International Journal of Multidisciplinary Research and Innovation (IJMRI)
ISSN: 3139-5902 | AGSIR Publisher | Volume 1, Issue 3 (July – August 2026)

CYBERSECURITY AND DIGITAL SOVEREIGNTY IN NIGERIA: GLITCHES AND DIAGNOSIS

Mark, Kingsley Chinonso PhD.

Department of Political Science, Nnamdi Azikiwe University, Awka, Nigeria

Received: 04 June 2026 | Accepted: 26 August 2026 | Published: 30 August 2026

DOI: https://doi.org/10.5281/zenodo.22179443

Abstract

Nigeria's rapid digital transformation, evidenced by a growing internet population, an expanding fintech sector, and increasing reliance on e-government platforms, has been matched by an equally rapid growth in cyber threats that now test the country's capacity to govern its own digital space. This paper examines cybersecurity and digital sovereignty in Nigeria as twin, mutually reinforcing challenges, using State Capacity theory (Mann, 1984; Migdal, 1988; Fukuyama, 2004) and Fragile State theory (Rotberg, 2004; Fund for Peace, 2024) as analytical lenses. It argues that Nigeria's difficulties in securing its cyberspace are not merely technical failures but symptoms of a deeper crisis of statehood: weak extractive, coercive, and infrastructural capacity; fragmented institutions; poor inter-agency coordination; and a widening gap between legislative ambition and enforcement reality .The paper diagnoses these problems as rooted in low institutional capacity, resource constraints, corruption, and poor legal precision, and situates them within the broader literature on state fragility in the developing world. It concludes that genuine digital sovereignty for Nigeria depends less on the proliferation of new legislation and more on building the administrative, coercive, and infrastructural capacity of the state to translate policy into enforceable practice.

Keywords: Cybersecurity, Digital sovereignty, e-governance, cyberspace, Nigeria

Introduction

The twenty-first century has witnessed the migration of state power, economic activity, and social life into cyberspace, a domain that recognises no natural borders and is therefore both a source of opportunity and a theatre of vulnerability for nation-states (Pohle & Thiel, 2020; Katsikas, 2025). For Nigeria, Africa's most populous country and one of the continent's fastest-growing digital economies, this migration has been especially consequential. Internet penetration surged from roughly forty-five million users in 2011 to over one hundred and fifteen million by 2021, and continues to expand alongside fintech innovation, e-government services, and the country's participation in the African Continental Free Trade Area's digital trade agenda (George, Musa, & Ajayi, 2022; World Bank Group, 2019). Information and communication technology now

contributes close to a fifth of national GDP, positioning Nigeria as a potential anchor of Africa's digital economy (International Trade Administration, 2025; Falade & Osho, 2026).

Yet this digital expansion has not been accompanied by a commensurate growth in the state's capacity to secure it. Cybercrime, ranging from advance-fee fraud and phishing to ransomware and large-scale data exfiltration, has become endemic, costing the Nigerian economy billions of dollars and eroding public trust in financial and governmental institutions (Abdullahi, Ph, & Rukayyat, 2021; CYFIRMA, 2025; Ogun Security, 2026).

Despite the enactment of the Cybercrimes (Prohibition, Prevention, etc.) Act 2015, its 2024 amendment (Hamu Legal, 2024; Omaplex Law Firm, 2024; DOA Law, 2024), the National Cybersecurity Policy and Strategy of 2021 (Osho & Onoja, 2015; Daniels, 2023), and the Nigeria Data Protection Act 2023 (Templars, 2023), Nigeria continues to experience an escalating wave of cyberattacks, data breaches, and digital fraud that undermine both national security and the country's claim to authority over its own digital space. Reports indicate that Nigeria recorded well over one hundred thousand data breach incidents in the first quarter of 2025 alone (Profiled Nigeria, 2025), that ransomware attacks against government agencies such as the Corporate Affairs Commission and the National Bureau of Statistics have exposed sensitive citizen and institutional data (Guardian Nigeria, 2026; Technology Times, 2025), and that the country loses an estimated five hundred million dollars annually to cybercrime (Ogun Security, 2026). These figures suggest a widening gap between the formal legal and policy architecture that Nigeria has constructed and its practical capacity to enforce that architecture (Falade & Osho, 2026; Mohammed, Usman, & Bello, 2019).

The problem, therefore, is not an absence of law but a deficit of state capacity: inadequate technical expertise within law enforcement and judicial institutions (Mohammed, Usman, & Bello, 2019; Eboibi, 2020), fragmented coordination among the Office of the National Security Adviser, the National Information Technology Development Agency, the Nigerian Communications Commission, and sectoral regulators (George, Musa, & Ajayi, 2022; Daniels, 2023), chronic underfunding, and a persistent outflow of skilled cybersecurity professionals (Osho et al., 2025; Nayak & Bello, 2024). This raises a central question that this paper seeks to address: to what extent do weaknesses in Nigeria's state capacity, as theorised by Mann (1984), Migdal (1988), Fukuyama (2004), and Rotberg (2004), explain the persistent glitches in the country's cybersecurity and digital sovereignty architecture, and what does a proper diagnosis of these weaknesses suggest for reform? Answering this question is important because cybersecurity failures in a country of Nigeria's size and regional influence carry implications not only for its own citizens but for the wider trajectory of digital governance across West Africa and the continent (Adewopo et al., 2024; INTERPOL, 2025).

A further dimension of the problem lies in the asymmetry between the pace of Nigeria's digital adoption and the pace at which its institutions have adapted to govern that adoption (Abdullahi, Ph, & Rukayyat, 2021; George, Musa, & Ajayi, 2022). Digital identity systems, mobile banking, e-government portals, and social media platforms have been embraced by tens of millions of Nigerians within a comparatively short period, often outstripping the capacity of regulators to establish, monitor, and enforce corresponding security standards (Nayak & Bello, 2024). This asymmetry produces a moving target: by the time an agency develops the capacity to secure one category of digital infrastructure, the threat landscape has often shifted toward new vectors, such as

artificial-intelligence-enabled fraud or cryptocurrency-based laundering, that existing frameworks were not designed to address (Garba, Lazarus, & Button, 2024; Falade & Osho, 2026). The problem is compounded by the transnational character of most cyber threats affecting Nigeria, since perpetrators frequently operate from outside the country's jurisdiction, exploiting gaps in international cooperation and mutual legal assistance that domestic reforms alone cannot close (Broadhurst & Chang, 2012; Olowu, 2009; Umejiaku & Anyaegbu, 2016). Left unaddressed, this widening gap between digital adoption and institutional adaptation threatens to entrench Nigeria's vulnerability rather than resolve it, making a rigorous, theoretically grounded diagnosis of the underlying causes both timely and necessary.

