Cybersecurity as a Pillar of Digital Sovereignty: A Scoping Review in Rethinking Governance in Nigeria and West Africa

Ezekwueme Augustine E. * and Adewumi Dolapo Sunday

Posted Date: 11 November 2025

doi: 10.20944/preprints202511.0790.v1

Keywords: telecommunication; cybersecurity; digital sovereignty; data transmission; sector dominance

 doi:10.20944/preprints202511.0790.v1

Article

Cybersecurity as a Pillar of Digital Sovereignty: A Scoping Review in Rethinking Governance in Nigeria and West Africa

Ezekwueme Augustine E. [1,*] and Adewumi Dolapo Sunday [2]

[1] University of Nigeria, Nsukka

[2] Federal University Oye Ekiti, Ekiti state

* Correspondence: augustine.ezekwueme.245033@unn.edu.ng

Abstract

This paper on Nigeria and West Africa reframes cybersecurity from a technological issue to a governance and sovereignty concern. This study uses postcolonial technology theory and institutional analysis to examine how infrastructure dependency, legal fragmentation, and foreign platform dominance make the region's digital ecosystems vulnerable to surveillance, cybercrime, and geopolitical influence. This paper examines Eurocentric digital sovereignty that promotes infrastructure autarky and hybrid governance frameworks that mix strategic autonomy and reliance. Big Tech dependence and regulatory intransigence affects state capacity, cybersecurity enforcement, and local cloud infrastructure in Kenya, South Africa, and Nigeria, according to this study. A Digital Sovereignty Index, cyber-independence plans, and ECOWAS-run infrastructure in every area are suggested. This paper proposes that Nigeria lead Africa's digital sovereignty framework with rights-based, inclusive, and decentralised cybersecurity governance. Finally, it indicates that digital sovereignty is about robust infrastructure, inventive organisational frameworks, and collaborative governance, not independence or centralisation. This study conclusions include further research recommendations to address AI governance, cross-country benchmarking, and African digital sovereignty.

Keywords: telecommunication; cybersecurity; digital sovereignty; data transmission; sector dominance

Introduction

Digital sovereignty has become a problem in international governance because it is changing how nations view their capability, legitimacy, and control in the digital era (Nanni & Santaniello, 2025). According to Bolli (2021), cyber threats, transnational data flows, and reliance on foreign infrastructure have made the once-marginal word central to strategic considerations. After the 2013 Snowden disclosures revealed Western intelligence agencies' global surveillance, digital reliance, surveillance capitalism, and extraterritorial data ownership prompted international conflict (Nanni & Santaniello, 2025). Even though most policy discourse has focused on Global North states, African governments, particularly Nigeria and West Africa, face both common and unique challenges in achieving digital sovereignty in infrastructurally constrained, externally mediated ecosystems (Jiang, 2024).

West Africa has seen digital change accelerate in the recent decade, which include but not limited to rapid growth of mobile connectivity and applications, e-governance, and online banking. However, this growth has been inconsistent due to an external technological dependent with more vulnerable to cyberattacks (Olofinbiyi, 2022). This imbalance is best illustrated by Nigeria, the region's economic leader and internet hub. Digital innovation is enhancing in education, e-commerce, and banking despite the country's dependence on foreign technologies and cybersecurity experts

 doi:10.20944/preprints202511.0790.v1

(Jiang, 2024). This dependence poses data security, infrastructural sovereignty, and monitoring political economy problems. Huawei's engagement in Nigeria's 5G infrastructure and undersea cable networks has raised concerns about technology dependence, geopolitical risk, and African states' data governance independence (Jiang, 2024).

All these worries are legitimate not just ideas, in Nigeria, phishing and ransomware attacks on financial systems is still escalating currently (Olofinbiyi, 2022). Still, the government's national response systems are inadequate, underfunded, and poorly integrated to defend these attacks. Although better than prior legislation, the 2015 Nigerian Cybercrime Act emphasises on sanctions and does little to protect key infrastructure, encourage cooperation between authorities, or promote strong public-private partnerships (Orji, 2021). The system's inconsistent enforcement and overlapping legislation are making institutions and users lose faith in Nigerian data protection authorities (Watney, 2024). Due to the lack of legal and institutional frameworks, cybersecurity is more of a strategic governance concern affecting sovereignty, rights, and development than a technical one, according to Hwang (2025).

