GAS Journal of Arts Humanities and Social Sciences (GASJAHSS)

Volume 3 | Issue 11, 2025 Homepage: https://gaspublishers.com/gasjahss/ ISSN: 3048-5002

Digital Sovereignty and National Security in Liberia: Policy Gaps and Strategic Imperatives

Dr. Ambrues Monboe Nebo

Ph.D. Student -Security Studies with an emphasis on International Security, Hill-City University, Benin Republic
Adjunct Faculty, Department of Sociology and Criminology, & Political Science, University of Liberia
Department of Criminal Justice & Forensic Science Program, African Methodist Episcopal University, Liberia

Received: *10.10.2025* | ***Accepted:*** *05.11.2025* | ***Published:*** *05.11.2025*

***Corresponding Author:** Dr. Ambrues Monboe Nebo

DOI: *10.5281/zenodo.17532967*

Abstract **Original Research Article**

Digital sovereignty has become a crucial factor in determining national security in a time when cyberspace has grown to be a crucial area of national interest. Like many developing countries, Liberia has two challenges: protecting its information infrastructure from both domestic and international threats while utilizing digital technologies for socioeconomic development. The landscape of digital sovereignty in Liberia is critically examined in this study, which also identifies enduring policy gaps that jeopardize the nation's cybersecurity posture and general security.

Employing a qualitative analytical framework grounded in digital sovereignty theory and the realist perspective of international relations, the research evaluates the adequacy of existing legal, institutional, and regulatory mechanisms. The findings reveal that Liberia's current policies lack comprehensive coverage, coordination, and enforcement mechanisms, leaving critical infrastructure and sensitive data exposed to cyber threats.

In response, the article suggests strategic imperatives that give top priority to strong legal frameworks, cybersecurity capacity building, interagency cooperation, and the incorporation of digital sovereignty concepts into national security planning. The study emphasizes the need for a unified national strategy that balances technological autonomy with security requirements by highlighting these doable tactics, which will ultimately increase Liberia's resilience to changing international cyber threats.

By offering a sophisticated understanding of the relationship between national security and digital sovereignty in the context of developing nations, this study advances both academic discussion and policymaking.

Keywords: Cybersecurity Policy, Digital Sovereignty, Liberia, National Security, Policy Gaps, Strategic Imperatives.

Introduction

The global security threats of the 21st century have expanded the scope of national security interests not only for powerful states but also for African nations, which are often perceived as being on the periphery of the international security decision-making structure.

Among the contemporary global security challenges that have emerged rapidly are cyber threats or attacks. In response, several powerful states (United States of America, China, Russia, etc.), including some African countries, have adopted measures to enhance their digital sovereignty and resilience. For instance, as part of its sovereignty and resilience planning, South Africa has shifted from a data-protection law (POPIA, effective 2021) to an explicit National Policy on Data and Cloud (May 2024), which mandates that certain government and national security-sensitive data be stored on domestic infrastructure and encourages the development of local cloud and data-center capacity. To lessen reliance on foreign infrastructure, the

policy integrates localization and cloud governance strategies with legal privacy protections (Department of Communications and Digital Technologies, 2024).

The Nigeria Data Protection Act (NDPA) 2023 has established a more robust legal framework, along with a specialized regulatory body, the Nigeria Data Protection Commission, and defined tiers of responsibilities for major data controllers. These measures are designed to enhance secure data handling for citizens and facilitate the implementation of regulations concerning the location and processing of data. Since its enactment, Nigerian authorities have signaled their intention to uphold higher standards for international cloud service providers operating within the country (Nigeria Data Protection Act, 2023).

To sustain essential government and business operations within the nation or region and to attract regional cloud services, Rwanda integrates its Smart Rwanda digital transformation strategy with strategic investments aimed at establishing local infrastructure. This effort encompasses both the planning for government digital transformation and the development of new data centers, such as the private pan-African data center projects in Kigali. This synergy of physical infrastructure and policy reinforces resilience and sovereignty, as outlined in the Smart Rwanda 2020 Master Plan (2015).

Similarly, Morocco has publicly announced significant initiatives, including plans for a large renewable-powered data center hub and sovereign cloud projects explicitly framed as measures to enhance digital sovereignty. These initiatives aim to host government and commercial data locally while expanding hybrid and sovereign cloud capabilities. Positioned to mitigate reliance on international data routes, these efforts are designed to bolster resilience (DIN news desk, 2025).

Liberia presents a spectacular case of occasional cyber attacks on its digital sovereignty. For instance, in 2016, Liberia's internet infrastructure was severely disrupted by a Distributed Denial of Service (DDoS) attack, which overwhelmed the country's sole internet cable. This attack was part of a broader campaign that affected multiple countries (The Guardian, 2016).

In June 2024, Liberia's top-level domain (.LR) was targeted by a cyberattack, leading to over 48 hours of service disruptions. The attack also involved multiple attempts to breach the Ministry of Post and Telecommunications' website, highlighting vulnerabilities in the nation's digital infrastructure (Peters, 2024).

In a direct response to the growing threat of cybercrime, President Joseph Boakai underscored its escalating significance, equating its disruptive potential to that of conventional military conflicts. He highlighted that cyber breaches have increased by more than 70% over the past two decades and cautioned that such activities undermine political and financial systems while facilitating organized criminal operations (Executive Mansion, 2024).

The most recent 2025 INTERPOL Report indicates that over 30% of reported crimes in both Western and Eastern Africa are cyber-related, with Liberia identified as one of the affected countries (INTERPOL, 2025). This finding not only aligns with the President's concerns but implicitly highlights a national security imperative for Liberia to enhance its cybersecurity frameworks and advocate for digital sovereignty. In light of this context, this article examines the theme "***Digital Sovereignty and National Security in Liberia: Policy Gaps and Strategic Imperatives"*** through three distinct research objectives, namely:

1. Examine Liberia's current digital sovereignty framework.
2. Identify policy gaps affecting national security.
3. Propose strategic imperatives to enhance cyber resilience and national security.