The problem is further sharpened by the fact that much of Nigeria's most sensitive digital infrastructure, including national identity databases, voter registration systems, and financial sector platforms, now underpins not only routine administrative functions but core democratic and economic processes (Paradigm Initiative, 2024; Profiled Nigeria, 2025). A breach or manipulation of election-related infrastructure, for instance, carries implications that extend well beyond data privacy into the realm of political legitimacy and national stability (Guardian Nigeria, 2026), while breaches of identity and financial systems undermine the trust upon which an increasingly cashless and digitally mediated economy depends (Ogun Security, 2026; Orji, 2019). Framing Nigeria's cybersecurity shortcomings purely as a technical or criminal-justice problem therefore risks understating their significance; they are, at their core, a question of whether the Nigerian state can be said to exercise effective, trustworthy authority over the digital infrastructure that increasingly mediates citizens' relationship with government, the economy, and one another (Rotberg, 2004; Fund for Peace, 2024).

From the above therefore, the paper interrogates the relationship between cybersecurity and digital sovereignty in Nigeria through the combined lens of State Capacity theory (Mann, 1984; Migdal, 1988; Fukuyama, 2004) and Fragile State theory (Rotberg, 2004; Fund for Peace, 2024). It proceeds from the premise that Nigeria's cybersecurity shortcomings are best understood not as isolated technical failures but as manifestations of a broader crisis of statehood, in which the formal architecture of law and policy has outpaced the state's practical ability to enforce, coordinate, and defend (Falade & Osho, 2026; Daniels, 2023; Nayak & Bello, 2024).

Review of Related Literature

Cybersecurity in Nigeria

Cybersecurity, broadly defined, refers to the body of technologies, processes, and practices designed to protect networks, devices, programmes, and data from attack, damage, or unauthorised access. According to George, Musa, and Ajayi (2022), it encompasses technical dimensions, such as encryption, firewalls, and intrusion detection, as well as legal, institutional, and human dimensions, including regulation, incident response capacity, and user awareness. Katsikas (2025) and Moerel and Timmers (2021) similarly argue that cybersecurity is increasingly treated not merely as an information-technology concern but as a matter of national security, given that critical infrastructure such as power grids, financial systems, and government databases now depend on interconnected digital systems that are vulnerable to disruption.

In the Nigerian context, cybersecurity has been shaped by the country's rapid but uneven digitalisation (George, Musa, & Ajayi, 2022; Abdullahi, Ph, & Rukayyat, 2021). Cybercrime manifests in diverse forms, including phishing, identity theft, misinformation, and the notorious advance-fee fraud, popularly known as "419" or "yahoo yahoo" scams, which have long stained Nigeria's international digital reputation and led to Nigerian internet service providers being blacklisted by global email systems (Chawki, 2009; Awhefeada & Bernice, 2020). Studies attribute the prevalence of cybercrime in Nigeria to a combination of socioeconomic drivers, including poverty, unemployment, corruption, and low digital literacy (Abdullahi, Ph, & Rukayyat, 2021; Hassan, Lass, & Makinde, 2012), alongside weak policy implementation and the pursuit of wealth and social status among young people drawn into fraud subcultures (Adeniran, 2008).

The institutional architecture for cybersecurity in Nigeria includes the Office of the National Security Adviser, which houses the National Computer Emergency Response Team, the Nigerian Communications Commission, the National Information Technology Development Agency, sectoral regulators such as the Central Bank of Nigeria, and the judiciary (George, Musa, & Ajayi, 2022; Falade & Osho, 2026). Despite this array of institutions, enforcement remains hampered by inadequate technical capacity, slow judicial processes, and limited inter-agency coordination (Mohammed, Usman, & Bello, 2019; Daniels, 2023). Between January and September 2025, Nigeria experienced a marked surge in data breaches and cybercrime activity spanning banking, telecommunications, government, and healthcare sectors, with dark-web actors observed selling banking databases, stolen credentials, and telecom records numbering in the tens of millions (CYFIRMA, 2025). Government institutions, including the Corporate Affairs Commission and the National Bureau of Statistics, have themselves fallen victim to ransomware (Guardian Nigeria, 2026; Technology Times, 2025), underscoring that vulnerability extends into the heart of the state apparatus rather than being confined to private citizens and businesses.

The financial sector illustrates the scale of the challenge with particular clarity. The Central Bank of Nigeria has reported that a substantial majority of attempted or successful fraud and forgery cases within the Nigerian banking system now stem from electronic channels (Hamu Legal, 2024), reflecting the migration of financial crime from physical to digital spaces alongside the growth of online and mobile banking. Fintech firms operating in Nigeria have similarly reported sharp increases in artificial-intelligence-driven attacks on the financial sector, including deepfake-enabled identity fraud and automated phishing campaigns (Ogun Security, 2026), illustrating that the threat landscape facing Nigerian institutions is evolving as quickly as, if not faster than, the tools available to counter it. Scholars have also documented the reputational costs of Nigeria's cybercrime problem, noting that Nigerian-linked internet traffic and email domains have historically faced elevated scrutiny and blacklisting by international systems (Awhefeada & Bernice, 2020; Chawki, 2009), a pattern that imposes indirect economic costs on legitimate Nigerian businesses and professionals seeking to engage in cross-border digital commerce. Taken together, this literature paints a picture of a digital ecosystem in which growth and vulnerability have expanded in tandem, with institutional responses consistently trailing behind the sophistication and scale of the threats they are meant to address (Falade & Osho, 2026; Mohammed, Usman, & Bello, 2019; Daniels, 2023).

A distinct but related strand of Nigerian cybersecurity scholarship focuses on the social and cultural dimensions of the country's cybercrime problem, particularly the phenomenon widely referred to as

"yahoo yahoo" (Adeniran, 2008; Chawki, 2009), a colloquial term for internet-based advance-fee fraud that has, in some urban youth subcultures, acquired an ambivalent social status somewhere between criminality and an informal, if illicit, career path. Researchers attribute the persistence of this subculture to a combination of high youth unemployment, weak formal-sector job creation, aspirational consumerism amplified by social media, and a widely perceived low probability of prosecution given the enforcement gaps discussed elsewhere in this essay (Hassan, Lass, & Makinde, 2012; Mohammed, Usman, & Bello, 2019). Some scholars caution that purely punitive responses to this phenomenon are unlikely to succeed in isolation, since they do not address the underlying economic incentives that draw young people into cybercrime (Adeniran, 2008); rather, they argue that sustained investment in legitimate digital-economy job creation, technical and vocational education, and youth entrepreneurship support constitutes an essential, if longer-term, complement to law enforcement and regulatory reform in addressing Nigeria's cybercrime problem at its social roots (Garba, Lazarus, & Button, 2024; Osho et al., 2025).

Digital Sovereignty in Nigeria

Digital sovereignty is a contested and evolving concept whose precise meaning varies across national contexts (Couture & Toupin, 2019; Pohle & Thiel, 2020). At its core, however, it refers to a state's capacity to govern its digital territory, encompassing the protection of digital infrastructure and the exercise of authority over digital communications, data, and technologies that affect its territory and citizens (Fleming, 2025; Pohle & Thiel, 2020). Digital sovereignty is often understood to comprise both protective and offensive dimensions: the ability to defend national digital space from external interference, and the capacity to project influence and drive innovation within that space (Katsikas, 2025; Yalamancheli, 2025). It has emerged as a strategic instrument through which governments seek to retain control over their technological futures rather than remaining passive recipients of foreign platforms, standards, and infrastructure (Moerel & Timmers, 2021).

