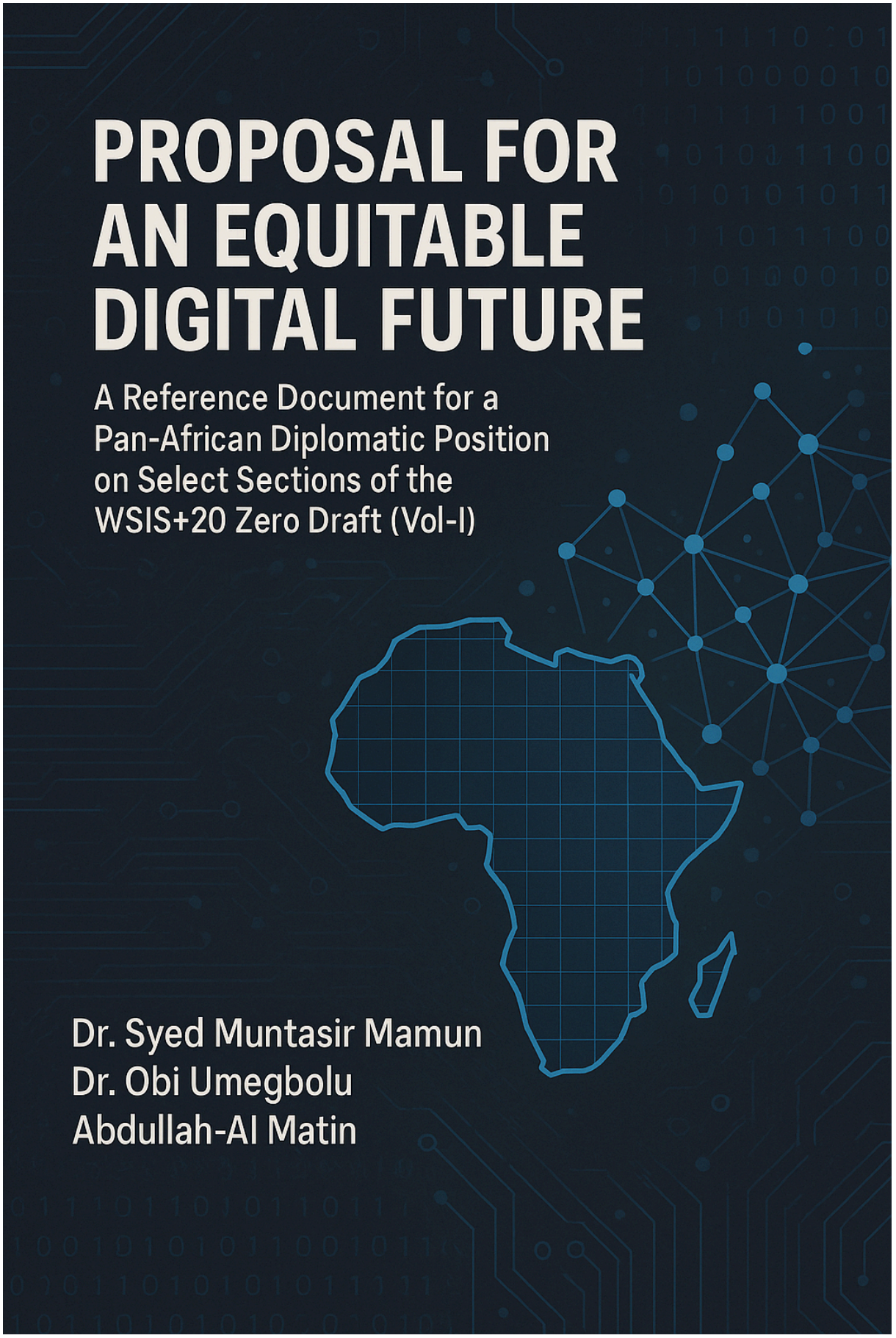
PROPOSAL FOR AN EQUITABLE DIGITAL FUTURE
A Reference Document for a Pan-African Diplomatic Position on Select Sections of the WSIS+20 Zero Draft (Vol-I)
Dr. Syed Muntasir Mamun
Dr. Obi Umegbolu
Abdullah-Al Matin

Proposal for an Equitable Digital Future: A Reference Document for a Pan-African Diplomatic Position on Select Sections of the WSIS+20 Zero Draft (Vol-I)

Abstract

The African continent's position on the **WSIS+20 Zero Draft Outcome Document** is presented as a diplomatic and developmental imperative, designed for the consideration of negotiating stakeholders. This paper asserts that the current draft, while reaffirming high-level principles, requires **actionable, financially backed, and rights-respecting commitments** to bridge the structural digital divides confronting African nations.

The comprehensive strategy is articulated across five critical pillars:

1. **Connectivity and Affordability:** Urging the adoption of a **2% GNI affordability target** for 2GB of mobile data to ensure meaningful access and dismantle the primary economic barrier to digital inclusion (ITU, 2022).
2. **Digital Sovereignty and Security:** Advocating for explicit support for **sovereign data governance** and capacity building, leveraging models like South Africa's POPIA to secure national data resources and mitigate technological dependency (Policy, 2024).
3. **Finance and Investment:** Demanding the endorsement of **innovative financing**—including blended finance and mechanisms linking debt instruments to resilient digital infrastructure—to sustainably close the continent's substantial ICT funding gap (AIFAT, 2025).
4. **Finance, Trust, Human Rights and Digital Freedom:** Calling for a clear international commitment to an end to disproportionate **digital restrictions and digital constrictions**, which pose substantial threats to human rights, economic stability, and humanitarian efforts (Global Network Initiative, 2025).
5. **Digital Public Infrastructure (DPI):** Proposing support for an **Africa-centric, interoperable DPI model** to accelerate economic integration, facilitate the African Continental Free Trade Area (AfCFTA), and unlock the potential of youth and women-led entrepreneurship (Carnegie Endowment, 2025).

This document serves as a strategic roadmap, respectfully urging negotiators to incorporate these specific, evidence-based amendments to ensure the WSIS+20 outcome is a **transformative catalyst** for a truly inclusive, sovereign, and resilient digital future for the Global South.

Publication Details

Title: Proposal for an Equitable Digital Future:A Reference Document for a Pan-African Diplomatic Position on Select Sections of the WSIS+20 Zero Draft (Vol-I)

Authors: Dr. Syed Muntasir Mamun, Dr. Obi Umegbolu,Abdullah-Al Matin.

Publisher:AI for Africa Thinktank (AIFAT)A leading thinktank dedicated to advancing artificial intelligence in Africa, committed to transforming the continent through AI by engaging with academia, industry, governments, and communities.

Website: https://aifat.orgContact: info@aifat.orgAddress: [Redacted for privacy; please visit website for details]Established: 2023
Publication Date:2025
Edition: First Edition (Advisory Note)

Disclaimer: The views expressed in this document are those of the authors and do not necessarily reflect the official policy or position of AIFAT or any affiliated organizations. Critiques are NOT directed any government(s) in particular but calls for a generic and general appeal to a spirit of freedom, innovation and entrepreneurship in an environment of agency and franchise. While every effort has been made to ensure the accuracy of the information contained herein, the authors and publisher assume no responsibility for any errors or omissions.

Typefaces:

- Body Text: Times New Roman, 11.5 pt
- Footnotes and References: Times New Roman, 10 pt
- Designed using Adobe InDesign for layout and formatting.

Printing and Binding:Printed on acid-free paper for archival quality.Bound in softcover format.

Reference number: AIFAT-CS-00620251105

JEL Classification:O10 (Economic Development: General)O33 (Technological Change: Choices and Consequences; Diffusion Processes)O38 (Technological Change: Government Policy)O55 (Economywide Country Studies: Africa)L86 (Information and Internet Services; Computer Software; Digital Economy)L96 (Telecommunications)

Acknowledgments: This publication was made possible through the collaborative efforts of the AIFAT Advisory team and contributions from African stakeholders. Special thanks to the WSIS+20 negotiation participants for their insights.

For inquiries or permissions, contact: info@aifat.org

Table of Contents

Prologue

In the vast expanse of the digital frontier, where innovation converges with opportunity, Africa emerges not as a peripheral actor but as a central force shaping the global narrative. Two decades since the inception of the World Summit on the Information Society (WSIS), the WSIS+20 Review stands as a pivotal juncture—a moment to reflect on progress made and inequities endured. This document, born from the collective wisdom of African thinkers, diplomats, and visionaries, is more than a policy advisory; it is a clarion call for equity in an era where data flows like rivers and technology bridges or divides nations. As the continent harnesses its youthful dynamism and resilient spirit, we propose a Pan-African stance that transcends rhetoric, demanding actionable commitments to sovereignty, inclusion, and prosperity. Herein lies the blueprint for an equitable digital future, where Africa's voice echoes not in echoes of the past but in the bold strides toward tomorrow.