The Economic Community of West African States (ECOWAS) has showed concern in organizing cybersecurity governance throughout the region by creating model laws and programs to help people learn more about it. But execution has been hit-or-miss, dependent on donors, and often not in line with how things really work in the area (Calandro, 2020). Several West African countries have signed the African Union's Convention on Cyber Security and Personal Data Protection. This shows that more countries are committing to digital governance, but ratification and use in their own countries are still limited (Orji, 2021). These institutional dynamics prompt pressing enquiries: Can West African nations cultivate independent cybersecurity skills without reproducing dependency frameworks? What kind of regional cooperation are possible when there are uneven resources and geopolitical conflicts?

The COVID-19 pandemic further revealed the vulnerability of digital systems throughout the region, as extensive digitisation of health, education, and commerce occurred without proportional expenses in cybersecurity awareness, literacy, or infrastructure (Bagui et al., 2023). At the same time, there are still big differences between men and women in cybersecurity education and policy engagement. Women are much less likely than males to partake in technical roles, make decisions, or get digital security training (Botha-Badenhorst & Veerasamy, 2023). This exclusion not only increases digital inequality, but it also weakens the legitimacy of government structures that say they protect national sovereignty.

The study suggests that cybersecurity should be reconceptualised as a fundamental component of digital sovereignty in Nigeria and West Africa not solely as a defensive measure, but as a strategic tool for governance, development, and the safeguarding of rights. It asserts that legal change, regional collaboration, and capacity enhancement must be integrated into a more extensive epistemic transformation that perceives cybersecurity through the framework of sovereignty, inclusion, and postcolonial justice. The paper plans to start by examining the theoretical and geopolitical discourses related to digital sovereignty. It will then take a close look at Nigeria's cybersecurity ecosystem and put these changes in the context of the larger West African area. Lastly, it will look at different policy options and governance models that could help Nigeria and its neighbours have more independent, strong, and fair control over their digital futures.

2. Conceptual and Theoretical Framework

2.1. Digital Sovereignty

Digital sovereignty can be described as way whereby the government regulate data, infrastructure, and digital standards within its own boundaries (van Dijck et al., 2018). It deals with the power to regulate digital flows, oversee platforms, and have control over infrastructure (Chander & Lê, 2015). This idea, which comes from European ideas of territorial power, doesn't work as well

 doi:10.20944/preprints202511.0790.v1

in postcolonial places like Nigeria and West Africa, where infrastructure dependency and regulatory fragmentation are common (Nanni & Santaniello, 2025).

In most African countries, less than 10% of Internet Exchange Points are run by the local government. This means that important digital infrastructure is still controlled by other countries (Belli, 2021). This reduces the independence of the country and increases the risks of intelligence gathering. Nigeria's dependence on firms such as Huawei for 5G and broadband networks highlights the geopolitical vulnerabilities inherent in infrastructural reliance (Jiang, 2024). In Africa, states face more basic problems with access to infrastructure, regulatory capacity, and cyber resilience than in Europe, where digital sovereignty debates focus on overcoming U.S. tech supremacy (Nanni & Santaniello, 2025).

South Africa's hybrid model striking a balance between openness and control over infrastructure shows the struggle between global integration and protecting national interests (Jiang, 2024). The 2021 Transnet intrusion showed even further how cyber-attacks to infrastructure put state functions at risk (Timcke et al., 2023). Hwang (2025) contends that sovereignty necessitates more than cybersecurity legislation; it requires comprehensive policymaking, local capacity enhancement, and governance coherence domains frequently lacking in Nigeria. Consequently, digital sovereignty in West Africa must transcend normative imitation and advance towards culturally relevant frameworks of self-directed digital government.

2.2. Cybersecurity Governance

Cybersecurity governance in Nigeria and West Africa illustrates the challenges of overseeing a global public good amid limited institutional capability and reliance on external resources. Nye (2010) characterises cybersecurity as a public good—non-rivalrous and incomparable, which makes its provision challenging in markets and reliant on coordinated governance. However, this kind of coordination is still hard to find in the area because institutions are not well-connected and there is inadequate funding going into technical education (Calderaro & Craig, 2020). There are legal tools like Nigeria's Cybercrime Act (2015), but enforcement is hard because different agencies don't work together well (Chaudhary, 2023).