Nigeria's pursuit of digital sovereignty is most visibly expressed through two central instruments: the Cybercrimes (Prohibition, Prevention, etc.) Act, first enacted in 2015 and substantially amended in 2024 (Hamu Legal, 2024; Omaplex Law Firm, 2024; Niji Oni & Co, 2025), and the National Cybersecurity Policy and Strategy, first issued in 2014 and revised in 2021 (Osho & Onoja, 2015; PolicyVault Africa, 2023). Together, these instruments represent Nigeria's formal claim to authority over its cyberspace, empowering state institutions to protect critical national information infrastructure, prosecute cyber offences, and coordinate national defence against digital threats (Falade & Osho, 2026). The 2024 amendment to the Cybercrimes Act strengthened the National Computer Emergency Response Team, reduced the mandatory cyber-incident reporting window from seven days to seventy-two hours, mandated the routing of organisational internet traffic through sectoral Security Operations Centres, and raised the cybersecurity levy on electronic transactions from 0.005 percent to 0.5 percent of the value of transactions to bolster the National Cybersecurity Fund (Hamu Legal, 2024; Falade & Osho, 2026; DOA Law, 2024).

These reforms have been complemented by the Nigeria Data Protection Act 2023, which established the Nigeria Data Protection Commission as the country's principal data protection regulator (Templars, 2023), and by the National Cybersecurity Policy and Strategy's articulation of eight strategic pillars spanning governance, critical infrastructure protection, incident management, legal reform, defence capability, the digital economy, monitoring and evaluation, and international

cooperation (Falade & Osho, 2026; Daniels, 2023). Even so, scholarly analysis suggests that while these instruments mark genuine progress in Nigeria's assertion of authority over its digital domain, their practical contribution to sovereignty remains constrained by legislative ambiguity, particularly in provisions on cyberstalking and the definition of a "computer" (Eboibi, 2020; Rozen, 2024b), by weak enforcement capacity (Mohammed, Usman, & Bello, 2019), and by continued dependence on foreign technology partnerships and international cooperation mechanisms that, while necessary, dilute the unilateral control that full digital sovereignty implies (Falade & Osho, 2026).

Beyond the Cybercrimes Act and the National Cybersecurity Policy and Strategy, Nigeria's digital sovereignty agenda is also shaped by sector-specific instruments, including the Nigerian Communications Commission's regulations on subscriber identity module registration, the Central Bank of Nigeria's cybersecurity framework for the financial sector, and the National Identity Management Commission's oversight of the National Identification Number system (George, Musa, & Ajayi, 2022; IISS, 2023). Scholars note that this proliferation of sector-specific rules, while reflecting a genuine effort to embed digital sovereignty considerations across different domains of national life, has also produced a degree of regulatory fragmentation, with different agencies at times applying inconsistent standards or duplicating oversight responsibilities (Nayak & Bello, 2024; Daniels, 2023). This fragmentation is itself identified in the literature as a constraint on digital sovereignty, since a coherent assertion of authority over the digital domain requires not merely the existence of multiple rules but their coordinated and consistent application (Migdal, 1988; Falade & Osho, 2026). Analysts have also observed that Nigeria's digital sovereignty efforts remain heavily oriented toward domestic criminal and administrative law, with comparatively less attention paid to the geopolitical dimensions of digital sovereignty, areas in which more technologically advanced states have historically exercised disproportionate influence (Fleming, 2025; Qin, 2025).

Theoretical Framework

State Capacity and Fragile State Theory

State Capacity theory and Fragile State theory are two closely related, and in many respects complementary, strands of political science scholarship concerned with explaining variation in what states can and cannot do (Mann, 1984; Migdal, 1988; Rotberg, 2004).

Developed cumulatively through the work of several scholars from the 1980s onward. Michael Mann's 1984 paper, "The Autonomous Power of the State: Its Origins, Mechanisms and Results," published in the European Journal of Sociology, is widely regarded as foundational, introducing the influential distinction between "despotic power," the range of actions a state elite can take without routine negotiation with civil society, and "infrastructural power," the capacity of the state to actually penetrate society and implement its decisions logistically across its territory (Mann, 1984). Joel Migdal's 1988 book, Strong Societies and Weak States: State-Society Relations and State Capabilities in the Third World, extended this analysis specifically to developing states, arguing that state capacity is shaped by the relative strength of societal forces, such as clans, ethnic groups, and local power-holders, that compete with the state for social control (Migdal, 1988). Francis Fukuyama's 2004 work, State-Building: Governance and World Order in the Twenty-First Century, further popularised the distinction between the scope of state activity and the strength or capacity

with which that activity is carried out, arguing that weak capacity, rather than an overly limited scope of state functions, was the central problem facing many developing countries (Fukuyama, 2004).

State Capacity theory asks why some states are able to formulate and implement policy effectively, extract resources, maintain order, and deliver services, while others cannot, focusing attention on the administrative, coercive, extractive, and infrastructural dimensions of state power (Mann, 1984; Fukuyama, 2004). Fragile State theory, which developed substantially out of and alongside state capacity scholarship, focuses specifically on states whose capacity has eroded to the point where they struggle to perform core functions such as guaranteeing security, the rule of law, and basic welfare for their populations, situating such states along a spectrum ranging from weak, through fragile and failing, to collapsed (Rotberg, 2004; Fund for Peace, 2024).

Taken together, these frameworks provide a useful analytical bridge between the technical language of cybersecurity policy and the deeper political-institutional realities that determine whether such policy can actually be implemented (Migdal, 1988; Fukuyama, 2004; Falade & Osho, 2026). A state's ability to secure its cyberspace and assert digital sovereignty is, in this view, simply a specific application of its general capacity to govern effectively; a state that struggles to collect taxes, maintain security in its territory, or coordinate its bureaucracy is unlikely to coordinate effectively across the technical, legal, and institutional demands of cybersecurity (Mann, 1984; Rotberg, 2004).

State Capacity theory conventionally identifies several interrelated dimensions of capacity that are useful for analysing cybersecurity governance. Extractive capacity refers to the state's ability to mobilise financial and material resources, a dimension directly relevant to whether a government can adequately fund cybersecurity agencies, forensic laboratories, and training programmes (Mann, 1984). Coercive capacity refers to the state's ability to enforce compliance and deter wrongdoing, relevant to the prosecution and deterrence of cybercriminals (Mohammed, Usman, & Bello, 2019). Administrative or bureaucratic capacity refers to the competence, coordination, and professionalism of the civil service, relevant to whether agencies such as the National Information Technology Development Agency and the Nigerian Communications Commission can translate policy into coherent, well-implemented programmes (Migdal, 1988; Daniels, 2023). Infrastructural capacity, in Mann's (1984) specific usage, refers to the state's ability to actually reach into society to implement its decisions, a dimension especially pertinent to whether cybersecurity mandates can be enforced uniformly across Nigeria's diverse states, sectors, and levels of digital development. Fragile State theory builds upon these same dimensions but applies them diagnostically, treating persistent shortfalls across several dimensions simultaneously as evidence of a broader condition of state fragility rather than as isolated policy failures (Rotberg, 2004; Fund for Peace, 2024), a diagnostic orientation that is particularly well suited to explaining the pattern of recurring, interlinked glitches evident in Nigeria's cybersecurity and digital sovereignty architecture.

