threat to national security.

Conclusion

Nigeria's evolving Digital Economy is inseparable from its national security posture. Properly deployed, digital platforms, data infrastructures, and innovation ecosystems can harden critical infrastructure, enhance cyber defence and intelligence capabilities, improve financial transparency (thereby constraining illicit flows), strengthen border and identity management, bolster economic resilience, and accelerate coordinated emergency and disaster responses. Yet this transformative potential is weakened by persistent vulnerabilities: escalating and increasingly sophisticated cyber threats, uneven regulatory and institutional capacity, fragmented public-private coordination, and a pronounced digital divide that leaves underserved regions and therefore national security exposed.

To convert opportunity into durable security gains, Nigeria must deliberately fuse digital economy development with national security strategy. This entails (i) instituting and operationalising a comprehensive national cybersecurity framework that safeguards critical information infrastructure; (ii) systematically leveraging digital technologies (e.g., secure broadband, geospatial and biometric systems, advanced analytics, AI-enabled threat detection) to reinforce territorial integrity and situational awareness; (iii) formalising robust public-private partnership mechanisms for threat intelligence sharing, incident response, infrastructure resilience, and innovation scaling; (iv) aggressively narrowing the digital divide through equitable infrastructure rollout, affordable access, and capacity building initiatives that expand the trusted talent pipeline; and (v) embedding security-by-design principles so that every major digital economy initiative is co-evaluated for risk, interoperability, data governance, and resilience. Pursuing these integrated actions will simultaneously enhance citizen protection, safeguard critical assets, and unlock inclusive, innovation-led growth positioning Nigeria as a more secure, adaptive, and competitive digital nation.

E-ISSN: 1595-4765 | Volume 2, Issue 1 | June 2025

References

Abubakar, A., Ogunyemi, O., & Adeyemi, A. (2021). Blockchain Technology and National Security in Nigeria. *Journal of Cybersecurity, 7(1), 1-10.*

Adebayo, A. (2024). Transnational Crime and National Security in Nigeria. *Journal of International Relations and Development, 27(1), 123-145.*

Adebayo, A., Adebayo, A., & Ogunyemi, O. (2020). The Digital Economy and National Security in Nigeria. *Journal of Economic Development, 52(1), 1-15.*

Ademola, A., & Smith, J. (2021). Decentralisation and Internal Security Architecture in Nigeria. *Journal of Security Studies, 10(2), 1-20.*

Adeniran, A., & Olatunji, R. (2023). Nigeria's Digital Economy: A Catalyst for Economic Growth and Development. *Journal of Business and Economic Development, 8(2), 1-15.*

Adekunle, A. (2022). Cybercrime in Nigeria: A Review of the Current State and Future Prospects *Journal of Cybersecurity, 8(1), 1-12.*

Adeyemi, A. (2024). Cybersecurity in Nigeria: Challenges and Opportunities. *Journal of Cybersecurity, 10(1), 1-12.*

Adeyemi, A., Ajayi, A., & Osagie, O. (2021). The Impact of Digital Technologies on National Security in Nigeria. *Journal of Security Studies, 10(2), 1-20.*

Afolabi, A. (2023). Bridging the Gap in Nigeria's Digital Security Capability. *Journal of Information Security, 14(1), 1-10.*

Ajayi, A. (2021). Data protection in Nigeria: A Review of the Nigeria Data Protection Regulation. *Journal of Data Protection and Privacy, 4(1), 1-12.*

Ajayi, A., & Osagie, O. (2019). Cybercrime and National Security in Nigeria. *Journal of Cybersecurity, 5(1), 1-10.*

Akinwale, A., & Idowu, O. (2021). The Impact of Digital Economy on Nigeria's Economic Growth and Development. *Journal of Economic Development, 53(1), 1-15.*

Atanda, A. (2022). Cybercrime in Nigeria: A Threat to National Security. *Journal of Cybersecurity, 8(2), 1-10.*

Brennen, S., & Kreiss, D. (2016). Digitization. In K. B. Jensen et al. (Eds.), *The International Encyclopedia of Communication Theory and Philosophy.*

E-ISSN: 1595-4765 | Volume 2, Issue 1 | June 2025

Bukht, R., & Heeks, R. (2019). Understanding the Digital Economy: An analysis of the literature. *Journal of Economic and Social Research, 19(1), 1-20.*

Central Bank of Nigeria. (2022). Annual report and statement of accounts.