This paper addresses the study's objectives through four segments. The first segment, adhering to conventional research practices, encompasses three thematic areas: it begins with a brief overview of the study's significance. The final two sections outline the conceptual and theoretical foundations of the research. The conceptual framework emphasizes the

relationship between digital sovereignty and national security, moving beyond abstract notions to connect digital sovereignty with tangible national security outcomes and policy responsiveness, illustrated by case studies from Africa to provide empirical balance. The theoretical grounding, also bolstered by empirical evidence, features three prominent theories in security and international relations: realism, liberal institutionalism, and securitization theory. Together, these justify Liberia's quest for digital sovereignty, which is critical to its national security interests.

Consider the core of the paper, the second segment highlights key themes: a concise overview of cybersecurity threats facing Liberia, an assessment of the current state of Liberia's digital sovereignty and national security risks, and an analysis of existing policy gaps.

Finally, the third segment emphasizes strategic imperatives and policy recommendations, concluding with a coherent summary.

Methodology and Materials

With the emergence of digital sovereignty and national security as pressing issues in Liberia, this article adopts a conceptual-empirical approach, utilizing a mixed-methods approach that is predominantly qualitative. To enhance the analysis, it incorporates quantitative data. It relies significantly on secondary sources obtained from a thorough examination of documents and policies, such as the Liberia ICT Policy, Data Protection Acts (if available), Telecommunications Acts, and the National Security Strategy. Additionally, the study in passing reference regional instruments like the ECOWAS Cybercrime Act and the AU Convention on Cyber Security and Personal Data Protection, as well as documenting instances of cybersecurity attacks that threaten Liberia's digital sovereignty.

Significance of the Study

From an academic standpoint, this study contributes to the growing body of research on cybersecurity and digital sovereignty in the Global South, particularly within fragile nations such as Liberia. It presents a case-by-case analysis of how governance, external dependencies, and digital infrastructures influence national security. By applying theoretical discussions about sovereignty in the digital age, this research highlights the specific vulnerabilities and institutional weaknesses unique to Liberia, often overlooked in academic circles. Furthermore, it paves the way for comparative studies among African countries that face similar challenges related to digital governance.

On a policy level, the study identifies critical shortcomings in Liberia's institutional, legal, and strategic frameworks concerning digital sovereignty. It underscores the urgent need for comprehensive policies regarding data protection, cyber defense, and digital infrastructure management to safeguard national security. The findings can aid the government of Liberia, regional organizations like ECOWAS, and international partners in formulating effective strategies that balance security, economic growth, and sovereignty. Practically, it offers a roadmap for enhancing defenses against cyberattacks, reducing dependence on external digital infrastructures, and ensuring that digital governance aligns with national security objectives.

Conceptual Foundation

This sub-title highlights the nexus or relationship between digital sovereignty and national security. To begin with, a conceptual clarification is important to lay the foundation for the nexus.

Digital sovereignty

The concept of digital sovereignty has been interpreted in various ways within the literature. For instance, Hulkó, Kálmán, and Lapsánszky (2025) define it as the capacity of a country or region to control its own digital infrastructure, data utilization, and technological advancements, free from external influence. This definition emphasizes the significance of independence in digital governance, highlighting the necessity for self-sufficiency in digital infrastructure and data management.

In contrast, Braun and Hummel (2024) propose that digital sovereignty may serve as part of a normative

framework focused on vulnerability and freedom. Their definition suggests that digital sovereignty encompasses not only control but also the alignment of digital governance with values such as liberty and resilience.

In her contribution to the discourse, Pohle (2020) argues that the concept of digital sovereignty has emerged as a significant term in political discussions aimed at reaffirming the importance of the nation-state, encompassing its economy and citizens, within the global governance of digital infrastructures and the advancement of digital technologies. In this context, digital sovereignty is perceived as a rhetorical device employed by states to assert their relevance and authority in the global digital arena.

These definitions indicate a lack of complete consensus on the precise meaning of the concept, as digital sovereignty increasingly becomes a focal point in both national and international policy dialogues.

Therefore, this paper adopts a working definition of digital sovereignty that is deeply rooted in existing definitions of the concept. It defines digital sovereignty as the capacity of a state to assert and maintain effective control, autonomy, and legal authority over its digital infrastructures, software, protocols, and data flows. This definition highlights the importance of upholding and safeguarding the state's values, laws, and strategic interests, while also acknowledging the interdependent and open nature of the digital landscape.

In the contemporary digital era, digital sovereignty, encompassing control over data, infrastructure, and technological autonomy, has emerged as a vital national security concern. The evolution of this necessity has been driven by increasing cyber threats, geopolitical tensions, and the strategic significance of digital assets.

Just as traditional sovereignty involves control over political authority and physical territory, digital sovereignty reflects a state's ability to govern and regulate digital infrastructure, data, and online activities within its borders. Essentially, the concept of sovereignty is extended into the digital realm through the notion of digital sovereignty (DeNardis, 2020; Maurer, 2018).

National Security

In this study, national security is defined as the safeguarding and defense of the state, encompassing its institutions, economy, political processes, critical infrastructure, and citizens against a range of threats, including foreign influence, sabotage, disruption, and espionage. A state's capacity to address these threats in the digital realm is influenced by its digital sovereignty (Internet Society, 2022). Space systems—including GPS, satellite navigation, space-based communication, and surveillance assets—alongside the virtual network and internet, are essential components of the state's critical infrastructure and hold significant strategic importance for its national security interests.