New ideas like "cyber diplomacy" and the "sovereign cloud" have become worldwide ways to deal with cybersecurity governance. Cyber diplomacy lets countries talk about rules and establish confidence across borders, but West Africa doesn't have an organised way to do this because of deficiencies in training and strategy (Zwarts, du Toit, & von Solms, 2022). Trade agreements are having a more and greater impact on national cybersecurity policy, but Nigeria's inadequate regulatory structures make it hard to put them into action (Gummadi, 2024). The "sovereign cloud" paradigm, which aims for localised data control, is still mostly a dream in the region because of its reliance on infrastructure (Gummadi, 2024).

Norms are not universal; they are socially formed through diplomacy, a process in which African governments remain peripheral (Salmiati & Singh, 2024). India's multilevel cyber diplomacy demonstrates how the Global South can influence global regulations, something that is severely lacking in Nigeria (Chaudhary, 2023). Cybersecurity in West Africa will continue to be a weak and poorly funded public benefit without changes to institutions and cooperation across countries in the region.

2.3. Postcolonial Technology Theory

Cybersecurity governance in Nigeria and West Africa should be viewed within postcolonial technology theory, is a theoretical approach that attempts to disrupt the dominant discourse of colonial power. Which examines how digital infrastructures sustain geopolitical reliance. Couldry and Mejias (2019) contend that digital colonialism is evident in the global extraction and domination of data and platforms by influential entities in the Global North, hence sustaining disparities in infrastructural ownership and epistemic agency. In Nigeria, reliance on foreign cloud services, cybersecurity vendors, and data infrastructure indicates a fundamental incapacity to achieve genuine

 doi:10.20944/preprints202511.0790.v1

digital sovereignty (Nanni & Santaniello, 2025). Such dependence perpetuates colonial frameworks wherein governance is externally imposed.

Jiang (2024) shows how countries in the Global South are stuck between Western ideas of internet openness and China's control over infrastructure. This means that countries like Nigeria have limited sovereignty because of clashing geopolitical goals. Timcke, Gaffley, and Rens (2023) emphasise that South Africa's 2021 Transnet cyberattack exposed infrastructural weaknesses that need dependence on external cybersecurity entities, transforming cyber threats into instruments of neocolonial soft power. Olofinbiyi (2022) affirms this perspective with figures indicating that South Africa's cybercrime losses surpass R2.2 billion yearly, primarily attributable to postcolonial infrastructural reliance.

Belli (2021) demonstrates that BRICS nations have sought to mitigate Western platform supremacy by investing in sovereign Internet Exchange Points (IXPs) and cloud infrastructure. But Nigeria's broken digital ecosystem and West Africa's lack of coordinated investment make it harder to reject. In the end, cybersecurity in the region can't be separated from the fundamental imbalances in ownership and power that are a legacy of colonialism and are built into the very structure of cyberspace.

3. Empirical Context: Cybersecurity Challenges in the Global South

3.1. Infrastructure Dependence

West African nations, especially Nigeria, Ghana, and Kenya, continue to be primarily dependent on foreign-owned digital infrastructure particularly cloud platforms, data centres, and submarine cable systems thereby compromising digital sovereignty and cybersecurity independence. Ogidiaka et al. (2022) discovered that 80% of Nigerian organisations rely on foreign cloud providers owing to inadequate local infrastructure, insufficient trust in domestic vendors, and a scarcity of trained cybersecurity professionals. Onwuka (2024) further illustrates, by longitudinal panel regression, that foreign direct investment is highly connected to external ownership of essential digital infrastructure in Nigeria, Ghana, and Kenya. This makes countries more dependent on infrastructure and less likely to come up with new ideas. According to UN data, donor-led investment has failed to create independent digital ecosystems in Nigeria and Ghana, where performance is substantially worse than the world average (0.2209 vs. 0.4939).

3.1.1. Some Major Foreign-Owned Digital Infrastructures and Companies That Nigeria Depends On Include the Following:

3.1.1.1 Google (United State)

- **Infrastructure**: You Tube, Android OS, Google Cloud Platform, and the Equiano subsea cable
- **Dependency:** Nigeria depends mostly on Google’s cloud storage, search engines, and digital advertising infrastructure.

3.1.1.2 Meta (formerly known as Facebook)

- **Infrastructure:** Facebook, Instagram, WhatsApp, and Meta’s data transmission network
- **Dependency:** Nigerians mostly rely on these platforms for social communication, business marketing, and digital commerce.

3.1.1.3 Microsoft (United State)

Infrastructure: Azure Cloud, LinkedIn, Office 365.