EXECUTIVE SUMMARY

This Advisory Note, presented by the AI for Africa Thinktank (AIFAT), serves as a strategic diplomatic roadmap for African negotiators and stakeholders involved in finalizing the World Summit on the Information Society (WSIS)+20 Zero Draft Outcome Document. It asserts that while the existing Zero Draft is philosophically sound, it lacks the concrete, financially backed, and rights-respecting commitments necessary to dismantle the structural digital divides confronting African nations.

The report's core justification is to move the global digital agenda from mere principle-reaffirmation to measurable action, ensuring Africa is a sovereign and equal participant in the global digital future.

Core Strategic Pillars

The report’s strategy is articulated through five critical pillars (detailed in the main body) and is significantly strengthened by the four forward-looking pathways presented in Annex B.

Main Pillars (Vol-I)	Strategic Goal	Potential Sensitivity
Pillar I: Connectivity and Affordability	To translate aspirational goals into measurable, enforceable affordability targets, specifically by urging the adoption of a 2% GNI affordability target for 2GB of mobile data.	None (High consensus target)
Pillar II: Finance and Investment	To address the estimated annual $3 billion ICT funding gap by mandating blended finance models, debt instruments linked to resilient digital infrastructure, and a fair allocation of Special Drawing Rights (SDRs) for digital development.	Low (High consensus on finance needs)

Main Pillars (Vol-I)	Strategic Goal	Potential Sensitivity
Pillar III: Digital Sovereignty and Data Governance	To mandate international support for the development of secure, sovereign, and Africa-centric Digital Public Infrastructure (DPI) and data governance capacity, ensuring local data creates local value.	None (High consensus on sovereignty)
Pillar IV: Protecting Human Rights and Digital Freedoms	To secure a clear international commitment to an end to disproportionate digital restrictions and censorship, establishing safeguards against politically motivated digital constrictions.	High (Potential friction point with governments employing digital restrictions for stability/security).
Pillar V: Inclusion and Capacity Building	To secure explicit commitments and resources for closing the gender and youth digital divide through targeted skills programs and ensuring the meaningful participation of marginalized groups in digital policy.	None (High consensus on inclusion)

Annexes and Future Pathways

The document includes vital supplementary annexes to guide negotiators on cutting-edge policy areas:

Annex	Title	Immediate Future Pathway
Annex A	(Implied: Proposed WSIS Textual Amendments)	Contains the specific, line-by-line revisions and diplomatic interventions proposed for the

Annex	Title	Immediate Future Pathway
		WSIS+20 Zero Draft outcome text, operationalizing the five core pillars.
Annex B	Pathways into the Immediate Future: Proposed New Pillars	Outlines four additional thematic areas critical for Africa's long-term digital resilience and global competitiveness: AI Governance, Digital Trade Harmonization, Cybersecurity Resilience, and robust Monitoring & Evaluation (M&E) mechanisms.
Annex C	(Implied: Conceptual Framework)	Provides the theoretical foundation, referencing concepts like Fluid Institutions and Fluid Institutionalism (a policy model for dynamic regulatory adaptation) as a strategic tool for future-proofing African governance against rapidly evolving technologies like AI.

The report concludes that only a respectfully assertive diplomatic posture, backed by these specific, measurable proposals, will ensure that the final WSIS+20 outcome serves as a catalyst for genuine, equitable digital transformation across the African continent.

A Diplomatic Proposal for an Equitable Digital Future: The African Position on the WSIS+20 Zero Draft

1.0 Introduction

The World Summit on the Information Society (WSIS) established a global framework for a people-centred, inclusive, and development-oriented Information Society. As the global community prepares for the **WSIS+20 Review in 2025**, the resulting Zero Draft outcome document presents a critical juncture to evaluate two decades of progress and chart the future of digital cooperation (African Perspective Note, 2025). This paper is specifically structured as a high-level briefing document intended for the **stakeholders, delegates, and negotiating bodies** responsible for finalizing the WSIS+20 outcome text. For the African continent, this review is not merely an administrative exercise but a pivotal opportunity to address systemic inequalities embedded in the current digital architecture. While significant progress has been made—evidenced by flourishing innovation hubs, robust fintech adoption, and increasing connectivity rates in key markets (AIFAT, 2025)—Africa continues to grapple with foundational challenges: a persistent digital divide, unsustainable data costs, and an unequal voice in global digital governance (WSIS Africa Perspectives, 2025). This position paper serves to articulate a unified, comprehensive, and respectfully assertive African perspective, ensuring the final WSIS+20 outcome moves beyond principle-reaffirmation to concrete, development-focused commitments that align with the continent's sovereign visions and the objectives of the African Union’s Agenda 2063.

2.0 Problem Statement

The central challenge addressed by this paper is that **the current WSIS+20 Zero Draft outcome document, while philosophically sound, lacks the concrete, measurable, and structural commitments necessary to dismantle the persistent barriers that perpetuate digital inequality for African nations.**

This gap manifests through three primary structural impediments:

1. **Financial Imbalance and Affordability:** The Zero Draft needs to work on prescribe innovative mechanisms to address the estimated **$3 billion annual ICT funding gap** and the high national debt burdens that restrict domestic investment, requiring to further work on generating actionable targets for reducing mobile data costs that remain economically prohibitive for the majority of the population (AIFAT, 2025).
2. **Sovereignty and Security Deficit:** The initial draft of the document shows some deficits in robust in mandating international support for the development of secure, sovereign data infrastructure and capacity building, leaving African nations vulnerable to technological dependency, exploitation, and threats to national data security - in spite of the ongoing public and private sector engagements for sponsoring innovation and entrepreneurship via tech generation (WSIS Africa Perspectives, 2025). The remakrable success of the likes of the

Nigerian fintech blossom needs encouragement and support from the global comity of nations (AIFAT, 2025)

3. **Trust, Human Rights and Governance:** The Zero Draft be strengthened to incorporate more explicit and robust language, which will facilitate the establishment of clear, enforceable guidelines for minimizing and managing digital restrictions. Such an inclusive approach is crucial to mitigate potential risks to fundamental human rights, preserve economic continuity, and ensure the uninterrupted provision of essential services across the continent. Ultimately, securing and maintaining trust within the state system and its apparatus is an indispensable foundation for the entire framework of an equitable Information Society.

3.0 Aim

The primary aim of this paper is to **propose targeted, actionable revisions and additions to the WSIS+20 Zero Draft outcome document** that effectively translate the shared vision of a development-oriented Information Society into measurable commitments. Specifically, the paper aims to secure consensus on measures that:

1. Establish concrete and time-bound targets for achieving affordable, meaningful connectivity.
2. Foster the development of sovereign Digital Public Infrastructure (DPI) and secure data governance frameworks across the continent.
3. Mandate the protection of digital human rights, particularly for restrictions like digital restrictions, and ensure inclusive participation of women, youth, and underserved populations .

4.0 Scope

The scope of this comprehensive analysis is defined by the following boundaries:

- **Geographical Focus:** The paper exclusively concentrates on the collective and diverse perspectives of African Union member states, drawing upon some illustrative national priorities to illustrate pan-African challenges.
- **Thematic Focus:** The analysis is strictly confined to five key thematic pillars that represent the continent's highest priorities for the WSIS+20 review: Universal Connectivity & Affordability, Digital Sovereignty & Data Governance, Finance & Investment, Human Rights & Inclusion, and Digital Public Infrastructure (DPI) & Innovation.
- **Documentary Focus:** The examination is limited to analyzing and proposing amendments to the text of the WSIS+20 Zero Draft outcome document, informed by official African regional consultation reports and expert policy briefs.

Based on the content of the document, the section on the justification and purpose of the report can be structured as follows:

5.0 Justification and Purpose of the Report

This report, Proposal for an Equitable Digital Future: A Reference Document for a Pan-African Diplomatic Position on Select Sections of the WSIS+20 Zero Draft (Vol-I), serves as a high-level briefing and strategic intervention in global digital policy.

Rationale and Justification

The primary justification for this advisory note is the recognition that the World Summit on the Information Society (WSIS)+20 Review presents a pivotal opportunity for Africa to address systemic inequalities embedded in the current global digital architecture. The document argues that while the existing WSIS+20 Zero Draft outcome is "philosophically sound," it currently is in need of a more concrete, measurable, and structural commitments necessary to dismantle persistent barriers that perpetuate digital inequality for African nations. The report is justified by three primary structural impediments facing the continent:

* Financial Imbalance and Affordability: The Zero Draft needs to prescribe innovative mechanisms to address the estimated $3 billion annual Information and Communication Technology (ICT) funding gap and tackle the high national debt burdens that restrict domestic digital investment.

* Sovereignty and Security Deficit: The initial draft shows a deficit in mandating robust international support for the development of secure, sovereign data infrastructure and capacity building, leaving African nations vulnerable to technological dependency and exploitation.