Brief Nexus between Digital Sovereignty and National Security

The capacity of a state to regulate and protect its digital infrastructure, data, and technological landscape from external influences or cyber threats is central to the interplay between digital sovereignty and national security. Emphasizing the importance of safeguarding critical infrastructure, Kuerbis (2020) asserts that maintaining control over digital systems, such as power grids, communication networks, and financial frameworks, helps avert cyber attacks that could potentially undermine national security. In a related vein, Segal (2019) argues that digital sovereignty empowers a state to develop and implement technologies (e.g., AI, 5G networks) in alignment with its national interests, thereby reducing reliance on foreign suppliers that may pose security risks.

The integration of AI, cyberspace, and technology into national security strategies or policies allows a state to demonstrate digital sovereignty by signaling its autonomy and control. However, in practice, most states achieve only a partial form of digital sovereignty due to the profound global interdependencies in data, infrastructure, and

innovation ecosystems. For example, cloud services operated by multinational hyperscalers, software tools from U.S. or Indian companies, chips manufactured in Taiwan or South Korea, and other contemporary digital systems are intricately embedded within global supply chains. Even when a state successfully develops its own capabilities, many components and intellectual property are often sourced from elsewhere (Baldoni & Di Luna, 2025).

Moreover, adversarial pressures, coercion, and geopolitical risks significantly impede a nation's quest for complete digital sovereignty, even when such objectives are embedded within national security strategies or policies. This suggests that a state's sovereignty can be compromised by sanctions, diplomatic pressures, or the preeminence of major technology platforms. External entities may restrict access to crucial services, limit the export of essential components, or exert influence over technology firms. For instance, although Russia has made efforts to assert control over its internet, known as "Runet," it still depends on certain elements of the global internet (Fratini, 2024). Similarly, Africa largely relies on various aspects of the global internet. In countries like Nigeria, South Africa, and Kenya, governments, banks, and major corporations heavily depend on global cloud providers and content delivery networks (CDNs), affecting policies, privacy, and resilience due to the influence of these external companies (Blumberg, Gelle, & Tamburro, 2024).

Theoretical Grounding/Framework

This study adopts a multi-theoretical approach, anchored in Cyber Sovereignty Theory, while also drawing upon insights from Realist perspectives on national security. Together, these frameworks provide a lens for analyzing how Liberia's dependence on foreign digital infrastructures limits its policy autonomy, exposes vulnerabilities in national security, and necessitates strategic interventions to achieve digital sovereignty.

Cyber Sovereignty Theory

Viewed as the most relevant theory, it confers the right on states to govern and control their digital space, data, networks, and ICT infrastructure, just as they control their physical territories (Hong & Goodnight, 2019). This right stems from national sovereignty, which governs and legitimizes the existence of states. This right, which is the dependent variable, comes with responsibilities (independent variables) that states must undertake to ensure digital sovereignty.

According to Mueller (2024), this right entails regulatory authority over content, infrastructure, data flows, and (in many formulations) determining what is permissible in cyberspace inside their borders. Similarly, Zhu et al (2016) identified key dimensions of the theory, which also border on the state's responsibility.

Internal control — regulation of infrastructure, censorship, surveillance, content moderation, etc. This is done through the formulation of relevant policy and strategy.

External recognition — asserting that other states should respect that internal authority (e.g., no interference). This ambition is also enhanced by policy and strategy.

Normative framing — through the same policy and strategy, states demonstrate the right to determine conditions of access, content, privacy, etc., often justified by claims to security, cultural integrity, public order, and so forth.

The fact that this theory confers the right of digital sovereignty on states does not guarantee absolute digital sovereignty. What it does is patrial sovereignty. As supported by realistic examples not too long ago, this is because of the profound global interdependence in data, infrastructure, and innovation ecosystems.

Realist Perspectives

The realist perspective on digital sovereignty can be understood by first recalling the core assumptions of realism in international relations (IR) and then seeing how these map onto debates about digital or cyber sovereignty.

Core Realist Assumptions

The theory, advanced by prominent scholars such as Waltz (1979), Morgenthau (1948), Mearsheimer (2001), and Walt (1978), is grounded in several core assumptions.

First, it posits that states are the principal actors within the international system, existing in a condition of "anarchy" with no overarching authority governing them (Walt, 1987). Second, the primary objective of states is to ensure their survival while maximizing their security and power, often assessed in terms of relative rather than absolute gains.

Sovereignty, defined as effective control over both territory and people, is a fundamental aspect of this perspective (Morgenthau, 1948). Realist notions of sovereignty view the state as the ultimate authority within its borders, possessing the power to regulate internal matters free from external interference.

Lastly, the anarchic nature of the international system leads states to adopt self-help strategies; they cannot rely on others for security, thereby engaging in power competition, balancing, and occasionally conflict (Waltz, 1979).

In light of these assumptions, digital sovereignty emerges as an extension or adaptation of these concerns within the realm of digital and dataspace.

When examining the concept of digital sovereignty through the lens of realism, several key themes emerge:

State control over digital infrastructure and data is viewed as an essential component of power and security. Realists interpret states' attempts to regulate digital infrastructure, data flows, networks, platforms, and cyberspace as critical to their national security and capacity to project power. For instance, Akhtar and Iqbal (2025) assert, "From a theoretical standpoint, cyber sovereignty aligns with realist theories of international relations, which emphasize the sovereignty and national interests of the state. The state will seek to claim ownership of any domain through which a threat could arise or be transmitted." This claim underscores how digital sovereignty is perceived as an extension of the realist focus on domains of power and control, such as territorial, economic, and military, into the digital sphere.