Dependency: Some of the Nigeria government agencies, banks and other companies make use Microsoft Azure for cloud hosting, data storage, and enterprise software.

 doi:10.20944/preprints202511.0790.v1

3.1.1.4 Huawei (China)

Infrastructure: Telecommunications equipment, 4G/5G network infrastructure, and data center technologies.

Dependency: Huawei is a major supplier to MTN, GLO, Airtel, and 9mobile networks in Nigeria.

3.1.1.5 Oracle (United State)

Infrastructure: Cloud-based enterprise solutions, databases, and ERP systems.

Dependency: Nigerians banks, university, and government mostly rely on it for managing large-scale data and operations.

Jiang (2024) shows that South Africa and Kenya depend on Chinese underwater cables and cloud services, similar to colonial eras when foreign governments controlled essential infrastructures despite being sovereign. Geopolitics, not national planning, determine telecom and data infrastructure in Nigeria (David & Tijjani, 2025). Because dependence creates systemic cyber vulnerabilities, they suggest the government invest in regional data centres, independent cloud platforms, and telecommunications infrastructure. Reactive, externally-sourced cybersecurity plans cannot defend the state from cyber manipulation or eavesdropping. Infrastructure dependency is a postcolonial governance issue in the digital state's construction, not just a technological one.

3.2. Legal and Regulatory Gaps

Outdated, fragmented, and inconsistently enforced laws hinder cybersecurity governance in Nigeria and West Africa. The Nigerian National Communications Commission (NCC) and National Information Technology Development Agency in Nigeria share several duties. This creates ambiguity and hinders enforcement, according to Calandro (2020). South Africa has coordination challenges that make adopting global cyber standards like vulnerability disclosure or infrastructure protection harder (Calandro, 2020).

South Africa's Cybercrimes Act and POPIA are ineffective, according to Watney (2024), due to vague definitions of violations and slow enforcement. Simba-Mwogosi et al. (2025) found that Tanzania lacks cybersecurity laws and monitoring for health record interoperability requirements, like Nigeria. Khan (2025) adds that African legal systems differ from GDPR-style frameworks in that they lack empirical examination of enforcement efficacy and are very diverse. Akinbowale, Zerihun, and Mashigo (2025) indicate that insufficient cybercrime law enforcement contributes to rising cyber-fraud, notably in banking. Digital trust and sovereign sovereignty are eroded when cyberspace law enforcement replaces individual protection.

3.3. External Threats and Internal Weaknesses

Developing nations are facing more frequent and powerful cyberattacks on critical facilities. Most attacks occur in finance, healthcare, and media. After analysing 897 cyberattacks worldwide, Roumani and Alraee (2024) found that healthcare institutions were most vulnerable to data breaches and service outages and that nation-state and ransomware actors targeted public health and financial systems. According to Motlhabi et al. (2022), poor threat intelligence and inter-agency coordination led to frequent breaches at South African banks, ISPs, and utilities. These results coincide with the African Union Cybersecurity Strategy (2022), which notes insufficient regional coordination and event reporting.

In the meanwhile, cybersecurity personnel are scarce. After reviewing 280 job ads, Kruger, Futcher, and Thomson (2022) found that South Africa needed more threat analysts, engineers, and SOC professionals. They blamed institutions for not investing in these areas. National survey data validated by De Jager, Futcher, and Thomson (2023) shows that public organisations lack time, money, and staff to handle cybersecurity concerns. Ashley et al. (2022) found that gamified training increased threat response after linking skill shortages to industrial control system dangers. The ITU

 doi:10.20944/preprints202511.0790.v1

Global Cybersecurity Index (2021) placed many African states in the bottom half. Due to their lack of cyber-readiness and reliance on Zoom and Google, their systems were vulnerable to outside attacks.

4. Cybersecurity as Digital Sovereignty: New Governance Models

4.1. Towards Sovereign Digital Infrastructure

The government must fund and operate cloud storage, data centres, and internet exchange points for Nigeria and West Africa to regain their digital infrastructure. Our current circumstance makes us heavily dependent on external sources. Ogidiaka et al. (2022) found that 80% of Nigerian enterprises chose international cloud services over Galaxy Backbone. They cite the company's low trustworthiness, lack of innovation, and unreliable infrastructure. This move weakens cybersecurity and gives foreigners influence over data flows.