* Trust, Human Rights, and Governance: The need for stronger, more explicit language to establish clear, enforceable guidelines for minimizing and managing digital restrictions, which pose threats to human rights, economic continuity, and essential services.

The Ends it Serves (Primary Aims)

The core purpose of the paper is to propose targeted, actionable revisions and additions to the WSIS+20 Zero Draft outcome document, effectively translating the shared vision of a development-oriented Information Society into measurable commitments.

Specifically, the report serves the following ends:

* To Articulate a Unified Position: It serves to articulate a unified, comprehensive, and respectfully assertive African perspective to ensure the final outcome moves beyond mere principle-reaffirmation to concrete, development-focused commitments.

* To Achieve Measurable Commitments: It aims to secure consensus on measures that:

* Establish concrete and time-bound targets for achieving affordable, meaningful connectivity.

* Foster the development of sovereign Digital Public Infrastructure (DPI) and secure data governance frameworks across the continent.

* Mandate the protection of digital human rights and ensure the inclusive participation of women, youth, and underserved populations.

* To Align Global Policy with African Vision: Ultimately, the document's end goal is to align global efforts with the continent's sovereign visions and the specific objectives of the African Union’s Agenda 2063.

Status Update for Negotiators

This initial submission provides the foundational context, problem statement, and strategic aim of the African Position. The following sections—**Pillars I through IV**—will provide the detailed diplomatic arguments, supported by specific country use cases and robust evidence.

6.0. Pillar I: Universal, Meaningful, and Affordable Connectivity

Intervention: African nations note the urgency of addressing the affordability gap, which remains a primary barrier to universal access, far outweighing infrastructure deficits alone (WSIS Africa Perspectives, 2025).

Rationale: African nations are increasingly emphasizing that while infrastructure development is crucial, the most significant impediment to achieving universal digital access is not solely a deficit in physical connectivity, but rather the pervasive challenge of the affordability gap. This perspective, highlighted in recent discussions such as the WSIS Africa Perspectives report in 2025, underscores a critical shift in focus. The cost associated with access—including mobile data, devices, and necessary digital skills training—far outweighs the problems presented by infrastructure shortcomings alone. High taxes on ICT equipment and services, coupled with generally low household incomes across the continent, render digital participation an unattainable luxury for a vast segment of the population, even in areas where network coverage is present. Addressing this economic barrier through policy interventions, subsidies, and innovative financing models is now recognized as the most urgent and direct route to meaningfully close the digital divide and unlock the continent's full potential for social and economic transformation.

6.1. Proposal: Actionable Affordability Targets (Para 28, 62)

Intervention: The continent respectfully suggests strengthening **Paragraphs 28 and 62** to endorse the goal of achieving broadband access where the cost of 2GB of data is reduced to **below 2% of average monthly gross national income (GNI) per capita**.

Rationale: The continent, through its collective engagement and analysis of current global digital development strategies, respectfully suggests a substantive strengthening of Paragraphs 28 and 62 within the relevant policy framework. This proposed revision is aimed at formally endorsing and establishing a more ambitious and measurable global target for digital inclusion.

Specifically, the suggested modification is to explicitly state the goal of achieving widespread and affordable broadband access, quantified by the metric that the cost of a minimum benchmark data package of **2GB** ought to be reduced to **below 2% of the average monthly gross national income (GNI) per capita**.

This targeted financial threshold is considered critical for several reasons:

1. **Bridging the Affordability Gap:** The current global average cost often presents a significant barrier to entry, particularly in developing nations. Adopting the 2% target, widely recognized as the global standard for affordability, directly addresses this digital divide rooted in economic disparity.
2. **Driving Universal Access:** By setting a concrete, measurable, and time-bound affordability goal, the policy framework will catalyze necessary investments and regulatory reforms to ensure broadband is accessible to the poorest and most marginalized populations.
3. **Fostering Digital Economy and Social Inclusion:** Achieving this affordability target is essential for realizing the full socio-economic benefits of connectivity, including participation in the digital economy, access to essential services (education, health), and overall social empowerment.

The strengthening of **Paragraphs 28 and 62** with this specific metric will transform the policy from a general statement of intent into a practical, verifiable roadmap for achieving meaningful and sustainable digital transformation across the continent and the world.

- **Use Case and Rationale: The Persistent Global Digital Divide in Mobile Broadband Cost**

While the global trend shows a positive trajectory, with mobile broadband costs decreasing to an average of 1.3% of Gross National Income (GNI) per capita in 2023, a significant and concerning disparity persists. Data from 2022 reveals that mobile broadband in the median low-income economies cost approximately **seven times more** relative to income than the world median (Lucidity Insights, 2024; ITU, 2022). This staggering cost differential creates a profound barrier to genuine "meaningful" digital access.

This disparity disproportionately impacts countries across the developing world. In many of these economies, the high effective cost of data severely limits the capacity of the majority of the population to engage in the digital economy, access essential online services (such as e-health and e-education), and participate fully in civil society (WSIS Africa Perspectives, 2025). High data costs transition access from a tool for development into a luxury good, constraining economic participation and hindering national productivity.

To effectively bridge the global digital divide and unlock mass digital inclusion, achieving the global affordability target—where 1 Gigabyte (1GB) of mobile broadband data costs 2% or less of GNI per capita—is absolutely vital. Reaching this 2% threshold is not merely a statistical goal; it represents the inflection point where mobile connectivity becomes accessible to the poorest segments of society, transforming it from a luxury into a fundamental utility for economic and social empowerment. The current cost gap highlights the urgent need for targeted policy interventions, infrastructure investment, and regulatory reforms focused on reducing the effective price of data in low-income markets.

6.2. Proposal: Resilient Financing and Infrastructure (Para 72, 73)

Intervention: African stakeholders encourage the Zero Draft to facilitate **innovative financing mechanisms** (Para 76) that move beyond traditional loans, focusing on resilience.

Rationale: African stakeholders have strongly urged that the Zero Draft of the upcoming global framework ought to prioritize and facilitate the establishment of innovative financing mechanisms (as noted in Para 76). This encouragement stems from a collective understanding that current approaches, which heavily rely on traditional, debt-creating loans, are often inadequate for the scale of development and climate challenges facing the continent. The proposed shift is towards diverse, creative, and non-debt instruments that specifically focus on building and enhancing **resilience** across various sectors, including climate adaptation, healthcare, food security, and infrastructure development. The goal is to move beyond short-term financial fixes to secure long-term, sustainable economic stability and growth.

Rationale for the Proposal Innovative Financing:

The demand from African stakeholders for a paradigm shift in development finance is critical and urgent. The continent is disproportionately impacted by global crises, including the accelerating effects of climate change, persistent public health deficits, and economic volatility. Traditional financing, primarily composed of sovereign debt, has proven to be a double-edged sword. While it provides immediate capital, the resultant debt burden often constrains fiscal space, forcing governments to allocate significant

portions of their budgets to debt servicing rather than essential social and economic investments. This cycle ultimately undermines the very goal of sustainable development.

Therefore, the prioritization of **innovative financing mechanisms** in the global framework is non-negotiable for African nations. These mechanisms are envisioned to be diverse and multi-faceted, potentially including:

1. **Non-Debt Instruments:** Focusing on equity investments, blended finance structures that de-risk private sector participation, guarantees, and results-based financing models such as development impact bonds (DIBs).
2. **Global Taxation and Levies:** Exploring possibilities for global financial transaction taxes, carbon levies on international shipping or aviation, or similar mechanisms that generate predictable, non-repayable revenue streams for development and climate action.
3. **Harnessing Natural Capital:** Developing robust frameworks for 'debt-for-nature' or 'debt-for-climate' swaps, which simultaneously reduce debt and finance conservation or climate adaptation projects.
4. **Special Drawing Rights (SDRs) Rechanneling:** Advocating for more effective and equitable rechanneling of underutilized SDRs from developed to developing countries, moving beyond simply loaning them back through multilateral development banks.

The core objective of this shift is not just to secure funding, but to fundamentally build and enhance **resilience** across the continent. This resilience must be systemic, encompassing:

- **Climate Adaptation:** Financing for early warning systems, climate-resilient infrastructure (e.g., roads, energy grids), and sustainable land-use practices.
- **Healthcare Systems:** Investment in local pharmaceutical manufacturing, strengthening primary healthcare networks, and enhancing pandemic preparedness.
- **Food Security:** Support for climate-smart agriculture, irrigation projects, and resilient supply chains to insulate populations from external shocks.
- **Sustainable Infrastructure:** Funding for transformative, regional infrastructure projects, particularly in renewable energy and digital connectivity, using models that minimize debt creation.