Applying State Capacity and Fragile State theory to Nigeria's cybersecurity and digital sovereignty challenges reveals a consistent pattern: the country possesses considerable "despotic" or formal legal authority in cyberspace, expressed through an increasingly elaborate architecture of statutes, policies, and regulatory bodies, but comparatively limited "infrastructural power," that is, the practical capability to implement and enforce that authority uniformly and effectively (Mann, 1984;

Falade & Osho, 2026). Mann's (1984) distinction is instructive here. The Cybercrimes Act and its 2024 amendment, together with the National Cybersecurity Policy and Strategy, represent the state's formal assertion of despotic authority over cyberspace, criminalising a wide range of offences and creating institutions such as the National Computer Emergency Response Team (Hamu Legal, 2024). Yet the persistent gap between legislative ambition and enforcement outcomes, evident in low prosecution rates, fragmented inter-agency coordination, and repeated breaches of government systems (Mohammed, Usman, & Bello, 2019; Guardian Nigeria, 2026), reflects a shortfall in infrastructural power: the everyday, logistical capacity to penetrate and secure the digital domain across sectors and geography.

Migdal's (1988) state-in-society model further illuminates why this gap persists. Just as Migdal argued that developing states must contend with strong societal actors that limit central control over physical territory, Nigeria's cyberspace is similarly contested by non-state actors, including transnational cybercriminal syndicates, financially motivated ransomware groups, and loosely organised domestic fraud subcultures such as the "yahoo yahoo" phenomenon (Adeniran, 2008; Chawki, 2009), whose persistence reflects the state's limited capacity to project authority into digital as well as physical peripheries. Fukuyama's (2004) capacity-versus-scope framework helps explain why simply expanding the scope of cyber legislation, as Nigeria did through the 2024 amendment, does not by itself resolve the underlying problem: without a corresponding increase in the strength or capacity to implement that legislation, an expanded scope of formal state activity in cyberspace can outpace the state's genuine administrative reach, producing law that is aspirational rather than operative (Nayak & Bello, 2024; Daniels, 2023).

Rotberg's (2004) Fragile State framework, meanwhile, directs attention to the erosion of core political goods as both cause and consequence of cyber insecurity. Nigeria's documented struggles with insecurity, corruption, weak judicial capacity, and uneven service delivery, the very indicators that place it fifteenth on the 2024 Fragile States Index among more fragile states internationally (Fund for Peace, 2024), are mirrored in its cybersecurity institutions: underfunded forensic units, slow prosecutions (Mohammed, Usman, & Bello, 2019), and a persistent outflow of trained cybersecurity professionals seeking better opportunities abroad (Osho et al., 2025; Nayak & Bello, 2024). In Rotberg's (2004) terms, a state that struggles to provide the political good of physical security also struggles to provide its digital-era analogue, cybersecurity, because both depend on the same underlying administrative, coercive, and fiscal capacities. This theoretical lens therefore reframes Nigeria's cybersecurity "glitches" not as discrete technical failures but as symptomatic expressions of broader, structural state fragility (Mann, 1984; Migdal, 1988; Rotberg, 2004), a reframing that has direct implications for how the problems discussed in the following section ought to be diagnosed and addressed.

It is useful, finally, to situate Nigeria within a comparative frame suggested by this literature. Fragile State scholarship generally distinguishes between states that are fragile because they lack the resources to build capacity, sometimes termed poverty-driven fragility, and states that possess considerable resources but whose capacity is undermined by governance failures, including corruption, elite capture, and weak accountability, sometimes termed governance-driven fragility (Rotberg, 2004; Fund for Peace, 2024). Nigeria, as an oil-rich economy with substantial fiscal resources and a large, well-educated professional class, including a globally recognised technology

and fintech talent pool (International Trade Administration, 2025), fits more readily into the second category. This distinction matters for policy, because it suggests that Nigeria's cybersecurity and digital sovereignty deficit is less a function of an absolute absence of resources or human capital than of how existing resources and capacity are allocated, coordinated, and retained (Migdal, 1988; Nayak & Bello, 2024). The persistent outflow of skilled cybersecurity professionals discussed as a glitch above is illustrative in this respect: it is not that Nigeria fails to produce capable cybersecurity talent, but that its institutions and labour market conditions often fail to retain that talent domestically (Osho et al., 2025), a governance rather than a purely resource-based failure. This comparative positioning within the Fragile State literature strengthens the case that Nigeria's path toward stronger digital sovereignty lies primarily through institutional and governance reform rather than through resource mobilisation alone.

Cybersecurity and Digital Sovereignty in Nigeria

Nigeria's digital economy has grown rapidly, but this growth has not been matched by a proportionate strengthening of the state's capacity to secure it (Falade & Osho, 2026; Nayak & Bello, 2024). The country recorded a cyberattack roughly every thirty-nine seconds according to the Nigeria Data Protection Commission (Ogun Security, 2026), and independent estimates place Nigeria's cumulative cybercrime losses at more than three billion dollars between 2019 and 2025, an average of approximately five hundred million dollars annually (Ogun Security, 2026), while other estimates using different methodologies place losses over a slightly related period at over eight hundred million dollars (Abdullahi, Ph, & Rukayyat, 2021). The Nigeria Deposit Insurance Corporation reported a 183 percent increase in e-payment fraud within the banking sector even before the current wave of attacks (Abdullahi, Ph, & Rukayyat, 2021), illustrating that vulnerability in Nigeria's digital ecosystem predates its most recent phase of expansion and has simply grown alongside it.

At the level of digital sovereignty, Nigeria has constructed a reasonably comprehensive formal architecture: the Cybercrimes Act 2015 and its 2024 amendment (Hamu Legal, 2024; Omaplex Law Firm, 2024), the National Cybersecurity Policy and Strategy of 2014 and its 2021 revision (Osho & Onoja, 2015; PolicyVault Africa, 2023), and the Nigeria Data Protection Act 2023, which established the Nigeria Data Protection Commission and, since September 2025, has required covered entities to notify data breaches within seventy-two hours (Templars, 2023; Ogun Security, 2026). Nigeria's 2022 accession to the Budapest Convention on Cybercrime (Council of Europe, 2022) further signals an effort to align with international cyber-governance norms. These developments represent genuine steps toward asserting sovereign authority over Nigeria's digital space (Falade & Osho, 2026). However, as the discussion below demonstrates, the practical reality of implementation reveals a persistent and, in places, widening gap between this formal architecture and Nigeria's ability to enforce it.