Realists stress that the state must maintain absolute authority within its borders. In the digital age, states consistently seek to assert jurisdiction over digital flows that cross traditional borders, including measures like data localization, control over cables, platforms, and regulation. As noted by Pierucci (2025), the notion of sovereignty necessitates control over territory, translated in digital terms as control over infrastructure and data flows.

In the context of the digital realm as a stage for power competition, realists view the digital domain not merely as a neutral platform for communication, but as a battleground for strategic competition. States seek to gain advantages, whether military, economic, or informational, while simultaneously attempting to deny similar advantages to others. On this claim, few scholars present substantial insight. Kanevskiy and Petrov (2024) expand on this viewpoint, asserting that "the weaponization and securitization of the Internet is a logical continuation of the crisis of the global liberal order." They contend that states are seeking to detach from a singular communicative space and to establish norms designed to safeguard themselves and their citizens from the overwhelming influence of Big Tech. This argument aligns with classic realist thought, wherein states perceive threats to their security, autonomy, and influence, prompting them to act accordingly in the digital realm.

According to Nye (2010), digital sovereignty encompasses infrastructure (servers, cables), regulation (data flows, platforms), and capability (cyber defense/offense), leading to a broader strategic competition among states. He further articulates that states may adopt digital sovereignty policies, such as data localization, nationalization of digital infrastructure, and platform control, in order to mitigate vulnerabilities to external influence or interference, such as cyber espionage, economic dependency, or platform dominance.

Moreover, Nye explains that despite the transnational nature of the Internet, states remain central actors striving to project power, protect

sovereignty, and control information domains, which reflects a realist perspective on cyberspace. Mearsheimer's theory of offensive realism posits that states compete for relative gains across all domains, including emerging digital spaces where sovereignty and security are at stake (Mearsheimer, 2001).

In his contribution to the discourse, Deibert (2013) argues that states are reasserting control over the Internet through surveillance, censorship, and cyber capabilities, a trend that is consistent with realist views of power politics in the digital landscape.

The Theory of Cyber Sovereignty Application to the Liberian Context

The theory of cyber sovereignty provides a framework for understanding the case of Liberia through two primary dimensions.

First, there is the rationale of national security. Liberia's ambitions to secure government systems, elections, financial assets, and sensitive data support the need for enhanced sovereign control, such as the implementation of laws, incident response mechanisms, and restrictions on detrimental foreign influence. The Liberia ICT Policy, along with official government communications, indicates that the country is actively pursuing a national cyber policy, a cybercrime bill, and the development of a robust cybersecurity advisory framework. These initiatives align with the principles of sovereignty and demonstrate Liberia's commitment to achieving digital sovereignty.

Second, there exists a significant capability gap that undermines this sovereignty. Data indices reveal that Liberia ranks low in terms of cybersecurity preparedness, suggesting that formal declarations of "sovereignty" lack substance unless accompanied by adequate capabilities, technical, legal, and human resources. In essence, genuine sovereignty necessitates capacity (as highlighted by the National Cyber Security Index, 2025).

In conclusion, applying the cyber sovereignty theory to Liberia reframes digital policy as a legitimate national security priority. However, the aspirations embedded in the theory must be supported by (1) tangible capacity building, (2) balanced legal protections for individual rights, (3) practical data governance that acknowledges economic and technical limitations, and (4) regional collaboration to prevent costly isolation or dependence. If Liberia approaches sovereignty as a strategic objective backed by measurable investments and safeguards, rather than merely a rhetorical aim, it can effectively enhance its digital sovereignty.

The Realist Perspective Application to the Liberian Context

The realist perspective provides a framework for understanding Liberia's situation from multiple dimensions.

First, there is strategic vulnerability due to dependence. From a realist standpoint, Liberia's reliance on external providers, coupled with its limited domestic infrastructure and developing cyber-governance, creates a dependency that could be exploited by rival or opportunistic states and transnational actors. This reflects a classic security concern regarding capability gaps and asymmetric dependence. While Liberia's official ICT policy and public communications indicate intentions to establish a government data center, a Computer Emergency Response Team (CERT), and upgrade infrastructure, the implementation of these plans has been inconsistent (Gaye, 2025).

Second, weak institutional and legal frameworks pose significant challenges. Liberia is in the process of developing legislation and agencies for addressing cybercrime and cybersecurity (e.g., the Liberia Cybersecurity and Privacy Management Agency; draft Cybersecurity Strategy). However, assessments and reviews by civil society reveal notable gaps in enforcement capacity, data protection institutions, and overall maturity on national cyber índices (Front Page Africa, 2025: Toe, 2024). Sober subscribers of the realist perspective would argue that until these capabilities are adequately strengthened, Liberia's bargaining power and its ability to safeguard its digital space will remain constrained.

Third, external partnerships serve both as a means of

mitigation and as leverage. International development partners, such as the World Bank, UNDP, ECOWAS, and the EU, play a significant role in Liberia's digital agenda by providing capabilities and investment (World Bank Group, 2025). However, they also influence decisions regarding suppliers, standards, and governance. Recent engagements with donors and national digital events indicate a heightened focus on finalizing policies and strategies. Sober subscribers to the realist perspective would interpret these partnerships as strategic hedges, beneficial in the short term, yet they create dependencies that require careful management.

Examination of Liberia's current digital Sovereignty Framework

The term "digital sovereignty framework" refers to a structured approach, comprising policies, rules, and technical architectures, through which an entity, such as a country, organization, or community, establishes control, autonomy, and resilience over its digital landscape, including data, infrastructure, software, and operations.

In other words, "digital sovereignty framework" refers to the collection of policies, technical controls, and governance mechanisms that facilitate the realization of sovereignty (Microsoft Ignite, 2025).

According to Microsoft Ignite (2025), the digital sovereignty framework can be best understood through three interrelated pillars:

Data Controls: These determine who has access to data, where it is stored, and how it is processed.