The eventual goal is a transition from a reliance on short-term financial fixes to a long-term strategy for achieving self-sustaining economic stability and inclusive growth, empowering African nations to better navigate and recover from future global shocks. The new global framework must serve as the political and legal catalyst for this financial transformation.

Use Case and Rationale for Digital Resilience Investment

Countries grappling with high susceptibility to external, non-financial shocks—ranging from sudden public health crises and climate-induced disasters to geopolitical instability and supply chain disruptions—are poised to realize significant and transformative benefits from concerted, targeted international support aimed at fortifying and expanding their digital infrastructure.

The core, compelling rationale for this focused international intervention is the urgent necessity to build deep-seated national resilience and ensure the continuous, unimpeded maintenance of critical governmental, economic, and social services, particularly during periods when traditional physical infrastructure, such as power grids, transportation networks, and physical communication lines, inevitably falters or is entirely compromised.

Digital infrastructure, including resilient fiber optic networks, decentralized cloud computing facilities, secure data storage centers, and mobile connectivity platforms, acts as a critical lifeline and a crucial element of redundancy. For nations in volatile environments, investing in robust digital systems is not merely an economic opportunity but a fundamental security imperative. This support ought to encompass:

1. **Hardening and Redundancy:** Funding for the creation of redundant network pathways, geographically dispersed data centers, and advanced cybersecurity measures to protect vital information systems from deliberate attack or systemic failure.
2. **Service Continuity:** Enabling the rapid deployment of essential digital services (e.g., telemedicine, remote education, digital financial services, and e-governance) to maintain societal function and economic activity even when citizens are confined or infrastructure is damaged.
3. **Early Warning and Response:** Developing digital platforms that facilitate real-time data collection, analysis, and dissemination, significantly enhancing the capacity of national authorities to forecast, prepare for, and respond effectively to emerging shocks.
4. **Inclusivity and Access:** Prioritizing last-mile connectivity and digital literacy programs to ensure that underserved populations, often the hardest hit by external shocks, are not excluded from accessing life-saving information and essential digital services.

In essence, strategic international investment in digital resilience serves as a potent form of preventive development aid, offering a high-leverage mechanism to mitigate the long-term human and economic costs associated with unforeseen global turbulence.

A clear and compelling example illustrating the critical need for resilient digital infrastructure is the lessons from **Mozambique**, a nation frequently confronting severe and escalating impacts of tropical cyclones and other extreme weather events. The country's unique geographical and topographical features contribute to its vulnerability,

resulting in geographically dispersed and often fragile infrastructure. This vulnerability and the consequent resilience of its government and its people necessitates a proactive and substantial effort toward an interpretation of a robust, **climate-resilient digital systems narrative**.

Such systems must be meticulously designed and engineered to not only endure but also maintain full operational capacity in the face of recurrent extreme weather events, including high winds, flooding, and power outages. The resilience of this digital backbone is paramount for several critical functions:

1. **Continuity of Communication:** Ensuring that emergency services, government agencies, and the general public can maintain contact, particularly when terrestrial lines of communication are destroyed. This includes resilient satellite and mesh networking solutions.
2. **Emergency Response Coordination:** Providing the platform for real-time data collection, risk assessment, resource allocation, and logistical coordination for search, rescue, and relief operations. Reliable digital systems are the nervous system of an effective disaster response.
3. **Access to Essential Government and Financial Services:** Guaranteeing that citizens, especially those displaced or severely impacted, can still access crucial government aid, digital identification, and financial services, such as mobile money transfers for immediate relief and recovery efforts.

Building this resilience requires a multi-faceted strategy encompassing reinforced physical infrastructure (e.g., elevated data centres, hardened fibre optic cables), redundancy in network architecture (e.g., diversified power sources, multiple backhaul routes), and the implementation of advanced disaster recovery and business continuity protocols. Investment in such digital resilience is not just an IT concern; it is a fundamental pillar of national security, economic stability, and humanitarian preparedness in the face of a changing climate.

Similarly, **some** nations battling with challenges in power generation and distribution that demonstrably cripple essential economic activity, stand to gain meaningful and transformative benefits from targeted investment in **solar-powered Information and Communication Technology (ICT)** infrastructure. This strategic shift towards solar power represents a vital pathway to energy security for the digital sector. By effectively decoupling digital networks—including mobile base stations, community telecentres, and critical data infrastructure—from the inherently unreliable and often-failing national grid, a decentralized solar power system provides a robust, continuous, and uninterrupted platform essential for the expansion and deepening of commerce, the uninterrupted delivery of high-quality education, and the reliable functioning of healthcare services (as highlighted in *WSIS Africa Perspectives, 2025*).

This necessity is particularly acute and profoundly critical for remote and deeply rural communities. In these areas, reliance on the national grid is often tenuous at best,

characterized by either complete lack of access or highly erratic and unstable power supply. Solar-powered ICT not only resolves the immediate power reliability challenge but also significantly lowers the long-term operational costs associated with generator fuels and grid connection fees. Furthermore, the deployment of resilient, solar-backed ICT infrastructure fosters digital inclusion, empowering remote populations to participate in the burgeoning digital economy, access distance learning opportunities, and utilize crucial telehealth services, thereby bridging the significant digital and developmental divide that currently exists between urban and rural Africa.

Innovative Financing Mechanisms for High-Debt State Systems

To ease the financial burden associated with these critical infrastructure investments, particularly for economies already straining under high sovereign debt, a paradigm shift toward innovative and sustainable financing mechanisms is necessary. The traditional reliance on outright grants or conventional loans often exacerbates debt vulnerabilities, making it imperative to explore alternative frameworks.

Consideration ought to be given to creating structured frameworks that directly link international aid, or more strategically, structured **debt relief**, to specific, verifiable **digital infrastructure investment targets**. This approach transforms debt—a liability—into a catalyst for development. Under such a mechanism, a portion of the sovereign debt is conditionally forgiven, or payments are redirected into a ring-fenced fund, contingent upon the debtor nation meeting pre-agreed milestones. These milestones must be measurable and transparently verifiable, such as:

- **Broadband Coverage Expansion:** Achieving a defined percentage increase in national high-speed internet penetration (e.g., reaching 75% coverage in rural areas by a specified date).
- **Fiber Optic Backbone Deployment:** Successful commissioning of a planned kilometer-count of national or regional fiber optic cable infrastructure.
- **Data Center and Cloud Infrastructure:** Establishment of Tier-III standard data centers to support local data sovereignty and digital services.
- **Digital Skills and Literacy Programs:** Investment in nationwide initiatives to enhance the digital capabilities of the workforce and general population, ensuring equitable access to the new infrastructure.

This "Debt-for-Digital-Development" model ensures that financial support directly translates into tangible, long-term productive assets that enhance economic competitiveness and social inclusion. Furthermore, this conditional approach provides a strong incentive for governments to prioritize digital transformation, enhances accountability in public spending, and offers creditors a clear path to seeing their forbearance yield developmental returns. International Financial Institutions (IFIs) and multilateral development banks ought to play a central role in structuring, auditing, and guaranteeing the integrity of these novel financing frameworks.

For some nations currently grappling with significant external debt obligations, the introduction of innovative financial instruments such as "Digital Transformation Debt Swaps" offers a paradigm-shifting mechanism. These specialized swaps could be structured to transform a substantial portion of external financial liabilities—which often hinder national development—into dedicated domestic capital. This newly freed capital would be exclusively ring-fenced for high-impact, strategic projects focused on building digital resilience and expanding access to secure, high-speed digital networks.

This innovative approach ensures a direct and measurable translation of financial concessions into tangible, productive assets. By specifically targeting digital infrastructure, the funds would immediately be channeled into creating secure, expansive digital networks, thereby boosting long-term national economic productivity, fostering a robust e-governance framework, and enhancing overall socio-economic stability (AIFAT, 2025). Furthermore, by mandating that debt relief funds be dedicated solely to digital resilience and expansion, the international community can ensure both a commitment to fiscal responsibility from the recipient nation and a guaranteed investment in transformative, future-proof development, moving beyond temporary budgetary relief to genuine structural change. This model addresses the core development challenge by linking financial restructuring directly to the enabling infrastructure of the modern global economy and as such deserves special attention from the Zero Draft negotiators..

---

7. Pillar II: Digital Sovereignty, Data Governance, and Security

Intervention: Acknowledging that the digital future must be built on trust and self-determination, African nations are keen to assert greater **digital sovereignty** over their national data assets (African Perspective Note, 2025).

Rationale: African Digital Sovereignty – A Strategic Imperative

Acknowledging the fundamental understanding that the digital future, particularly for emerging economies and developing nations, must be built upon the foundational pillars of trust, robust security, and the essential right of national self-determination, African nations are increasingly prioritizing the assertion of greater **digital sovereignty** over their national data assets. This strategic push is not merely a technical or regulatory preference; it is a critical geopolitical and economic imperative rooted in the recognition of data as a critical national resource in the 21st century—often termed the "new oil." The analogy underscores the conviction that the nation or entity that controls the data flow, processing, and intellectual property derived from that data holds significant leverage in the global economic and political arena. This growing emphasis on sovereignty reflects a desire to move beyond a purely consumption-based model of technology adoption toward one where African nations are active participants and governors of their own digital space.