Onwuka (2024) found that external infrastructure ownership adversely affects local enforcement capacity and cybersecurity resilience in Kenya, Ghana, and Nigeria. The essay proposes regional data centre networks to reduce reliance and localise data in African governments. The country must have enough storage and operating capacity for localisation limitations to work (Jiang, 2024). Nigerian policymakers may follow South Africa's hybrid architecture that uses foreign infrastructure, open-source software, and cross-border data agreements (Jiang, 2024). The BRICS plan incorporates South African and Brazilian investments in decentralised, sovereign IXPs and open cloud ecosystems to sidestep US and EU digital monopolies, according to Belli (2021). Instead of centralised surveillance, these alternatives promote public-private partnerships and regional cooperation to improve infrastructure capacity. Nigeria and West Africa need physical infrastructure and legal frameworks that foster open-source innovation, interoperability, and regionally based data governance to achieve digital sovereignty.

4.2. Institutional Innovation

West Africans need infrastructure and institutional transformation to achieve digital sovereignty. This is especially true for regional collaboration, inclusive multi-stakeholder governance, and national CSIRT empowerment. Timcke et al. (2023) say institutional inconsistencies and a weak, centralised CSIRT architecture hampered South Africa's response to the 2021 Transnet hack. Like Nigeria's dysfunctional incident response system, real-time cyber attacks would be hard to respond to. A Cyber Threat Intelligence Exchange Framework was created by Motlhabi et al. (2022) using South African telecom data. This emphasises CSIRT cross-border cooperation. Due to poor information exchange and coordination, African states like Nigeria have fragmented and ad hoc cybersecurity policies. The Zwarts et al. (2022) Cyber Diplomacy and Awareness Framework emphasises the need for regional, technical, and diplomatic governance to be consistent and proposes the ECOWAS Cybersecurity Framework to align regional norms and cooperate in responding to threats. De Jager, Futcher, and Thomson (2023) believe that inadequately equipping public agencies is a major hurdle to implementing comprehensive cybersecurity measures, and this is not restricted to state institutions. Their statewide poll suggests that the public sector, educational institutions, and enterprises partner on standard training policies and programs to build capacity. If institutions are not inclusive, CSIRTs and legal frameworks risk becoming meaningless symbols. If West Africa and Nigeria want to build cybersecurity within sustainable sovereignty, they require multi-tiered governance systems that promote cooperation, talent development, and regional unity.

 doi:10.20944/preprints202511.0790.v1

4.3. Policy Proposals

Nigeria and West Africa need targeted policy reforms to integrate cybersecurity into digital sovereignty and solve capacity deficiencies and structural dependencies. A national Digital Sovereignty Index might measure infrastructure, regulatory uniformity, data localisation, cyber resilience, and other subjects using evidence. According to Simba-Mwogosi et al. (2025), these actions will unify Tanzania's digital policies and make institutions more accountable for e-health governance. Nigeria should invest in sovereign infrastructure, institutional change, and workforce development for cyber-independence. This plan must determine the time and amount of reducing external cloud services, crucial hardware, and cybersecurity software. Akinbowale, Zerihun, and Mashigo (2025) show that South Africa's cyberfraud vulnerabilities are linked to its foreign security equipment dependence. Local cryptographic device, firewall, and router manufacturers should be strengthened and regulatory technology labs established. These proposals are crucial for Nigeria because its public and financial sectors use imported security technologies. African nations must collaborate on digital hardware and software sovereignty as well as policy alignment. ECOWAS countries may pool funds for research and purchasing to help African enterprises and supply chains. Cybersecurity in Nigeria should move from reactive legislation to proactive statecraft with a Digital Sovereignty Index, cyber-independence plan, and hardware localisation policy. This includes industrial policy sovereignty, technical autonomy, and resilient regions.

5. Critical Debates and Counterarguments

5.1. Can Sovereignty Be Achieved Without Autarky?

The need for comprehensive infrastructure independence for digital sovereignty is debated. Nanni and Santaniello (2025) propose viewing sovereignty as a strategic relationship between independence and dependency. Their comparative study explains that economic protectionism generally means infrastructure isolation or cumbersome data localisation requirements, which hinder innovation and global interoperability. Jiang (2024) endorses a hybrid sovereignty paradigm, citing South Africa and India as open standards countries that selectively localise sensitive systems. This suggests a link between digital autonomy and global connectivity. Opponents say this midway position is hard to sustain. Mueller (2017) states that nationalising the internet hinders global multistakeholder collaboration because its technical design is global. He worries that cyber sovereignty could threaten internet interoperability. Cyber nationalism, which arises when states demand excessive control over digital territories, may lead to fragmentation, repression, and a lack of faith in global internet norms, according to Souter (2022). These opposing views show that digital sovereignty strives to protect national interests while threatening the openness that makes the internet work globally. Thus, gaining sovereignty while keeping connectedness is difficult.