Operational Controls: These enable organizations to maintain transparency and authority over their digital operations.

Technological Independence: This entails selecting, managing, and securing the digital infrastructure and software stack without excessive reliance on foreign technologies or proprietary constraints.

Considering the menaing of digital sovereignty framework, no doubt Liberia has demonstrated the commitment to digital sovereignty framework. However, it does not yet have a completed and fully operational digital sovereignty framework in place. This assertion is supported by several facts.

The most recent document is the Liberia Information & Communications Technology (ICT) Policy (2019–2024), an amendment of the National Telecommunications and ICT Policy 2010-2015.

What does this policy include that support digital sovereignty?

National Data Center (NDC) — the policy explicitly requires building a Government National Data Center to host government systems, provide a central repository of national data, backup/disaster-recovery and support G2G/G2C services. A national data centre is a core technical step toward keeping sensitive government data under national control

Government-wide network (GovNet) & e-government hosting — the policy mandates a GovNet and government hosting so government services aren't fully dependent on foreign hosts for day-to-day operations

Management of the .lr ccTLD — the policy calls for localizing administrative/technical management of Liberia's country-code top level domain (.lr), which is an element of internet resource sovereignty

Cybersecurity & CERT and consumer privacy / data protection principles — the policy requires establishing cybersecurity structures (CERT) and sets out consumer privacy and data protection objectives based on universal principles, important legal/organizational pieces of sovereignty and control

Where the policy is limited (weaknesses vs. full digital sovereignty)

No clear, mandatory data-localization rule — the policy sets out data protection principles and promotes a national data centre but does not impose a blanket legal requirement that certain categories of "sovereign" or sensitive data must be stored only inside Liberia. That means data may still be hosted/processed offshore unless complementary law or procurement rules require otherwise.

Ownership / control and procurement details are vague — the policy often proposes PPPs and private

sector roles (e.g., carriers, cable consortiums, metro fiber), but does not always specify national ownership, governance safeguards or access/escrow/oversight conditions that prevent foreign control of critical infrastructure. The policy, therefore may enable foreign operators to host/operate infrastructure unless implementation contracts include sovereignty protections.

Implementation, capacity and funding dependency — the document repeatedly notes the need for funding, PPPs and regulatory follow-up; without well-resourced implementation, building the NDC, GovNet and cybersecurity institutions will lag — undermining the policy's promise. A regional analysis of African digital sovereignty shows that building data centers alone is insufficient without legal, procurement, and ownership measures.

Inarguably, the policy demonstrates Liberia's commitment by creating the framework and infrastructure priorities (NDC, GovNet, ccTLD, CERT, data-protection principles) needed to advance digital sovereignty. However, it does not by itself fully protect Liberia's digital sovereignty because it lacks mandatory localization / legal protections for sensitive data, explicit ownership/oversight conditions for privately run critical infrastructure, and depends heavily on implementation, procurement terms and complementary laws and regulations. Without those additional legal and contractual safeguards, sovereignty risks remain.

Next, the Personal Data Protection & Privacy Act of 2024.

Liberia has a draft bill titled the Personal Data Protection & Privacy Act of 2024 (or similar) that has been validated by stakeholders but has yet to be endorsed by the National Legislature (Toe, 2024).

Developed by the Ministry of Posts and Telecommunications (MoPT), with support from Internews under the European Union-funded Liberia Media Empowerment Project (LMEP), the proposed law, a standalone comprehensive instrument, is designed to provide structured guidance for the collection, processing, transmission, storage, protection, and use of personal information in Liberia (Toe, 2024).

Currently, Liberia does not have a standalone law on personal data protection. Once enacted, the legislation will supersede all other laws, decrees, executive orders, proclamations, and administrative regulations related to personal data. It aims to protect individuals' data without compromising the general interest of the state.

When passed into law, It will also impose penalties for unauthorized access, processing, and use of personal data, including the concealment of breaches and other malicious disclosures of personal information held by individuals and institutions responsible for managing such data.

One may argue that the Information & Communications Technology (ICT) Policy (2019–2024) and the Personal Data Protection & Privacy Act of 2024 are equivalent to a full digital sovereignty framework. On the contrary, they are not equivalent to a full digital sovereignty framework. This is because of one simple reason. That is , digital sovereignty involves not just data protection, but also control of digital infrastructure, local hosting, local capacity, procurement rules that favour national ownership/oversight. Reports show that in Liberia there are concerns over foreign-dominated contracts and lack of local-firm participation in key digital projects (which affects sovereignty) (Koinyeneh, 2025). Analysis shows these policies create an institutional and legal base that helps Liberia exercise some elements of digital sovereignty (regulation of networks, licensing, recognition of electronic transactions), but they do not by themselves provide full protection of digital sovereignty because important pieces are missing (data-protection/privacy, cybercrime, clear rules on data-localization, state access, and modern cybersecurity).

The bottom line is that these policies give Liberia the regulatory structure to govern telecommunications (a necessary condition for digital sovereignty). But without modern complementary laws — data protection/privacy, cybercrime and incident-response, and clear rules on state access and cross-border data flows, Liberia cannot fully exercise and defend its digital sovereignty in the ways states commonly do today.

Identification of Policy Gaps Affecting National Security

In the twenty-first century, Liberia's quest for digital sovereignty is still a vital part of national security, but the nation's capacity to protect its information space and digital infrastructure is still being threatened by serious policy gaps. A weak institutional and legal framework makes it difficult to manage cybersecurity, data protection, and digital governance, even with the creation of the Liberia National ICT Policy (2019–2024) and other related strategies. These flaws put Liberia at risk for threats like data breaches, cyberattacks, and reliance on foreign technology, all of which jeopardize national security and the defense of vital state resources. Therefore, bolstering Liberia's digital sovereignty and guaranteeing a safe and independent digital future depend on identifying and filling these policy gaps that also reflect the realist perspectives on Liberia's digital sovereignty pursuit.