This gap is not static; it has, if anything, widened in recent years even as the formal architecture has grown more elaborate. The launch of a new inter-agency coordinating body, sometimes referenced in policy circles as a national multi-agency cybercrime coordination council, illustrates continued institutional experimentation aimed at closing coordination gaps identified as far back as the original 2015 Cybercrimes Act (Ogun Security, 2026; Daniels, 2023). Yet the persistence of high-profile breaches even after such institutional innovations suggests that the challenge lies less in the

absence of coordinating mechanisms on paper than in the practical capacity, funding, and political will required to make those mechanisms function as intended. Deloitte's Nigeria Cyber Security Outlook for 2026 estimates that the country lost more than three billion dollars to cybercrime between 2019 and 2025 (Ogun Security, 2026), while separate United Nations Office on Drugs and Crime estimates place losses at over eight hundred million dollars across a related period using a different methodology (Abdullahi, Ph, & Rukayyat, 2021); although the two estimates are not directly comparable, both point to losses of a similar order of magnitude and confirm that Nigeria's cybersecurity shortfall carries substantial and continuing economic costs. This economic dimension reinforces the sovereignty stakes of the problem, since a state that cannot protect the economic value generated within its digital space struggles to translate formal legal authority into the material capacity, additional revenue, and public trust needed to reinforce that authority going forward (Rotberg, 2004; Fund for Peace, 2024).

Glitches to Cybersecurity and Digital Sovereignty in Nigeria

Several recurring glitches characterise the current state of cybersecurity and digital sovereignty in Nigeria. The first is the scale and frequency of data breaches affecting both public and private institutions. Nigeria recorded over one hundred and nineteen thousand data breach incidents in the first quarter of 2025 alone (Profiled Nigeria, 2025), and unauthorised online platforms have been found selling sensitive citizen data, including National Identification Numbers, Bank Verification Numbers, driver's license details, and international passport information, for as little as one hundred naira per record, with one such platform receiving over half a million visits in a single month (Paradigm Initiative, 2024). This illustrates a fundamental breakdown in the state's ability to safeguard the very identity infrastructure, such as the National Identification Number and Bank Verification Number systems, upon which much of its digital governance now depends.

The second glitch concerns ransomware attacks against government institutions themselves. In 2025, the Corporate Affairs Commission suffered a major ransomware attack attributed to a threat actor group that reportedly exfiltrated approximately twenty-five million documents amounting to roughly 750 gigabytes of data, while the National Bureau of Statistics and other agencies, including the Lower Niger River Basin Development Authority and the Nigerian Navy, have also been targeted, with sensitive internal data leaked (Guardian Nigeria, 2026). INTERPOL's (2025) Africa Cyberthreat Assessment Report placed Nigeria third among African countries for ransomware detections in 2024, with 3,459 recorded incidents (INTERPOL, 2025; Technology Times, 2025). That such attacks can penetrate agencies responsible for company registration, national statistics, and even elements of national security infrastructure illustrate the vulnerability of Nigeria's core administrative and data systems.

The third glitch is weak enforcement and prosecutorial capacity. Despite the existence of the Cybercrimes Act since 2015 and its strengthening in 2024, investigations and prosecutions continue to be hampered by inadequate forensic expertise, slow judicial processes, and limited inter-agency coordination among the Office of the National Security Adviser, the National Information Technology Development Agency, the Nigerian Communications Commission, and law enforcement bodies (Mohammed, Usman, & Bello, 2019; Daniels, 2023; George, Musa, & Ajayi, 2022). The 2024 amendment's reduction of the incident-reporting window to seventy-two hours and its mandate for sectoral Security Operations Centres represent genuine improvements (Hamu Legal,

2024), yet these measures depend on technical infrastructure and personnel that remain unevenly available across sectors and regions.

The fourth glitch relates to legislative and definitional ambiguity, particularly around provisions on cyberstalking, which have historically been criticised for being invoked against journalists, bloggers, and government critics for posts deemed merely "annoying" or "insulting," raising concerns about the misuse of cybersecurity law to curtail legitimate expression rather than to address genuine criminal conduct (Rozen, 2024b; LIRAD, 2025). Similarly, the Act's ambiguous conceptualisation of what constitutes a "computer" continues to grant judges wide interpretive latitude, undermining the predictability that a rights-respecting and coherent legal framework requires (Eboibi, 2020). The expanded surveillance powers introduced in 2024, which permit security agencies to intercept communications without a court order in "urgent" situations, further illustrate the tension between strengthening state authority in cyberspace and protecting citizens' digital rights (NALTF, 2025; Ifemeje & Okwuosa, 2020), a tension that itself reflects unresolved questions about the appropriate scope and limits of state power.

The fifth glitch is the persistent outflow of skilled cybersecurity professionals, commonly referred to as "brain drain," which significantly reduces Nigeria's domestic capacity to implement its own cybersecurity strategy (Osho et al., 2025; Nayak & Bello, 2024). Even as the National Cybersecurity Policy and Strategy emphasises the development of a robust cybersecurity workforce as central to a thriving digital economy, the country continues to lose trained personnel to better-resourced markets abroad, leaving critical vacancies within government agencies and the private sector alike (Falade & Osho, 2026). The sixth glitch concerns Nigeria's continued dependence on foreign-owned digital infrastructure and platforms, including cloud hosting, undersea cable connectivity, and dominant global technology firms, which constrains the country's practical ability to exercise full sovereign control over the data and communications that flow through its digital territory, even where the formal legal authority to do so exists (Moerel & Timmers, 2021; Fleming, 2025).

A seventh glitch concerns the tension between rapid legislative reform and stable, predictable implementation: because the Cybercrimes Act has already been substantially amended once, in 2024, institutions and regulated entities face a continually shifting compliance landscape that can itself become a source of confusion and non-compliance (Omaplex Law Firm, 2024; DOA Law, 2024), particularly for small and medium-sized enterprises with limited capacity to keep pace with obligations such as the raised cybersecurity levy. An eighth and final glitch lies in the underdeveloped state of public cybersecurity awareness: despite the National Cybersecurity Policy and Strategy's stated commitment to public sensitisation, independent assessments continue to find relatively low levels of everyday digital hygiene among Nigerian internet users (Profiled Nigeria, 2025; Hassan, Lass, & Makinde, 2012), evidenced by the continued effectiveness of comparatively unsophisticated phishing and social-engineering attacks. This suggests that even where technical and legal defences are strengthened, the human dimension of cybersecurity remains an under-addressed vulnerability that compounds the structural weaknesses discussed above.

Diagnosis of the Associated Problems

Diagnosing these glitches through the lens of State Capacity and Fragile State theory suggests that their root cause is not primarily a deficiency of law but a deficiency of capacity across several interlocking dimensions of statehood (Mann, 1984; Migdal, 1988; Fukuyama, 2004; Rotberg, 2004). Administratively, Nigeria's cybersecurity institutions remain fragmented, with overlapping mandates among the Office of the National Security Adviser, the National Information Technology Development Agency, the Nigerian Communications Commission, and sectoral regulators producing coordination failures that slow incident response and blur accountability (George, Musa, & Ajayi, 2022; Daniels, 2023), a pattern consistent with Migdal's (1988) observation that weak states struggle to achieve coherent, centralised control even where formal authority exists on paper.