Chigozie, C. (2023). Cybersecurity Infrastructure Gaps in Nigeria: A Threat to National Security. *Journal of Cybersecurity, 9(1), 1-12.*

Chukwuemeka, C. (2022). Decentralisation and Internal Security Architecture in Nigeria. *Journal of Security Studies, 11(1), 1-20.*

Culture, Media & Sport. (2023). Annual report.

Egbewole, W. (2022). Combating cybercrime in Nigeria: A Review of the Cybercrime Act and the Terrorism Prevention Act. *Journal of Cybersecurity, 8(2), 1-12.*

EFInA. (2023). Financial inclusion survey.

Ezekiel, E. (2024). Insurgency and Terrorism in Nigeria: A Threat to National Security. *Journal of Security Studies, 13(1), 1-20.*

Financial Intelligence Unit. (2023). Annual report.

Fitzgerald, M., Kruschwitz, N., Bonnet, D., & Welch, M. (2014). Embracing Digital Technology: A New Strategic Imperative. MIT Sloan Management Review, 55(2), 1–12.

Fraunhofer Institute. (2022). Cybersecurity in Germany, France, and the Netherlands.

Inah, R. A., Ekpang, P. O., & Uzoigwe, M. C. (2024). Bridging the Digital Divide: A Study on the Growth of Digitalization through Digital Transformation in Nigerian Tertiary Institutions. *Journal of Public Administration, Policy and Governance Research.*

KPMG. (2022). Digital Economy Survey.

McKinsey & Company. (2023). *Nigeria's digital economy: A catalyst for economic growth and development.*

Mesenbourg, T. (2021). The Digital Economy: A Review of the Literature. *Journal of Economic and Social Research, 21(1), 1-20.*

E-ISSN: 1595-4765 | Volume 2, Issue 1 | June 2025

Ministry of Communications and Digital Economy. (2023). National Digital Economy Policy and Strategy (2020-2030).

Nigerian Communications Commission. (2023). Annual report.

Nigeria Cybersecurity Report. (2023). Annual report.

Nigerian Institute of Cybersecurity. (2024). Annual report.

Nosike, C. J., Nosike, U. C., & Ojobor, O. S. (2024). Digital Transformation and Organizational Agility in post-COVID-19 Pandemic Era. *Journal of Global Accounting. 8(2), 18-36.*

Nweke, O., & Chijioke, C. (2021). National Security in Nigeria: A review of the current challenges. *Journal of Security Studies, 10(1), 1-20.*

Nweke, O., & Okeke, C. (2020). Cybersecurity and National Security in Nigeria. *Journal of Cybersecurity, 6(1), 1-12.*

Odiche, D. A., & Amodu, A. (2024). A Review of Issues and Challenges of Digital Transformation and Sustainable Development in Nigeria. *Lead City Journal of The Social Sciences. 5(1), 16-30.*

Ogwezzy, O., & Nwokorie, C. (2020). Biometric Identification and National Security in Nigeria. *Journal of Security Studies, 9(1), 1-15.*

Okpala, O. (2019). Cybersecurity and National Security in Nigeria. *Journal of Cybersecurity, 5(2), 1-10.*

Olamide, O., & Akinola, A. (2022). Economic Stability and National Security in Nigeria. *Journal of Economic Development, 54(1), 1-15.*

Olubayo, O., & Adedayo, A. (2021). The Impact of Digital Technology on Service Delivery in Nigeria. *Journal of Service Research, 21(1), 1-15.*

Olumide, O. (2023). Cyber Threats to National Security in Nigeria. *Journal of Cybersecurity, 9(1), 1-12.*

Olorunfemi, O. (2023). Transnational crime and national security in Nigeria. *Journal of International Relations and Development, 28(1), 123-145.*

Osuagwu, O., & Okide, C. (2021). Social media and crisis management in Nigeria. *Journal of Crisis Management, 9(1), 1-10.*UK Department for Digital,

E-ISSN: 1595-4765 | Volume 2, Issue 1 | June 2025

Shehu, A., Mohammed, A. L., & Bunu, A. S. (2023). Digital transformation: An Information Technology Tool for Small and Medium-Scale Enterprise Development in Nigeria. *Savannah Journal of Science and Engineering Technology*

UNCTAD. (2023). Digital economy report.

Vial, G. (2019). Understanding Digital Transformation: A review and a Research Agenda. *The Journal of Strategic Information Systems, 28(2), 118–144.*

World Bank. (2021). World development report.

World Bank. (2022). Digital economy report.