The drive for digital sovereignty, therefore, encapsulates the strategic objective to exert full national control over the entire data lifecycle: the **creation, flow, storage, utilization, and governance** of data generated by citizens, businesses, and government entities within their territorial borders. This comprehensive control is sought to achieve several critical, interlinked goals. Economically, it aims to foster local digital industries, ensure equitable value capture from national data, and prevent capital flight associated with the reliance on foreign cloud and data services. Geopolitically, it is a mechanism for protecting national security interests, safeguarding against foreign surveillance, and ensuring legislative and judicial jurisdiction applies to all data processing within the nation. Culturally and socially, digital sovereignty seeks to protect citizen privacy, uphold democratic principles in the digital sphere, and ensure that data-driven policy decisions align with national values and priorities, fundamentally asserting the right of self-determination in the digital age.

Key Drivers for Asserting Digital Sovereignty:

1. **Economic Value and Resource Control:** Data is the primary input for artificial intelligence, machine learning, and the entire digital economy. By controlling data, African nations seek to ensure that the economic value derived from this resource accrues domestically, fostering local innovation, data-driven industries, and high-value job creation, rather than being extracted by foreign entities under current regimes.

2. **National Security and Trust:** Reliance on foreign infrastructure and legal frameworks for data storage and processing introduces significant national security vulnerabilities. Asserting sovereignty is crucial for protecting sensitive government, military, and citizen data from unauthorized access, espionage, and foreign surveillance, thereby building indispensable public trust in digital services.
3. **Regulatory Autonomy and Legal Jurisdiction:** Digital sovereignty allows African states to establish domestic regulatory frameworks that align with their own social values, cultural norms, and specific developmental objectives, independent of the dominant legal and regulatory regimes of major global technology powers. This includes the ability to enforce national data privacy laws and ensure local law enforcement and judicial access to relevant data under domestic jurisdiction.
4. **Mitigating External Dependencies:** By promoting local data centres, cloud infrastructure development, and indigenous digital service providers, African countries aim to reduce an over-reliance on a few dominant foreign technology providers. This mitigation strategy enhances resilience against potential service disruptions, sanctions, or politically motivated technological withdrawal.

The assertion of digital sovereignty is a holistic, forward-looking strategy designed to safeguard the continent's long-term interests, ensuring that the digital transformation serves as an engine for inclusive, secure, and self-determined development. This collective aspiration, as articulated in strategic documents like the African Perspective Note (2025), reflects a growing awareness that ceding control of national data to external entities—often large multinational technology corporations—poses significant risks to economic development, security, and political autonomy. Digital sovereignty is therefore being pursued through several interconnected policy and technological fronts:

1. **Data Localization and Governance:** African states are exploring and enacting new legislation that mandates the storage and processing of certain categories of sensitive national and citizen data within the country's physical borders. This is complemented by strengthening domestic data protection laws, establishing independent regulatory bodies, and harmonizing regional frameworks to facilitate secure cross-border data flows within the continent (e.g., under the auspices of the African Union).
2. **Infrastructure and Connectivity Control:** The push for sovereignty extends to controlling the underlying digital infrastructure. This involves investing in national and regional fiber optic networks, establishing robust and secure national cloud computing facilities, and ensuring greater domestic ownership and management of critical internet exchange points (IXPs).
3. **Skills and Innovation:** True digital sovereignty requires a skilled workforce capable of developing and managing independent digital solutions. Nations are prioritizing massive investments in digital literacy, STEM education, and fostering a vibrant local tech and start-up ecosystem to reduce reliance on proprietary foreign technologies and platforms.

The Imperative of Digital Sovereignty in the African Context

Digital sovereignty, at its core, represents a nation's fundamental capacity to govern and regulate its entire digital space, encompassing infrastructure, data flows, and technological ecosystems within its defined geopolitical borders. This control is exercised to ensure that the digital environment aligns seamlessly with national laws, prevailing social values, and long-term strategic economic and security interests.

For African nations, this assertion of digital sovereignty is swiftly transitioning from a theoretical concept into a paramount, non-negotiable policy agenda. The urgency is driven by a confluence of critical factors. Historically, many African economies have been net consumers of technology, leading to significant reliance on foreign-owned digital platforms and infrastructure for critical services, from financial transactions to public health administration. This dependency creates vulnerabilities, including risks of data exploitation, surveillance, and economic disruption stemming from external policy shifts or corporate decisions.

The push for digital sovereignty on the continent is multifaceted, centering on several key pillars:

1. **Data Governance and Localization:** This involves establishing robust national regulatory frameworks for how citizens' and government data is collected, stored, processed, and transferred. African nations are increasingly advocating for data localization requirements, ensuring that strategic national data resides within their physical borders and is subject to national jurisdiction. This is a vital step in protecting personal privacy, maintaining state security, and unlocking the economic value of data for the local economy.
2. **Infrastructure Ownership and Resilience:** True sovereignty requires control over the physical and logical underpinnings of the digital world—the fiber optic cables, data centers, mobile network infrastructure, and satellite connectivity. Investment in nationally owned and operated infrastructure is seen as crucial for bolstering network resilience against external attacks and ensuring uninterrupted access to critical services, thereby reducing dependence on foreign entities that may prioritize external interests.
3. **Cybersecurity and National Security:** The digital domain has become a new frontier for geopolitical competition. Digital sovereignty is indispensable for establishing autonomous, effective national cybersecurity capabilities to defend against state-sponsored attacks, cybercrime, and technological espionage, which often target critical national infrastructure and democratic processes.
4. **Policy Space and Regulatory Autonomy:** Asserting digital sovereignty ensures that African governments retain the necessary policy space to craft regulations that foster local innovation, address unique national development challenges, and prevent potential anti-competitive behavior by global tech giants. It is about balancing the benefits of global connectivity with the imperative to foster a domestic digital economy that serves the national development agenda.
5. **Digital Public Infrastructure (DPI), Innovation, and Entrepreneurship:**

> Proposing support for an **Africa-centric, interoperable DPI model** to accelerate economic integration, facilitate the African Continental Free Trade Area (AfCFTA), and directly unlock the potential of digital **innovation and youth/women-led entrepreneurship** (Carnegie Endowment, 2025).

In essence, digital sovereignty is viewed not merely as a defensive measure but as a developmental prerequisite, allowing African nations to secure their digital future, promote economic inclusion, and ensure that the digital revolution serves the continent's distinct path to sustainable development.

The core strategic imperative is to ensure that the rapid advancements and immense, transformative opportunities presented by the burgeoning digital economy are effectively and equitably harnessed. This is essential to drive robust domestic prosperity, foster genuinely inclusive economic growth, and accelerate comprehensive socio-economic development across all strata of society. Achieving this goal mandates a proactive and deliberate stance in shaping precisely how digital technologies are adopted, meticulously deployed, and competently managed within the national context. The objective is to maximize their developmental impact across critical national sectors, including finance (e.g., FinTech, digital payments), education (e.g., e-learning, digital literacy), healthcare (e.g., telemedicine, health data systems), and public governance (e.g., e-government, public service delivery). This proactive approach requires not merely adoption, but strategic foresight and regulatory frameworks designed to channel digital innovation towards public good.

Crucially, however, the escalating drive for **digital sovereignty** is fundamentally and equally motivated by the paramount imperatives of national security, the preservation of constitutional democracy, and the maintenance of autonomous self-rule in the digital sphere. **Connecting autonomy, agency and franchise under a thematic formulation of authority = responsibility = accountability is a non-negotiable redline.**

A position of reliance, particularly an over-reliance, on digital infrastructure, dominant platforms, and core data processing centres that are entirely controlled, operated, or architecturally designed by foreign entities introduces a spectrum of systemic and significant national vulnerabilities. These risks are multifaceted and profound. They include, but are not limited to, the persistent potential for unwarranted and unmonitored surveillance of citizens and government operations, the systemic exploitation of national and personal data by external state or non-state actors for economic or political advantage, and the inherent susceptibility of critical national infrastructure (e.g., power grids, financial systems, communication networks) to suspectedly foreign-initiated disruptions, sabotage, or malicious cyber-attacks. Therefore, digital sovereignty is conceived as a necessary defensive shield to protect the nation's integrity and autonomy in an increasingly digitized and interconnected world. It signifies the nation's capacity to govern its own digital space, enforce its own laws, and protect its citizens' rights without undue external interference.By asserting control over their digital destiny, African

nations aim to mitigate these risks. This often translates into policy actions such as advocating for local data storage and processing (data localization), investing in domestic digital infrastructure (such as national fibre-optic networks and data centres), developing local technical expertise, and crafting comprehensive legal and regulatory frameworks that govern cross-border data flows and the operations of global tech giants within their jurisdictions.