Fiscally and technically, chronic underfunding and limited forensic infrastructure constrain the state's ability to investigate and prosecute cybercrime (Mohammed, Usman, & Bello, 2019), even though the 2024 increase in the cybersecurity levy, from 0.005 percent to 0.5 percent of electronic transaction value, represents an attempt to expand the resource base available for enforcement (Hamu Legal, 2024). This shortfall reflects what Mann (1984) would characterise as a deficit in infrastructural power: the state may possess the despotic authority to criminalise cyber offences, but it lacks the logistical and technical capacity to detect and punish them consistently across the country's diverse and rapidly digitising sectors. In Fukuyama's (2004) terms, the scope of Nigeria's cybersecurity ambition, reflected in an increasingly detailed legal and policy architecture, has consistently outpaced the strength, or practical capacity, available to implement it, producing a widening implementation gap rather than a resolution of underlying vulnerabilities (Nayak & Bello, 2024; Daniels, 2023).

Socially and politically, corruption, weak judicial independence in practice, and the broader indicators of fragility that place Nigeria among the more fragile states internationally, including internal insecurity and uneven public service delivery (Fund for Peace, 2024), undermine public trust in the state's ability to protect citizens' data and digital identities, which in turn discourages breach reporting and cooperation with law enforcement (Ifemeje & Okwuosa, 2020; Rozen, 2024a). Rotberg's (2004) emphasis on the state's capacity to deliver core political goods is directly applicable here: a state that struggles to guarantee physical security and the rule of law is similarly ill-equipped to guarantee its digital-era analogue, and the persistent outflow of skilled cybersecurity professionals compounds this weakness by depleting the very human capital the state needs to close the gap (Osho et al., 2025). Finally, structural dependence on foreign digital infrastructure and platforms reflects Nigeria's position within a broader global digital economy shaped by more capacious and technologically advanced states (Moerel & Timmers, 2021; Fleming, 2025), a dependence that mirrors the classical fragile-state condition of limited autonomy vis-à-vis external actors and that constrains the country's capacity to exercise full and independent digital sovereignty even when its legal authority to do so is not in question.

It is worth emphasizing that this diagnosis does not imply that legislative reform is unimportant; rather, it suggests that legislative reform functions as a necessary but insufficient condition for closing Nigeria's cybersecurity and digital sovereignty gap. The 2024 amendment to the Cybercrimes Act, the Nigeria Data Protection Act 2023, and the revised National Cybersecurity Policy and Strategy each represent meaningful improvements to the formal architecture of Nigeria's digital governance, and each addresses genuine gaps identified in earlier frameworks (Templars,

2023; Hamu Legal, 2024; Falade & Osho, 2026). The theoretical analysis advanced here simply cautions against treating such legal reforms as self-executing. Consistent with Fukuyama's (2004) argument that many developing states err by expanding the scope of state activity without a corresponding investment in capacity, Nigeria's repeated pattern of legislative amendment followed by continued high rates of breach and enforcement failure suggests that future reform efforts should be evaluated not merely by the comprehensiveness of the resulting legal text but by measurable improvements in prosecution rates, incident response times, breach prevention, and public trust, indicators that speak directly to the underlying capacity that both Mann (1984) and Rotberg (2004) identify as the true determinant of whether formal sovereignty translates into effective, lived sovereignty.

Conclusion

This paper examined cybersecurity and digital sovereignty in Nigeria through the combined lens of State Capacity and Fragile State theory, arguing that the persistent glitches evident in the country's digital governance, ranging from mass data breaches and ransomware attacks on government institutions to weak enforcement, legislative ambiguity, professional brain drain, and dependence on foreign infrastructure, are best understood not as isolated technical shortcomings but as manifestations of deeper and long-standing weaknesses in Nigerian statehood (Falade & Osho, 2026; Mohammed, Usman, & Bello, 2019; Fund for Peace, 2024). Mann's (1984) distinction between despotic and infrastructural power, Migdal's (1988) state-in-society framework, Fukuyama's (2004) capacity-versus-scope analysis, and Rotberg's (2004) account of state fragility together provide a coherent explanation for why an increasingly elaborate legal and policy architecture, comprising the Cybercrimes Act, the National Cybersecurity Policy and Strategy, and the Nigeria Data Protection Act, has not translated into commensurate improvements in Nigeria's practical cybersecurity outcomes or its capacity to exercise genuine digital sovereignty.

The implication of this analysis is that closing Nigeria's cybersecurity and digital sovereignty gap requires more than additional legislation; it requires sustained investment in the administrative, technical, fiscal, and human capacities that translate formal authority into enforceable practice (Nayak & Bello, 2024; Daniels, 2023; Osho et al., 2025). Without such investment, Nigeria risks a widening divergence between the sophistication of its cyber laws and the reality of its cyber vulnerabilities, a divergence that carries consequences not only for Nigerian citizens and institutions but for the country's standing and influence within the wider digital governance of West Africa and the African continent (Adewopo et al., 2024; INTERPOL, 2025).

More broadly, Nigeria's experience offers a cautionary illustration for other developing states pursuing digital sovereignty under conditions of constrained state capacity. It demonstrates that the drafting of comprehensive cyber legislation, while a necessary first step, is not by itself evidence of genuine sovereign control over the digital domain; sovereignty in the digital era, as in the physical one, must ultimately be measured by a state's demonstrated capacity to protect its citizens, institutions, and critical infrastructure in practice (Rotberg, 2004; Katsikas, 2025). Applying State Capacity and Fragile State theory to this problem does not counsel pessimism, however; rather, it clarifies where reform efforts are likely to yield the greatest returns, directing attention away from an exclusive focus on legislative text and toward the administrative, fiscal, and human-capital investments that determine whether that text becomes operative. In this sense, the theoretical

framework employed in this essay offers not only an explanation of Nigeria's present cybersecurity glitches but also a roadmap, however partial, for their resolution.

Recommendations

Flowing directly from the diagnosis above, the following three recommendations are advanced not as isolated policy suggestions but as an integrated agenda for closing the gap between Nigeria's formal legal authority over its digital space and its practical capacity to defend and govern that space (Falade & Osho, 2026; Nayak & Bello, 2024). Each recommendation targets a distinct dimension of state capacity identified in the theoretical discussion (Mann, 1984; Migdal, 1988; Rotberg, 2004), namely infrastructural and administrative capacity, the balance between coercive authority and rights-respecting governance, and the extractive and human-capital foundations upon which sustainable digital sovereignty ultimately depends.

1. Strengthen Institutional and Technical Capacity.

The Nigerian government should prioritise sustained investment in the technical and administrative capacity of its cybersecurity institutions, including the National Computer Emergency Response Team, sectoral Security Operations Centres, and law enforcement forensic units (Mohammed, Usman, & Bello, 2019; Daniels, 2023). This entails funding specialised training, equipping digital forensic laboratories, and improving coordination mechanisms among the Office of the National Security Adviser, the National Information Technology Development Agency, the Nigerian Communications Commission, and the judiciary (George, Musa, & Ajayi, 2022), so that the state's infrastructural power in cyberspace grows in step with its formal legal authority (Mann, 1984). A dedicated, ring-fenced portion of the National Cybersecurity Fund, now bolstered by the increased cybersecurity levy (Hamu Legal, 2024), should be allocated specifically to measurable capacity-building outcomes, such as the number of forensic analysts trained, average incident-response times, and the proportion of reported breaches that result in successful investigation, so that progress can be tracked and institutions held accountable in ways that go beyond the mere existence of new units or offices.