5.2. Security vs Openness

Digital sovereignty regulations are billed as protections against cyber-attacks and foreign surveillance, but concerns are increasing that they could restrict human liberties and support authoritarian governments. Hwang (2025) reports that over 180 nations employed "national cybersecurity" to block websites and social media platforms from 2015 to 2023, mainly during political protests and elections. Political misuse of digital sovereignty destroys its legitimacy and breaches democracy.

Olofinbiyi (2022) claims that a lack of civil society engagement and transparency in cybersecurity choices has led to a top-down regulation approach in South Africa. The outcome is a security system that a few may exploit, revealing the government's narrow national interests. Critics like Mueller (2017) say sovereignty claims without stakeholder responsibility damage internet accessibility. Cyber nationalism—governments trying to control digital domains—is rising, and Souter (2022) warns that it leads to surveillance, fragmentation, and limitation. Under strong sovereignty models, digital

 doi:10.20944/preprints202511.0790.v1

authoritarianism may thrive in West Africa, where governments often fail to protect individuals' rights. Any national cybersecurity policy that balances cyber defence and accountability must include human rights safeguards, openness, and oversight.

5.3. Private Sector Dominance

A primary dispute during the discourse on digital sovereignty is the ability of Nigeria and other African countries to oppose the supremacy of Big Tech without impeding innovation or discouraging private investment. Calderaro and Craig (2020) assert that in low-capacity countries, technical proficiency and cybersecurity resilience are less centred on platform management and more reliant on improved capacity and information sharing. Their analysis warns that completely shutting out the private sector could take away necessary resources for governments to use for digital transformation and innovation.

Timcke et al. (2023) also criticise the entire nationalisation of cybersecurity infrastructure, using the Transnet cyberattack in South Africa to show how outsourcing might be risky and how complete state control is not possible in situations where there isn't a lot of technical knowledge. Instead, they suggest strong public-private partnerships that are overseen by defined national rules. These frameworks can help strategic independence without damaging operational capacity. Zwarts et al. (2022) support multi-stakeholder cyber diplomacy, claiming that collaborative governance that includes governments, tech companies, universities, and civil society is a way to find a balance between state sovereignty and private innovation. In West Africa, where the government isn't very strong and digital ecosystems are still growing, leaving out the private sector could lead to institutional stagnation. The goal is not to get rid of corporate power, but to control it so that it fits with national goals and public ideals through accountable, pluralistic frameworks.

6. Conclusion and Policy Recommendations

This paper suggests that cybersecurity is a governance and sovereignty issue in West African countries like Nigeria and should be rethought beyond defensive or technical roles. Cybersecurity is pivotal to control national data flows, infrastructure, and normative digital frameworks in this era of infrastructure dependency, regulatory fragmentation, and geopolitical asymmetries. Digital sovereignty requires institutional stability, infrastructure investment, and purposeful innovation, not reactive legislation. To advance this agenda, three policy goals are clear. Nigeria requires sovereign cloud platforms, national data centres, and decentralised networks to develop its digital infrastructure independently of the US, EU, and China. Businesses, organisations, and academic institutions should have a say in cybersecurity policy, and governance models should be open and inclusive. This can prevent authoritarianism. Thirdly, regional cooperation is essential. Nigeria, the most technologically advanced country in West Africa, can support a pan-African governance agenda that reflects common principles and independence ambitions and a unified ECOWAS cybersecurity framework. More research is needed along with policy changes. An all-inclusive African Cybersecurity Sovereignty Index would let states assess their progress and improve. To ensure that new tech fits democratic values and regional demands, we must examine AI governance through the perspective of African digital sovereignty as AI is integrated into more cybersecurity tools and governance systems.