In essence, digital sovereignty is a multifaceted strategic policy for Africa: it is a tool for economic empowerment, a shield for national security, and a guarantor of political autonomy, ensuring that the continent's digital future is determined by its own citizens and institutions.

7.1. Proposal: Supporting Sovereign Data Governance (Para 94, 96)

Intervention: The continent encourages strengthening language in **Paragraphs 94 and 96** to explicitly recognize and support the sovereign right of nations to govern data that originates within their territories, including assistance for developing local, secure data infrastructure.

Rationale: The unified position of the diverse nations and regional blocs spanning the African continent is a forceful advocacy for a significant and crucial strengthening of the operative language contained within the draft international agreement. This proposed amendment is specifically and strategically directed at two key provisions: Paragraphs 94 and 96.

This comprehensive revision is fundamentally designed to achieve two primary and interconnected strategic objectives, which are considered non-negotiable for the continent's future in the digital era:

1. **Ensuring Digital Sovereignty:** The amendments seek to establish a clear and robust framework that guarantees the absolute right of African nations to govern their own digital space, infrastructure, and data. This includes the autonomy to formulate and enforce national policies concerning data localization, cross-border data flows, and the regulation of global digital platforms, thereby protecting national interests from undue external influence or unilateral technological control.
2. **Promoting Equitable Development and Technological Transfer:** The strengthened language aims to mandate concrete mechanisms for fostering equitable access to digital technologies, capacity building, and essential knowledge transfer. This objective is centered on closing the persistent digital divide, ensuring that the benefits of the global information society translate into tangible socio-economic growth, and empowering African states to become creators, not just consumers, of digital innovation, ultimately driving sustainable and inclusive development across the continent.

The African Group's stance underscores the belief that the current wording of

Paragraphs 94 and 96 lacks the necessary commitment and clarity to effectively safeguard these vital interests, necessitating a bolder, more prescriptive text within the final resolution for several reasons.

Firstly, the most significant proposed change is the explicit recognition and unwavering support for the sovereign right of individual nations to govern and regulate all data that originates within their geographical territories. This includes the right to determine where, how, and by whom this data is stored, processed, and accessed. This stance is a direct response to the challenges posed by cross-border data flows and the need to protect national interests, privacy, security, and economic value derived from their own digital resources.

Secondly, and in direct support of the principle of data sovereignty, the continent is requesting concrete commitments and assistance for developing local, secure data infrastructure. This includes, but is not limited to, the establishment of national and regional data centers, secure cloud computing facilities, and robust fiber-optic networks. Such infrastructure development is seen as vital for several reasons:

- Security: To minimize reliance on foreign-controlled infrastructure, thereby mitigating external risks of surveillance, data breaches, and unauthorized access.
- Economic Development: To foster a local digital economy, create skilled jobs, and ensure that the economic benefits of data localization remain within the originating country.
- Digital Inclusion: To bridge the digital divide by making essential digital services more accessible, reliable, and affordable for all citizens.
- Regulatory Compliance: To empower national regulatory bodies to enforce their data protection and privacy laws effectively.

The ultimate goal of the current concerted effort to strengthen Paragraphs 94 and 96 within the proposed framework is to fundamentally reshape the architecture of global digital governance. This initiative is driven by a multifaceted vision centered on three core, interdependent principles.

Firstly, a primary objective is the establishment of a **global digital governance framework that respects national borders and sovereignty in the digital realm while respecting the economic needs of individuals and enterprises**. This involves moving away from an unrestricted, borderless internet paradigm toward one where national jurisdictions have the clear authority to regulate digital activities, data flows, and internet infrastructure within their territories, consistent with international laws and evolving trends in the e-commerce and digital trade domains. This principle seeks to harmonize the physical concept of sovereignty with the reality of digital operations, ensuring that state institutions can enforce their laws, protect their citizens' digital rights, and manage national security concerns without undue foreign interference or extraterritorial application of other nations' laws.

Secondly, the push aims to ensure **fair, equitable, and substantial technological capacity building for all developing nations**. This goes beyond merely providing access to technology; it encompasses a systematic transfer of knowledge, skills, and intellectual property necessary for these countries to independently build, maintain, and innovate their own digital infrastructure and services. This capacity building must focus on developing a sovereign digital ecosystem, including expertise in data governance, cybersecurity, cloud computing, and advanced connectivity. The ultimate intention is to close the global digital divide not just in terms of access, but in terms of autonomous technological competence and policy-making ability. **Spatially, this would also ensure a fractal augmentation of autogenic Artificial Intelligence as the tecnocene draws ever nearer.**

Thirdly, the expansion is focused on promoting a **more balanced, decentralized, and inclusive global data ecosystem**. This seeks to challenge the current model characterized by the excessive concentration of data, processing power, and governance control in the hands of a few dominant global technology corporations and nations. The revised framework would promote principles of data localization, data sovereignty, and fair benefit-sharing from the exploitation of global data resources. The goal is to democratize the data economy, empowering developing nations to realize the economic and developmental value of the data generated within their borders, thereby fostering a more equitable distribution of digital wealth and power globally.

By strengthening these two paragraphs, the proponent states seek to institutionalize these principles, transitioning from mere aspiration to enforceable norms and mechanisms within the international system of digital cooperation.

- **Use Case and Rationale: Proactive Regulatory Frameworks for Data Sovereignty and Protection in Africa**

The African continent is demonstrating a clear and accelerating trend towards establishing **robust data governance frameworks**. This movement is driven by a critical, dual imperative: to foster the essential free flow of data that powers the burgeoning digital economy, while simultaneously safeguarding national security interests and protecting the fundamental digital rights and privacy of its citizens. This balancing act is crucial for ensuring that the promise of digital transformation is realized responsibly and equitably across the continent.

At the heart of this regulatory shift is the principle of **data sovereignty**. This concept posits that data generated within a country's geographical borders ought to be subject to and managed primarily under domestic regulatory and legal control. This is not merely a technical or administrative concern, but a matter of national policy, digital autonomy, and a foundational element for fostering trust in the digital ecosystem. For African nations, asserting data sovereignty is a means of reclaiming control over valuable digital assets, ensuring that economic benefits are retained locally, and establishing

jurisdictional clarity in an increasingly cross-border digital landscape.

The contemporary imperative for robust and cohesive data governance is catalysing a wave of significant legislative and strategic initiatives across the continent. This drive is rooted in the recognition that a predictable and secure digital environment is fundamental to achieving broader economic and social development goals.

In the legislative sphere, an increasing number of African nations are either developing entirely new, state-of-the-art data protection and privacy laws or undertaking comprehensive updates of outdated existing frameworks. While these national laws often draw inspiration from established global benchmarks, such as the European Union's pioneering General Data Protection Regulation (GDPR), they are meticulously tailored to reflect specific local socio-economic, cultural, and legal contexts. Key provisions commonly embedded in this new generation of legislation include:

- **Mandatory Requirements for Explicit Consent:** Ensuring that individuals have clear control over the processing of their personal data, often through affirmative and unambiguous consent mechanisms.
- **Data Localization Provisions (Context-Specific):** While not universally applied, some jurisdictions are incorporating measures that require certain categories of sensitive or strategic data to be stored and/or processed within national borders to enhance sovereignty and security.
- **Prompt Breach Notification:** Establishing stringent obligations for data controllers and processors to report security breaches to supervisory authorities and affected individuals in a timely manner.
- **Establishment of Independent Supervisory Authorities (ISAs):** Creating dedicated, autonomous bodies tasked with enforcing data protection laws, investigating complaints, issuing sanctions, and promoting public awareness. These authorities are crucial for effective oversight and building public trust.
- **Enhanced Data Subject Rights:** Granting citizens rights such as the right to access, rectify, erase (right to be forgotten), and port their personal data, aligning with international best practices.

Beyond national efforts, continental and regional bodies are playing a vital, coordinating role. Their primary objective is the *harmonization* of these diverse national legal frameworks. This harmonization is essential to facilitate seamless, secure, and compliant **intra-African data transfers**. The ability to move data efficiently across borders, while maintaining a high standard of protection, is not merely a technical requirement but a strategic enabler for pan-African economic integration. This is particularly paramount for ensuring the operational success and full potential realization of major initiatives such as the **African Continental Free Trade Area (AfCFTA)**, which fundamentally relies on the free flow of digital services and data.

> The overarching, collective goal of this multifaceted push for comprehensive data governance is to forge a **predictable and trustworthy digital ecosystem**.