Absence of a Comprehensive Digital Sovereignty Framework

As established under the subtopic that examines Liberia digital sovereignty framework, it is cystal that Liberia lacks an integrated national digital sovereignty policy that defines ownership, control, and protection of national data and digital infrastructure.

Implication for National Security: Without clear sovereignty boundaries, critical national data can be hosted, processed, or controlled by foreign entities, exposing the state to espionage, data manipulation, and cyber intrusión. Ministry of Posts and Telecommunications (2019). Liberia ICT Policy 2019–2024 acknowledges data security but provides no framework for asserting digital sovereignty.

Weak Cybersecurity Legislation and Enforcement

While the Liberia Cybercrime Act (2021) was enacted, enforcement mechanisms, institutional capacity, and coordination remain weak.

National Security Implications: Cyberattacks on financial systems, government databases, and communication networks could undermine national security and public trust. ECOWAS Commission (2022) noted that Liberia still lacks a fully operational Computer Emergency Response Team (CERT) and consistent cybersecurity strategy implementation. This concern from ECOWAS Commission resonates with the realist perspective that raised a red flag on the national security implication.

Absence of Data Protection and Privacy Regulation

Until passed ino law, Liberia has no Data Protection Act or independent Data Protection Authority to regulate data collection, storage, and transfer.

National Security Implication: Sensitive citizen and government data stored on foreign servers remain vulnerable to unauthorized access or exploitation, threatening sovereignty and national security. African Union (2022) Report on Data Protection Implementation in Africa highlights Liberia among states without a data protection legal framework. Again, this disclosure resonates with the realist perspectives, raising a red flag on this implication.

Limited Institutional Coordination on Digital Governance

Digital governance responsibilities are fragmented across the Ministry of Posts and Telecommunications, the Liberia Telecommunications Authority (LTA), and the National Security Agency (NSA) without a centralized coordinating mechanism.

National Security Implications: Overlaps and silos hinder intelligence sharing and unified cybersecurity defense. UNDP Liberia (2023) Digital Readiness Assessment emphasizes coordination and inter-agency integration as key gaps in Liberia’s digital transformation efforts. Of course, this gap aligns with the realist view alarmed security national security implications for Liberia.

Overdependence on Foreign ICT Infrastructure and Service Providers

Liberia relies heavily on external companies for internet backbone connectivity, cloud storage, and cybersecurity tools.

National Security Implications: External control of digital infrastructure can compromise data sovereignty and national command during crises or cyber conflicts. World Bank (2022). Liberia Digital Economy Country Assessment warns that reliance on foreign providers increases exposure to external vulnerabilities.

Low National Cybersecurity Awareness and Capacity

Limited training and awareness among government officials, law enforcement, and citizens weaken cyber defense.

National Security Implication: This human capacity deficit undermines national preparedness to identify and respond to digital threats.

ITU (2022) Global Cybersecurity Index ranked Liberia among low-performing states in cybersecurity capacity building.

Weak Integration of Digital Sovereignty in National Security Policy

National Security and Defense policies (e.g., National Security Strategy of Liberia, 2008) make minimal reference to digital sovereignty, cyber defense, or digital resilience.

National Security Implication: The absence of digital elements in security doctrine limits preparedness for cyber warfare, hybrid threats, and digital espionage.

Strategic Imperatives to Enhance Cyber Resilience and National Security.

Improving Liberia's national security and cyber resilience calls for a multipronged strategy that fills in current policy gaps and complies with strategic imperatives.

Strengthening Legal and Regulatory Frameworks

Goals to safeguard physical ICT infrastructure and deal with cybersecurity are outlined in Liberia's National ICT Policy (2019–2024). Nevertheless, the policy is devoid of specific provisions pertaining to cybercrime and cyberoffenses. According to a study assessing Liberia's cybercrime laws, effective enforcement and protection are hampered by the laws' incomplete conformity with international norms (Gilbert & Gilbert, 2024).

Strategic Imperative: Revise and enact comprehensive cybercrime legislation that aligns with international standards, ensuring robust legal frameworks for cybersecurity.

Enhancing Institutional Capacity and Coordination

The Liberia Cyber Crime Prevention and Mitigation Agency (LCCPMA), established in 2019, aims to provide cybersecurity and digital forensics education. Additionally, the Ministry of Post and Telecommunications is working towards establishing a Digital Forensic Laboratory to enhance national security and advance the country's cyber capabilities (Media Foundation of West Africa, 2020).

Strategic Imperative: Strengthen the capacity of LCCPMA and other relevant institutions through training, resource allocation, and inter-agency coordination to effectively address cyber threats.

Investing in Cybersecurity Education and Public Awareness

President Boakai has emphasized the importance of prioritizing cybersecurity, urging the legislature to fast-track the Cybercrime Bill (Michael, 2024). Furthermore, initiatives like the 24-hour cybersecurity hackathon aim to bridge the gap between classroom theory and hands-on practice, empowering youth and strengthening digital defense (Ashiru, 2025).

Strategic Imperative: Invest in cybersecurity

education and public awareness campaigns to build a knowledgeable workforce and an informed citizenry capable of recognizing and mitigating cyber threats.

Fostering Regional Collaboration and Compliance

Liberia's participation in regional initiatives, such as the ECOWAS Cybersecurity Strategy, underscores the importance of regional collaboration in addressing cyber threats (KPMG, 2022).

Strategic Imperative: Enhance regional collaboration by aligning national cybersecurity strategies with regional frameworks, ensuring compliance with international standards, and participating in joint initiatives to combat cyber threats.