References

1. Akinbowale, M. E., Zerihun, M. F., & Mashigo, P. N. (2025). The impact of legal framework on cyberfraud perpetration in the South African banking industry. *Asian Journal of Economic Modelling, 14*(1), 1–12. https://doi.org/10.18488/11.v14i1.4036
2. *Alakitan, M., & Makinde, E. (2024). Where are the ethical guidelines? Examining the governance of digital technologies and AI in Nigeria. Policy & Internet.* https://doi.org/10.1002/poi3.416

 doi:10.20944/preprints202511.0790.v1

3. Alper, C. E., & Miktus, M. (2019). Bridging the mobile digital divide in Sub-Saharan Africa: Costing under demographic change and urbanization. *PSN: Population & Family Planning (Topic)*. https://doi.org/10.5089/9781513519197.001
4. Ashley, T. D., Kwon, R., Gourisetti, S., Katsis, C., Bonebrake, C., & Boyd, P. A. (2022). Gamification of cybersecurity for workforce development in critical infrastructure. *IEEE Access, 10*, 112487–112501. https://doi.org/10.1109/ACCESS.2022.3216711
5. Bagui, L., Lusinga, S., Pule, N., Tuyeni, T., Mtegha, C. Q., Calandro, E., Chigona, W., & Solms, S. V. (2023). The impact of COVID-19 on cybersecurity awareness-raising and mindset in the Southern African Development Community (SADC). *The Electronic Journal of Information Systems in Developing Countries, 89*(3). https://doi.org/10.1002/isd2.12264
6. Belli, L. (2021). The BRICS countries and the shaping of digital sovereignty. In L. Belli & E. Zingales (Eds.), *Platform Regulations: How Platforms Are Regulated and How They Regulate Us* (pp. 113–132). Springer. https://doi.org/10.1007/978-3-030-56405-6_7
7. Botha-Badenhorst, D., & Veerasamy, N. (2023). Examining barriers to entry: Disparate gender representation in cybersecurity within Sub-Saharan Africa. *International Conference on Gender Research*. https://doi.org/10.34190/icgr.6.1.1148
8. Calderaro, A., & Craig, A. J. S. (2020). Transnational governance of cybersecurity: Policy challenges and global inequalities in cyber capacity building. *Third World Quarterly, 41*(6), 917–938. https://doi.org/10.1080/01436597.2020.1729729

   Chaudhary, P. K. (2023). India's cybersecurity diplomacy: Building global alliances. *ShodhKosh: Journal of Visual and Performing Arts, 4*(2). https://doi.org/10.29121/shodhkosh.v4.i2.2023.3386
9. Couldry, N., & Mejias, U. A. (2019). *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism*. Stanford University Press.
10. David, I. C., & Tijjani, A. (2025). Enhancing energy security in Nigeria: An analysis of international efforts (2015–2024). *South Asian Journal of Social Studies and Economics.* https://doi.org/10.9734/sajsse/2025/v22i1942
11. **de Jager, M., Futcher, L., & Thomson, K. (2023).** An investigation into the cybersecurity skills gap in South Africa. In L. Futcher, M. Coetzee, & M. Loock (Eds.), *Cybersecurity Competency Frameworks* (pp. 237–248). Springer. https://doi.org/10.1007/978-3-031-38530-8_19
12. Gummadi, J. C. S. (2024). Cybersecurity in international trade agreements: A new paradigm for economic diplomacy. *American Journal of Trade and Policy, 11*(1). https://doi.org/10.18034/ajtp.v11i1.738
13. Hwang, H. (2025). Digital sovereignty in an era of cyber threats and global connectivity. *International Journal of Multidisciplinary Research Updates, 9*(2), 23–41. https://doi.org/10.53430/ijmru.2025.9.2.0023
14. Jiang, M. (2024). Models of state digital sovereignty from the Global South: Diverging experiences from China, India and South Africa. *Policy & Internet*. https://doi.org/10.1002/poi3.427
15. Khan, H. (2025). Cross-border data privacy and legal support: A systematic review of international compliance standards and cyber law practices. *Asian Journal of Governance, Business and Economics*, *14*(1), Article a4gbeb22. https://doi.org/10.63125/a4gbeb22
16. Kruger, M., Futcher, L., & Thomson, K. (2022). A thematic content analysis of the cybersecurity skills demand in South Africa. In *Cybersecurity Education and Research* (pp. 24–38). https://doi.org/10.1007/978-3-031-12172-2_3
17. Motlhabi, M. B., Pantsi, P., Mangoale, B., Netshiya, R., & Chishiri, S. (2022). Context-aware cyber threat intelligence exchange platform. *International Conference on Cyber Warfare and Security*. https://doi.org/10.34190/iccws.17.1.42
18. Mueller, M. (2017). Will the Internet fragment? Sovereignty, globalization and cyberspace. *Polity Press.*
19. Nanni, M., & Santaniello, M. (2025). *Unthinking digital sovereignty: A critical reflection on origins, objectives, and practices*. *Policy & Internet*. Wiley Online Library
20. *Nte, N. D., Enoke, B. K., & Teru, V. A. (2022). A comparative analysis of cyber security laws and policies in Nigeria and South Africa. Law Research Review Quarterly.* https://doi.org/10.15294/lrrq.v8i2.56486
21. Nye, J. S. (2010). Cyber power. *Harvard Kennedy School Belfer Center Paper*. https://www.belfercenter.org/publication/cyber-power