This environment is specifically designed to:

- **Encourage Domestic Innovation:** By providing clarity and certainty to local entrepreneurs and tech startups, fostering a fertile ground for the development of African-led digital solutions.
- **Attract Foreign Direct Investment (FDI):** By offering international businesses a clear, standardised, and legally sound framework for operating, thus mitigating regulatory risk and increasing investor confidence.

Ultimately, this comprehensive data governance strategy is underpinned by a dual commitment: to ensure that the fundamental digital rights of African citizens are fully protected, while simultaneously safeguarding the strategic national and collective interests of African states in the rapidly evolving global digital economy.

The implementation of data sovereignty is manifesting through several key legislative and policy developments:

1. **Comprehensive Data Protection Laws:** A growing number of African nations are enacting and enforcing comprehensive data protection and privacy laws, often drawing inspiration from global standards like the European Union's General Data Protection Regulation (GDPR), but tailored to the unique socio-economic context of the continent. Some African countries have been at the forefront of this legal wave but many of their colleagues are not even there yet. These laws define citizens' rights regarding their personal data, impose strict obligations on data controllers and processors (both domestic and foreign), and establish independent regulatory authorities to ensure compliance.
2. **Cross-Border Data Transfer Regulations:** A critical component of data governance is controlling how data is transferred out of the country. African frameworks are increasingly specifying conditions, mechanisms (like standard contractual clauses or certification schemes), and legal grounds for the secure and compliant movement of data across borders. This is a direct measure to ensure that data, once it leaves the country, does not escape domestic oversight and is afforded an equivalent level of protection in the destination jurisdiction.
3. **Data Localisation Requirements:** In certain strategic sectors, such as financial services, telecommunications, and government records, there is a distinct push toward mandatory data localisation. This requires that specific categories of data be stored and processed on servers physically located within the national territory. Proponents argue this enhances security, ensures accessibility for law enforcement and regulatory audits, and stimulates the development of local digital infrastructure (e.g., data centers). However, these requirements must be carefully balanced to avoid stifling foreign direct investment or increasing operational costs for multinational businesses.
4. **Harmonisation Efforts:** Recognizing the need for a unified digital market and to prevent fragmentation, regional bodies such as the African Union (AU) and regional economic communities (RECs) like ECOWAS and SADC are actively

working on harmonising data governance policies. The AU Convention on Cybersecurity and Personal Data Protection (Malabo Convention) serves as a foundational continental instrument, encouraging member states to adopt common principles and facilitate seamless, yet secure, data flows across the continent.

The proactive steps being taken are foundational to building a trusted digital environment in Africa. By asserting control over their data, nations are positioning themselves to fully leverage the economic potential of the data revolution while upholding the core principles of security, accountability, and the protection of citizens' fundamental human rights in the digital age.

A leading and internationally-recognized example of this progressive regulatory action in the global South is **Kenya's Data Protection Act (2019)**. This comprehensive and landmark legislation, which became operational in late 2019, represents a significant commitment by the Kenyan government to safeguard its citizens' privacy rights in the digital age, drawing inspiration from global standards like the European Union's General Data Protection Regulation (GDPR) while adapting them to the specific context of the African economy.

The Act introduces a pivotal requirement concerning data localization and cross-border data transfers. Specifically, it mandates that the personal data collected from Kenyan citizens—data subjects—must be processed either within the Republic of Kenya or, crucially, it can only be transferred to a foreign jurisdiction *if* that jurisdiction can adequately demonstrate an **equivalent level of data protection** to the standards set out in the Kenyan Act. The law requires data controllers and processors to conduct due diligence and often necessitates specific contractual clauses or certification mechanisms to validate this equivalence.

This stringent mechanism serves as a crucial and highly-cited use case for effectively balancing two critical, and often competing, imperatives: the needs of a modern, digitally-connected, and internationally-integrated economy on one hand, with the necessity for robust national regulatory oversight and control over its citizens' sensitive data on the other. By establishing a high-bar equivalence test, the Act ensures that Kenya remains open for digital business and foreign investment while preventing the country from becoming a data haven or a 'regulatory gap' through which international entities might exploit weaker data protection standards (KICTANet, 2025; Startup Graveyard Africa, 2025).

The Act's provisions are meticulously designed to achieve several strategic objectives: firstly, to prevent the exploitation of perceived data regulatory gaps or inconsistencies by large international corporations and tech giants; secondly, to foster deeper trust and confidence in Kenya's nascent but rapidly expanding digital ecosystem among its citizens; and thirdly, to position Kenya as a regional leader in data governance and digital rights, thereby potentially influencing data protection standards across the wider

East African community and the continent. The establishment of an independent Office of the Data Protection Commissioner (ODPC) further institutionalizes this commitment, providing the necessary enforcement and regulatory guidance to implement the Act's comprehensive framework.

Similarly, **South Africa's Protection of Personal Information Act (POPIA)** offers another comprehensive and rigorous legal blueprint for data governance, serving as a landmark piece of legislation on the African continent. POPIA establishes a detailed set of clear rules, conditions, and standards for the lawful processing of personal information, applicable to a wide spectrum of responsible parties, encompassing both public and private sector bodies operating within South Africa. This framework is anchored by eight foundational conditions for lawful processing, which include accountability, processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards, and data subject participation.

A critical aspect of POPIA is the establishment of the Information Regulator, an independent body tasked with overseeing and enforcing compliance with the Act. The Regulator plays a vital role in investigating complaints, issuing enforcement notices, and promoting awareness of data protection rights. The scope of POPIA is extensive, covering everything from the collection and storage to the dissemination and destruction of personal data, thereby providing a holistic shield for the data subject's privacy rights.

Critically, the Act is backed by a robust enforcement mechanism that imposes substantial penalties for non-compliance. These sanctions can include significant administrative fines, reaching up to ZAR 10 million (approximately $550,000 USD, though subject to exchange rate fluctuation), and potential imprisonment for severe and intentional violations. The imposition of such serious consequences is a direct manifestation of a serious and unambiguous commitment by the South African government to uphold and enforce data rights. This not only emphasizes the gravity of data protection but also provides a strong, legislative-backed deterrent against the misuse, neglect, or unauthorized disclosure of personal data (Pollicy, 2024). Furthermore, POPIA grants data subjects the right to institute civil proceedings against responsible parties for damages, adding an additional layer of accountability. The Act, therefore, represents a progressive and comprehensive model for securing digital rights in the modern era.

This progressive regulatory approach, actively championed and implemented by influential nations such as Kenya and South Africa, provides a crucial and supportive template for the rest of the African continent. This model is particularly vital for some of the other countries in Africa and beyond which possess immense and strategically important natural resources and critical national infrastructure. These nations face a particular and pressing imperative to secure comprehensive digital control, or data sovereignty, over the vast datasets generated by and related to the

management of these assets. For many other resource-rich African states, the principle of data sovereignty is not merely a technical or legalistic concern; it is intrinsically and fundamentally linked to their long-term economic sovereignty and their paramount national security interests.

The establishment of robust, pan-African or Africa-centric data protection laws and governance frameworks is therefore an essential step. By supporting and fostering these indigenous frameworks, the international community and continental organizations can enable African nations to gain the necessary control, oversight, and legal jurisdiction required to manage these sensitive and economically valuable datasets effectively. This capacity building is critical for ensuring that the benefits of the digital economy are harnessed for national development.

The continued and demonstrable success of these pioneering regulatory frameworks, like those in Kenya and South Africa, is absolutely crucial. Their success serves not only as a proof of concept but also as a catalyst for widespread adoption, which is necessary for fostering a truly secure, equitable, and autonomous digital future across the African continent. This continental effort is fundamental to ensuring that Africa controls its digital destiny and leverages its data as a strategic asset (WSIS Africa Perspectives, 2025).

7.2. Proposal: Ethical AI and Capacity Building (Para 15, 97)

Intervention: African nations may consider collaborating on a continental framework for the ethical development and deployment of Artificial Intelligence, supported by the principles in **Paragraphs 15 and 97**.

Rationale: African nations have a unique opportunity to demonstrate continental leadership by forging a unified, ethical framework for the development and deployment of Artificial Intelligence (AI). This collaborative endeavor ought to aim to harness the transformative power of AI for sustainable development, while simultaneously mitigating associated risks and ensuring alignment with African values and priorities.

The foundation for this continental framework must be robust, drawing directly upon established principles. Specifically, it ought to be supported by the ethical considerations and regulatory guidelines outlined in Paragraphs 15 and 97 of the relevant foundational documents.