Developing a National Cybersecurity Strategy

The National Security Strategy of Liberia, published in 2008, provided guidelines on improving coordination and oversight of multi-agency security activities. However, the evolving nature of cyber threats necessitates the development of a comprehensive National Cybersecurity Strategy.

Strategic Imperative: Develop and implement a National Cybersecurity Strategy that outlines clear objectives, roles, and responsibilities, ensuring a coordinated and effective response to cyber threats.

In summation, Liberia can improve its cyber resilience and national security by tackling these strategic imperatives: bolstering legal frameworks, building institutional capacity, advancing digital sovereignty, investing in education, encouraging regional cooperation, and creating a thorough cybersecurity plan. In addition to safeguarding vital infrastructure, these initiatives will promote a safe online environment that supports national growth.

Conclusion

This article set out to address three interrelated research objectives: the examination of Liberia's current digital sovereignty framework, the identification of policy gaps affecting national security, and the proposition of strategic imperatives to strengthen cyber resilience and national security. Guided by the theoretical framework, these objectives have been systematically explored and achieved.

The analysis underscores the critical nexus between technological autonomy and national security in Liberia. The country's current digital landscape reveals significant policy gaps that undermine its strategic resilience. Drawing on digital sovereignty theory, which asserts a state's inherent right and capacity to regulate, control, and protect its digital infrastructure, data, and cyberspace environment, it is evident that Liberia's ability to exercise full digital self-determination is constrained. These gaps, including weak institutional capacity, inadequate regulatory frameworks, and dependence on foreign digital platforms, expose the nation to both internal and external cyber threats.

From a realist perspective, the pursuit of digital sovereignty is not merely a technical or administrative concern but a strategic imperative. Liberia's national security is increasingly intertwined with its ability to control its digital space, as power projection in the twenty-first century relies heavily on information dominance and cyber capabilities. The realist lens highlights that unaddressed policy deficiencies could compromise Liberia's sovereignty, leaving critical infrastructure, governance mechanisms, and socio-economic networks vulnerable to manipulation or coercion by more technologically advanced states or non-state actors.

Strategically, the development and rigorous implementation of comprehensive policies to address these gaps are essential. This includes robust cybersecurity legislation, targeted investments in ICT capacity building, public-private partnerships to enhance technological resilience, and the establishment of a national data governance framework that safeguards national interests while adhering to international best practices. By proactively embedding digital sovereignty within its national security architecture, Liberia can strengthen its defensive posture, reduce dependency on external actors, and assert a credible role in the global digital

ecosystem.

Ultimately, achieving digital sovereignty serves both as a tool of state power and as a reflection of Liberia's commitment to national security. A forward-looking, realist-informed approach to closing policy gaps is crucial to ensuring that Liberia navigates the complex digital environment as a secure, independent, and strategically capable actor in the twenty-first century.

Disclaimer

The views and opinions expressed in this article are those of the author and do not necessarily reflect the official policy or position of any affiliated organization, institution, or employer. All content provided is for academic and informational purposes only. The author makes no representations as to the accuracy, completeness, suitability, or validity of any information contained herein and will not be liable for any errors, omissions, or delays in this information or any losses, injuries, or damage(s) arising from its display or use. Readers are advised to verify any information before acting upon it.

REFERENCES

Ashiru, G. (2025). Liberia Launches 24-Hour Cybersecurity Hackathon to

Empower Youth and Strengthen Digital Defense

https://www.techinafrica.com/liberia-launches-24-hour-cybersecurity-hackathon-to-empower-youth-and-strengthen-digital-defense/

Akhtar, N. & Iqbal, A. R. (2025). Cyber Sovereignty: National Security in the

Digital Age

Baldoni, R. & Di Luna, G. (2025). Sovereignty in the digital era: the quest for

continuous access to dependable technological capabilities

https://doi.org/10.1109/MSEC.2024.3500192

Braun, M. &, P. Hummel (2024). Is digital sovereignty normatively desirable?

ttps://doi.org/10.1080/1369118X.2024.2332624

Blumberg, S. Gelle, J. C., & Tamburro, I. (2024). Africa's leap ahead into cloud:

Opportunities and barriers

https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/africas-leap-ahead-into-cloud-opportunities-and-barriers?utm

DeNardis, L. (2020). The Internet in Everything: Freedom and Security in a

World with No Neutrality. Yale University Press.

DIN news desk (2025). Morocco asserts digital sovereignty with green data

center plan

https://digitalinfranetwork.com/news/morocco-asserts-digital-sovereignty-with-green-data-center-plan/

Deibert, R. (2013). Black Code: Inside the Battle for Cyberspace. Toronto:

Signal/McClelland & Stewart.

Department of Communications and Digital Technologies (2024). Electronic

Communications Act of 2005.

https://www.gov.za/sites/default/files/gcis_document/202406/50741gen2533.pdf

Executive Mansion (2024). President Boakai Opens 3-Day Cybersecurity

Conference to Address Growing Global Cybercrime Threat in Liberia

https://www.emansion.gov.lr/media/press-release/president-boakai-opens-3-day-cybersecurity-conference-address-growing-global?