 doi:10.20944/preprints202511.0790.v1

22. Ogidiaka, E., Ogwueleka, F., Irhebhude, M. E., & Orji, U. (2022). Local cloud computing service adoption in Nigeria: Challenges and solutions. *International Journal of Information Technology and Computer Science.* https://doi.org/10.5815/ijitcs.2022.04.01
23. Olofinbiyi, S. A. (2022). A reassessment of public awareness and legislative framework on cybersecurity in South Africa. *ScienceRise: Juridical Science*. https://doi.org/10.15587/2523-4153.2022.259764
24. Onwuka, I. N. (2024). Impact of investment climate on foreign direct investment in Nigeria, Ghana, Kenya and South Africa. *International Journal of Science and Research Archive.* https://doi.org/10.30574/ijsra.2024.13.2.2064
25. Orji, U. J. (2021). Moving beyond criminal law responses to cybersecurity governance in Africa. *International Journal of Criminal Justice*. https://doi.org/10.36889/ijcj.2021.002.
26. Roumani, Y., & Alraee, M. (2024). Examining the factors that impact the severity of cyberattacks on critical infrastructures. *Computers & Security, 148*, 104074. https://doi.org/10.1016/j.cose.2024.104074
27. Salmiati, & Singh, B. (2024). A cyber diplomacy framework for promoting global cybersecurity norms and cooperation. *International Journal of Advanced Networking and Applications*. https://doi.org/10.35444/ijana.2024.15422
28. Scott, W. R. (2008). *Institutions and Organizations: Ideas and Interests* (3rd ed.). SAGE Publications.
29. Simba-Mwogosi, J., Kaijage, S., Kinyua, J., & Shidende, N. (2025). Digital policy and governance frameworks for EHR systems in Tanzania: A scoping review. *Digital Policy, Regulation and Governance*. https://doi.org/10.1108/dprg-11-2024-0289
30. Souter, D. (2022). Sovereignty in the digital environment: A challenge to multistakeholder governance. *Association for Progressive Communications (APC) Policy Brief*. https://www.apc.org/en/pubs/sovereignty-digital-environment-challenge-multistakeholder-governance
31. Timcke, S., Gaffley, M., & Rens, A. (2023). The centrality of cybersecurity to socioeconomic development policy: A case study of cyber-vulnerability at South Africa's Transnet. *The African Journal of Information and Communication (AJIC)*. https://doi.org/10.23962/ajic.i32.16949
32. Ude, N., Ude, K., Ugbor, U., Igwe, C., & Ogu, E. (2021). E-governance and economic development in Sub-Saharan Africa: A case of Nigeria. *International Journal of Development Strategies in Humanities, Management and Social Sciences, 11*(1), 87–100. https://doi.org/10.48028/IIPRDS/IJDSHMSS.V11.I1.07
33. van Dijck, J., Poell, T., & de Waal, M. (2018). *The Platform Society: Public Values in a Connective World*. Oxford University Press.
34. Watney, M. (2024). Exploring South Africa's cybersecurity legal framework regulating information confidentiality, integrity, and availability. *International Conference on Cyber Warfare and Security*, 19(1), 210–219. https://doi.org/10.34190/iccws.19.1.1999
35. *Yizhen. (2025). Cyber security in Nigeria: Emerging issues, domestic governance and international cooperation. World Journal of Advanced Research and Reviews.* https://doi.org/10.30574/wjarr.2025.26.2.1687
36. Zwarts, H., du Toit, J., & von Solms, B. (2022). A cyber-diplomacy and cybersecurity awareness framework (CDAF) for developing countries. *European Conference on Cyber Warfare and Security*. https://doi.org/10.34190/eccws.21.1.226