2. Close Legislative Ambiguities While Safeguarding Civil Liberties.

Lawmakers should revisit ambiguous provisions in the Cybercrimes Act, particularly the definitions of cyberstalking and of a "computer," to ensure legal precision and prevent misuse against journalists, activists, and ordinary citizens exercising legitimate expression (Eboibi, 2020; Rozen, 2024b; LIRAD, 2025). Simultaneously, the expanded surveillance powers introduced in 2024 should be subject to clear judicial oversight and defined limits on data retention (Ifemeje & Okwuosa, 2020; NALTF, 2025), to strengthen public trust and align enforcement powers with democratic and constitutional safeguards, an essential foundation for sustainable digital sovereignty. A periodic, independent review mechanism, potentially involving the National Assembly's relevant committees alongside civil society and technical experts, should be established to assess how these provisions are applied in practice and to recommend further refinements as digital threats and case law evolve, ensuring that legislative precision keeps pace with both technological change and Nigeria's democratic commitments.

3. Invest in Indigenous Infrastructure and Workforce Retention.

To reduce dependence on foreign digital infrastructure and stem the outflow of skilled cybersecurity professionals (Osho et al., 2025; Nayak & Bello, 2024), the government should expand partnerships with universities and technical institutes to build a domestic cybersecurity talent pipeline, offer competitive incentives, including improved remuneration and career progression within public cybersecurity institutions, to retain trained personnel, and support the development of indigenous digital infrastructure, including data-hosting capacity and cybersecurity technologies (Moerel & Timmers, 2021; Fleming, 2025). Structured collaboration with the private sector and diaspora technology professionals, through mentorship programmes, secondments, and public-private research partnerships (Iyeomoan, 2025), could further help bridge the immediate capacity gap while longer-term domestic training pipelines mature, thereby strengthening the material and human foundations of genuine, self-sustaining digital sovereignty.

References

- Abdullahi, S., Ph, G., & Rukayyat, A. (2021). A historical assessment of cybercrime in Nigeria: Implication for schools and national development. Journal of Social Sciences, 9(9), 84-94. Available at: https://www.researchgate.net/publication/355000000_A_Historical_Assessment_of_Cybercrime_in_Nigeria
- Adeniran, A. I. (2008). The internet and emergence of the yahooboys sub-culture in Nigeria. Journal of Social Sciences, 2(December), 368-381.
- Adewopo, V., Azumah, S. W., Yakubu, M. A., Gyamfi, E. K., Ozer, M., & Elsayed, N. (2024). A comprehensive analytical review on cybercrime in West Africa. arXiv preprint arXiv:2402.01649. Available at: https://arxiv.org/abs/2402.01649
- Awhefeada, U. V., & Bernice, O. O. (2020). Appraising the laws governing the control of cybercrime in Nigeria. Journal of Law, Crime and Justice, 8(1), 30-49. Available at: https://doi.org/10.15640/jlcj.v8n1a3
- Broadhurst, R., & Chang, Y. (2012). Cybercrime in Asia: Trends and challenges. Journal of Asian Criminology, 1-26.
- CYFIRMA. (2025). Cyber threat assessment on Nigeria. CYFIRMA Research. Available at: https://www.cyfirma.com/research/cyber-threat-assessment-on-nigeria/

- Celeste, E. (2021). Digital sovereignty in the EU: Challenges and future perspectives. In Data protection beyond borders: Transatlantic perspectives on extraterritoriality and sovereignty (pp. 211-228).
- Chawki, M. (2009). Nigeria tackles advance fee fraud. Journal of Information Law, 2009(May), 1-20.
- Council of Europe. (2022). Nigeria's accession to the Budapest Convention on Cybercrime. Available at: https://www.coe.int/en/web/cybercrime/nigeria
- Couture, S., & Toupin, S. (2019). What does the notion of "sovereignty" mean when referring to the digital? New Media & Society, 21(10), 2305-2322.
- Creemers, R. (2022). China's emerging data protection framework. Journal of Cybersecurity, 8(1), 1-12.
- DOA Law. (2024). The Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act 2024: A primer on key amendments. Available at: https://www.doa-law.com/cybercrimes-act-2024/
- Daniels, O. (2023). National cybersecurity policy and strategy of Nigeria: A case study (Unpublished doctoral dissertation). Capitol Technology University.
- Eboibi, F. E. (2020). Conceptualising computers for cybercrime: Challenges in Nigerian law. Journal of Law and Technology, 12(2), 45-59.
- Falade, P. V., & Osho, O. (2026). Nigeria's digital sovereignty: Analysis of cybersecurity legislation, policies, and strategies. arXiv preprint arXiv:2601.06050. Available at: https://arxiv.org/abs/2601.06050
- Fleming, S. (2025, January 10). What is digital sovereignty and how are countries approaching it? World Economic Forum. Available at: https://www.weforum.org/stories/2025/01/europe-digital-sovereignty/
- Freedom House. (2024). Freedom on the net: Emerging cyber threats and regulatory gaps. Freedom House.
- Fukuyama, F. (2004). State-building: Governance and world order in the twenty-first century. Cornell University Press.
- Fund for Peace. (2024). Fragile States Index 2024: Nigeria country profile. Available at: https://fragilestatesindex.org/
- Gana, I. M., Ibrahim, A. F., Oluwaseyi, W. A., & Wali, A. I. (2024). Cyber warfare and national security in Nigeria: Threats and responses. Kwararafa Security Review, 1(2), 97-106.
- Garba, K. H., Lazarus, S., & Button, M. (2024). An assessment of convicted cryptocurrency fraudsters. Current Issues in Criminal Justice, 1-17.
- George, T., Musa, I., & Ajayi, P. (2022). Cybersecurity legislation in Nigeria: A review of the Cybercrime Act. African Journal of Information and Communication, 19(2), 45-60.