Fratini

Frontpage Africa (2025). Liberia: Internews Liberia, Partners Hold Intensive

Orientation for Legislative Journalists On Draft Data

Protection, Cybercrime Laws

https://allafrica.com/stories/202506260199.html?utm

Gaye, F. (2025). Liberia struggles to enforce privacy and data protection laws

https://africachinareporting.com/liberia-struggles-to-enforce-privacy-and-data-protection-laws/?utm

Gilbert, C & Gilbert, M. A. (2024). Bridging the Gap: Evaluating Liberia's

Cybercrime Legislation against International Standards

DOI: https://doi.org/10.51584/IJRIAS.2024.910013

Hulkó, G. Kálmán, J. & Lapsánszky, A. (2025). the politics of digital

Sovereignty and the European Union's legislation: navigating crises

https://doi.org/10.3389/fpos.2025.1548562

Hong, Y. & Goodnight, T. (2019). How to think about cyber sovereignty: the

Case of China DOI:10.1080/17544750.2019.1687536

INTERPOL (2025). New INTERPOL report warns of sharp rise in cybercrime in

Africa

https://www.interpol.int/en/News-and-Events/News/2025/New-INTERPOL-report-warns-of-sharp-rise-in-cybercrime-in-Africa?

Internet Society (2022). Navigating Digital Sovereignty and its Impact on the

Internet https://www.internetsociety.org/wp-content/uploads/2022/11/Digital-Sovereignty.pdf?

Kuerbis, B. (2020). Cybersecurity, digital sovereignty, and national security.

Journal of Strategic Security, 13(1), 45–62.

Kanevskiy, P. S. & Petrov, K. Y. (2024). Digital Actors and Digital Platforms in

the System of International Relations: Between Complex Interdependence and Online Sovereignty

https://doi.org/10.46272/2587-8476-2024-15-3-37-56

Koinyeneh, G. (2025). Liberian ICT Firms Warn of Sovereignty Risk in Foreign-

Dominated Contracts Local Tech Leaders Call for Fair Procurement, Protection of National Data Systems

https://allafrica.com/stories/202508190251.html

KPMG (2022). Advancing Cybersecurity with Africa

https://thegfce.org/wp-content/uploads/2023/05/GFCE-Final-Report-Advancing-Cybersecurity-With-Africa.pdf?

Media Foundation of West Africa (2020). State of Internet Foundation in

Liberia. https://www.mfwa.org/wp-content/uploads/2021/10/State-of-Internet-Freedom-In-Liberia-2020.pdf

Maurer, T. (2018). Cyber Mercenaries: The State, Hackers, and Power.

Michael, T. (2024). Fortifying Liberia's Digital Frontier: President Boakai's

Cybersecurity Vision for National Resilience

https://www.insightsliberia.com/post/fortifying-liberia-s-digital-frontier-president-boakai-s-cybersecurity-vision-for-national-resilien? Utm

Mueller, M. (2024). The Debate on Sovereignty in Cyberspace

https://www.internetgovernance.org/2024/12/31/the-debate-on-sovereignty-in-cyberspace/

Mearsheimer, J J. (2001). The Tragedy of Great Power Politics. New York: W. W.

Norton & Company

Morgenthau, H. J. (1948). Politics among Nations: The Struggle for Power and

Peace. New York: Alfred A. Knopf.

Microsoft Ignite (2025). Digital sovereignty

https://learn.microsoft.com/en-us/industry/sovereign-cloud/overview/digital-sovereignty?utm

Nigeria Data Protection Act (2023). https://placng.org/i/wp-

content/uploads/2023/06/Nigeria-Data-Protection-Act-2023.pdf

National Cyber Security Index (2025). Liberia

https://ncsi.ega.ee/country/lr_2022/?pdfReport=1&utm

Nye, J. S. (2010). Cyber Power. Harvard University, Belfer Center for Science

and International Affairs.

Peters, L. G. (2024). Liberia Government faces cyber attacks

https://www.tlcafrica1.com/govt-faces-cyber-attacks/

Pohle, D. (2020). Digital sovereignty DOI: 10.14763/2020.4.1532

Pierucci, F.(2025). Sovereignty in the Digital Era: Rethinking Territoriality and

Governance in Cyberspace

https://doi.org/10.1007/s44206-025-00189-4

Smart Rwanda 2020 Master Plan (2015).

https://www.minict.gov.rw/fileadmin/user_upload/minict_user_upload/Documents/Policies/SMART_RWANDA_MASTERPLAN.pdf

Segal, A. (2019). The Hacked World Order: How Nations Fight, Trade,

Maneuver, and Manipulate in the Digital Age. PublicAffairs.

The Guardian (2016). Massive cyber-attack grinds Liberia's internet to a halt

https://www.theguardian.com/technology/2016/nov/03/cyberattack-internet-liberia-ddos-hack-botnet?

Toe, B. N. (2024). Stakeholders Endorse Draft Legislation for Personal Data

Privacy and Protection

https://liberianinvestigator.com/news/stakeholders-endorse-draft-legislation-for-personal-data-privacy-and-protection/?utm

Waltz, K. N. (1979). Theory of International Politics. Reading, MA: Addison-

Wesley.

Walt, S. M. (1987). The Origins of Alliances. Ithaca: Cornell University Press.

World Bank Group (2025). Digital Liberia Week: Empowering Liberia’s Digital

Future

https://www.worldbank.org/en/events/2025/10/22/digital-liberia-week?utm

Zhu et al (2016). A Review of Major Viewpoints on Cyber Sovereignty around

the World DOI: 10.15302/J-SSCAE-2016.06.018

About the Author

Dr. Ambrues Monboe Nebo is an interdisciplinary researcher and senior police officer with over 20 years of experience in training, administration, and security intelligence. He holds academic backgrounds in Sociology, Peace and Conflict Studies, Humanitarian and Refugee Studies, Public Administration, Law Enforcement, and Peacekeeping. He is currently pursuing a Ph.D. in Security Studies at Hill-City University, Benin. He has taught at several universities in Liberia, served in academic leadership roles, and reviews for IJRISS. Dr. Nebo is the author of four books and numerous scholarly articles on Liberia and Africa's socio-political issues, available on Amazon, Academia.edu, ResearchGate, and Google Scholar. His academic profile is https://neboambrues.academia.edu in where his scholarly work can be assessed.