- Guardian Nigeria. (2026). Election data at risk as hackers hold govt agencies, banks to ransom. The Guardian Nigeria. Available at: https://guardian.ng/featured/election-data-at-risk-as-hackers-hold-govt-agencies-banks-to-ransom/
- Hamu Legal. (2024). Highlights of the Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act, 2024. Available at: https://hamulegal.com/highlights-of-cybercrimes-prohibition-prevention-etc-amendment-act-2024/
- Hassan, A. B., Lass, F. D., & Makinde, J. (2012). Cybercrime in Nigeria: Causes, effects and the way out. International Journal of Information Security, 2(7), 626-631.
- IISS. (2023). Cyber capabilities and national power, Volume 2: Nigeria. International Institute for Strategic Studies. Available at: https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2023/09/cyber-capabilities-and-national-power-vol-2/cyber-capabilities-and-national-power_volume-2_08-nigeria.pdf
- INTERPOL. (2025, May). Africa cyberthreat assessment report 2025 (4th ed.). Available at: https://www.interpol.int/content/download/23094/file/25COM009248%20-%20Cybercrime_Africa%20Cyberthreat%20Assessment%20Report_Design_2025-05%20v11.pdf
- Ifemeje, S., & Okwuosa, N. (2020). Privacy and cybercrime legislation in Nigeria: A rights-based analysis. Nigerian Law Review, 18(3), 88-104.
- International Trade Administration. (2025, September 8). Nigeria digital economy. Available at: https://www.trade.gov/country-commercial-guides/nigeria-digital-economy
- Iyeomoan, E. E. (2025). Fighting economic and financial crimes to make Nigeria great again: A doctrinal analysis of cybercrime law and policy. SSRN Electronic Journal. Available at: https://ssrn.com/abstract=5264583
- Katsikas, S. K. (2025). Towards a cybersecurity-oriented research agenda for digital sovereignty. Procedia Computer Science, 254, 279-288.
- Kianpour, M., Earls Davis, P. A., & Windekilde, I. M. (2025). Digital sovereignty in practice: Analyzing the EU's NIS2 directive. International Journal of Information Security, 24(4), 1-11.
- LIRAD. (2025). Analysis of Nigeria's Cybercrime (Prohibition, Prevention, etc.) (Amendment) Act 2024 and technology-facilitated gender-based violence. Lex Initiative for Rights Advocacy and Development. Available at: https://liradnigeria.org/analysis-of-nigerias-cybercrime-prohibition-prevention-etc-amendment-act-2024-and-technology-facilitated-gender-based-violence/
- Mann, M. (1984). The autonomous power of the state: Its origins, mechanisms and results. European Journal of Sociology, 25(2), 185-213. Available at: https://doi.org/10.1017/S0003975600004239
- Migdal, J. S. (1988). Strong societies and weak states: State-society relations and state capabilities in the Third World. Princeton University Press.

- Moerel, L., & Timmers, P. (2021). Reflections on digital sovereignty. EU Cyber Direct, Research in Focus Series.
- Mohammed, K., Usman, A., & Bello, S. (2019). Enforcement challenges under Nigeria's Cybercrime Act 2015: A critical review. African Journal of Criminology, 11(1), 22-39.
- NALTF. (2025). Nigeria's cybercrime reform. National Anti-Trafficking and Law Enforcement Framework. Available at: https://naltf.gov.ng/nigerias-cybercrime-reform/
- Nayak, S. K., & Bello, A. (2024). Evaluating the effectiveness and gaps in Nigeria's government cybersecurity policies: Recommendations for enhancing cybersecurity measures. Journal of Systematic and Modern Science Research, 5(9), 1-22.
- Niji Oni & Co. (2025). The Cybercrime (Prohibition, Prevention, Etc.) (Amendment) Act 2024. Available at: https://www.mondaq.com/nigeria/security/1701826/the-cybercrime-prohibition-prevention-etc-amendment-act-2024
- Ogun Security. (2026). Nigeria's cybersecurity reckoning: The breach wave and the council racing to catch up. Available at: https://www.ogunsecurity.com/post/nigeria-s-cybersecurity-reckoning-the-breach-wave-and-the-council-racing-to-catch-up
- Olowu, D. (2009). Cyber-crimes and the boundaries of domestic legal responses: Case for an inclusionary framework for Africa. Journal of Information, Law & Technology, 2009, 10-13.
- Omaplex Law Firm. (2024). An appraisal of the Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act, 2024 and its implications for the Nigerian society. Available at: https://omaplex.com.ng/an-appraisal-of-the-cybercrimes-prohibition-prevention-etc-amendment-act-2024-and-its-implications-for-the-nigerian-society/
- Orji, U. (2019). Cybersecurity obligations of financial institutions in comparative perspective. Journal of Financial Regulation, 7(2), 201-220.
- Osho, O., & Onoja, A. D. (2015). National cyber security policy and strategy of Nigeria: A qualitative analysis. International Journal of Cyber Criminology, 9(1), 120-133.
- Osho, O., Odumesi, J., Ayodele, J., Falade, P. V., Hamzat, L., & Oloyede, O. (2025, January). Nigeria cyber threat forecast 2025. Cyber Security Experts Association of Nigeria. Available at: https://doi.org/10.13140/RG.2.2.10921.71528
- Osho, O., Odumesi, J., Hamzat, L., & Abdulraheem, H. (2022, December). National cyber threat forecast 2023. Cyber Security Experts Association of Nigeria. Available at: https://doi.org/10.13140/RG.2.2.17129.67689
- Paradigm Initiative. (2024, June 20). Major data breach: Sensitive government data of Nigerian citizens available online for just 100 naira. Available at: https://paradigmhq.org/major-data-breach-sensitive-government-data-of-nigerian-citizens-available-online-for-just-100-naira/
- Pohle, J., & Thiel, T. (2020). Digital sovereignty. Internet Policy Review, 9(4). Available at: https://doi.org/10.14763/2020.4.1532

- PolicyVault Africa. (2023). National Cybersecurity Policy and Strategy. Available at: https://policyvault.africa/policy/national-cybersecurity-policy-and-strategy/
- Profiled Nigeria. (2025). Data breach reality in Nigeria: 119,000+ breaches in Q1 2025. Available at: https://profiled.ng/blog/profiled-nigeria-cybersecurity-data-breach-prevention
- Qin, H. (2025). Regulatory conflict and the struggle for digital sovereignty: A critical analysis of the EU-US data privacy framework. Studies in Law and Justice, 4(1), 46-59.
- Roberts, H., Cowls, J., Casolari, F., Morley, J., Taddeo, M., & Floridi, L. (2021). Safeguarding European values with digital sovereignty: An analysis of statements and policies. Internet Policy Review, Forthcoming.
- Rotberg, R. I. (Ed.). (2004). When states fail: Causes and consequences. Princeton University Press.
- Rozen, J. (2024a). Cybersecurity, privacy, and human rights: Balancing law enforcement powers in the digital age. International Journal of Cyber Law, 15(1), 33-50.
- Rozen, J. (2024b). Nigeria's cybercrime reforms leave journalists at risk. Al Jazeera.
- Rutherford, M. (2019). The CLOUD Act. Berkeley Technology Law Journal, 34(4), 1177-1204.
- Technology Times. (2025). Nigeria among worst hit in 2024 as Africa's ransomware crisis deepens. Available at: https://technologytimes.ng/ransomware-nigeria-among-worst-hit-in-2024/
- Templars. (2023). In a nutshell: Data protection, privacy and cybersecurity in Nigeria. Lexology. Available at: https://www.lexology.com/library/detail.aspx?g=f44586b1-0048-4d93-a461-4d8c0aada232
- Umejiaku, N. O., & Anyaegbu, I. M. (2016). Legal framework for the enforcement of cyber law and cyber ethics in Nigeria. Journal of Information Law, 15, 7130-7139.
- World Bank Group. (2019). Nigeria digital economy diagnostic report. Available at: https://documents1.worldbank.org/curated/en/387871574812599817/pdf/Nigeria-Digital-Economy-Diagnostic-Report.pdf
- Yalamancheli, H. (2025). Digital sovereignty meets agile delivery: Empowering governments to own their tech future. Journal of Computer Science and Technology Studies, 7(8), 1061-1068.