Key Elements of the Proposed Continental AI Framework:

1. **Ethical Governance and Oversight:**
    - Establish a Pan-African AI Ethics Committee to guide policy, monitor

implementation, and provide expert advice to member states.
    - Develop continent-wide standards for AI trustworthiness, focusing on **transparency, accountability,** and **explainability (TAE)**.
    - Ensure that AI systems deployed across the continent are designed to prevent bias and discrimination, particularly those that could exacerbate existing socio-economic inequalities.
2. **Data Sovereignty and Privacy:**
    - Institute strong cross-border data governance protocols that protect the data of African citizens and respect national data sovereignty laws.
    - Promote the ethical use of large datasets for public good initiatives, such as healthcare, agriculture, and climate adaptation, while upholding individual consent and privacy rights.
3. **Capacity Building and Inclusion:**
    - Invest in digital infrastructure and AI education across all levels to ensure equitable access to AI technology and skills.
    - Prioritize inclusive design, ensuring that AI solutions are accessible and relevant to diverse populations, including those in rural and underserved communities.
    - Foster regional Centers of Excellence in AI research and development to drive African-led innovation.
4. **Security and Risk Mitigation:**
    - Address the security implications of AI, including the prevention of misuse for surveillance, misinformation, and cyber warfare.
    - Develop harmonized safety standards for high-risk AI applications before they are deployed in critical sectors.

By collaborating on this comprehensive continental framework, African nations can position themselves as leaders in the global discussion on ethical AI, ensuring that technology serves the continent's long-term goals of prosperity and unity.

Use Case and Rationale for Proactive AI Governance and Cyber Capacity Building in Africa

The African continent is currently undergoing a profound and accelerating digital transformation, marked by the rapid and pervasive adoption of Artificial Intelligence (AI) technologies across virtually every sector. This technological revolution is not just theoretical; it is actively reshaping critical areas. For instance, in financial services, AI is now indispensable, driving sophisticated credit scoring models that enhance financial inclusion and powering advanced fraud detection systems that secure transactions. Similarly, in public administration, numerous nations are exploring and implementing AI solutions to improve service delivery and efficiency. A prime example of this proactive engagement is **Egypt's** concerted and high-level push to establish a robust and comprehensive national framework for AI ethics, governance, and responsible deployment specifically within its public services (as documented in WSIS Africa

Perspectives, 2025). This initiative underscores a growing continental recognition of AI's dual nature.

This rapid integration of AI into the socio-economic fabric of African nations necessitates an equally proactive, forward-thinking, and immediate approach to governance and regulation. The speed and scale of AI adoption mean that the window for establishing appropriate guardrails is closing quickly. The absence of well-defined and enforceable regulatory frameworks poses significant and multi-faceted risks. These include the exacerbation of societal inequalities through algorithmic bias, where systems inadvertently discriminate against certain populations; the critical threat of data privacy infringements due to the vast amounts of personal data AI systems require; and the ever-present potential for the malicious use or misuse of powerful AI technologies, from surveillance to disinformation campaigns. Consequently, establishing clear, context-specific, and internationally harmonized AI governance is not merely an option but an imperative for ensuring that Africa's digital transformation is equitable, secure, and beneficial to all its citizens.

A cornerstone of this proactive governance strategy must be the significant enhancement of **cyber capacity building** (Para 65) across the African continent. This imperative is particularly acute for nations currently grappling with elevated and increasingly sophisticated digital threats. These threats range from widespread financial fraud schemes and highly disruptive ransomware attacks to advanced persistent threats (APTs) targeting critical national infrastructure and key government services. Consequently, some of these state systems urgently require a substantial and sustained uplift in its national cyber resilience framework.

Building robust and self-sustaining local expertise is not merely desirable but essential. This capacity building must focus on cultivating a highly-skilled workforce, including certified cybersecurity professionals, expert data scientists proficient in ethical AI/ML practices, and regulatory experts well-versed in the dynamic landscape of digital law.

This local capacity serves a dual, critical function. First, it is indispensable for the effective monitoring, enforcement, and ethical auditing of standards for emerging and disruptive technologies, most notably Artificial Intelligence (AI). Local experts are best positioned to contextualize global best practices within national legal and socio-economic realities. Second, this localized skill set is paramount for the operational resilience needed to effectively mitigate, thoroughly investigate, and successfully prosecute the persistent and evolving spectrum of cyber threats (Startup Graveyard Africa, 2025).

Therefore, investing in comprehensive cyber capacity building represents a dual imperative for African nations: it acts as a powerful shield, protecting burgeoning digital economies from significant financial and reputational harm, while simultaneously empowering nations to competently regulate, ethically harness, and maximize the transformative potential of technologies like AI for sustainable development and

national security. This investment must be viewed not as a cost, but as a foundational strategic asset for the continent's digital future.

---

8. Pillar III: Protecting Human Rights and Digital Freedoms

Intervention: The economic and social costs of disproportionate restrictions on digital access demand a clearer, rights-based commitment within the Zero Draft.

Rationale: The existing formulation of the Zero Draft requires a stronger, explicit commitment to a rights-based approach regarding digital access, moving beyond passive acknowledgment to active protection. The imposition of disproportionate restrictions on access to digital technologies, the internet, and online information carries profound and multifaceted economic and social costs that cannot be ignored.

Economically, such restrictions, including blanket digital restrictions, content blocking, or disproportionate censorship, cripple digital economies, disrupt e-commerce, halt financial transactions, and sever vital links for remote work and education. They erode investor confidence in the stability of the digital ecosystem and disproportionately affect small and medium-sized enterprises (SMEs) that rely heavily on online platforms.

Socially, these restrictions are profoundly damaging. They suppress freedom of expression and assembly, impede access to essential information—especially during crises or elections—and undermine civic participation. Furthermore, they disproportionately affect marginalized groups, women, and individuals in remote areas, exacerbating existing digital divides and hindering progress on key sustainable development goals (SDGs).

Therefore, the **Zero Draft must clearly articulate a rights-based commitment** that recognizes unimpeded, non-discriminatory digital access as fundamental to human dignity and empowerment. This commitment ought to mandate:

1. **Strict Necessity and Proportionality:** Any measure limiting digital access must be demonstrably necessary, strictly proportionate to a legitimate public interest aim, and subject to independent judicial oversight.
2. **Transparency and Accountability:** All decisions concerning restrictions must be made public, with clear justification, and be subject to effective remedy and mechanisms for accountability.
3. **Non-discrimination:** Subject to the cause of law enforcement and public order, restrictions must not target specific groups, opinions, or political discourse arbitrarily.

By integrating this clear, rights-based standard, the Zero Draft will more effectively safeguard fundamental rights and ensure that digital technologies serve as engines of inclusive growth and social progress, rather than tools for control and exclusion.

8.1. Proposal: Regulating digital restrictions (Para 88, 99)

Intervention: Consideration may be given to suggest that **Paragraph 88** be strengthened to establish clear international best practices and safeguards against disproportionate or unreasonable **digital restrictions and censorship**, upholding human rights (Para 9, 10).

Rationale: Consideration may be given to suggest a significant strengthening of Paragraph 88 within the framework to explicitly establish robust international best practices and safeguards. This crucial amendment aims to prevent and challenge disproportionate digital restrictions without necessary reasoning which constrain access to communication. Such practices, enacted without due process or clear legal justification, violate the principles enshrined in existing international agreements, specifically referencing the importance of upholding access to information as fundamental rights articulated in Paragraphs 9 and 10 of the foundational document.

The proposed elaboration seeks to ensure that:

1. **Clear Definitions and Scrutiny:** International standards must clearly define what constitutes a legitimate restriction on internet access, ensuring that any such action is strictly necessary, proportionate, and non-discriminatory, subject to independent judicial or regulatory oversight.
2. **Protection of Rights:** The text ought to adequately state that mass surveillance, content blocking, and forced shutdowns, without legal and procedural robustness constrains the rights to freedom of expression, freedom of assembly, and access to information, which are essential for democratic participation and socioeconomic development. Faith and trust in the state system is endemic to the success of any state system. The African best practices could show a way to the world.
3. **Accountability and Remedy:** A mechanism ought to be established to ensure accountability for actors that impose disproportionate internet restrictions, including provisions for effective remedies and reparations for affected individuals and businesses.
4. **Technological Neutrality and Resilience:** The framework ought to promote principles of technological neutrality and resilience, encouraging the use of technologies and policies that can circumvent or resist unwarranted state-sponsored disruptions to connectivity.

- **Use Case and Rationale: digital restrictions in Africa and beyond: A Growing Crisis of Economic and Civil Liberties**

The escalating frequency of digital restrictions across the globe, and not only limited to Africa, presents a critical and multifaceted challenge, profoundly impacting both the trajectory of economic development and the guarantee of fundamental civil liberties. The data reveals a deeply troubling trend: the rate of these intentional, state-sponsored disruptions has dramatically increased, effectively doubling since 2016. This surge transforms what might be seen as an isolated incident into a concerning, systematic tool of governance.

The use of digital restrictions, such as digital restrictions, often arises in complex operating environments, particularly during periods of intense political or civil sensitivity, where states may prioritize maintaining national security or public order. However, there is a global imperative to recognize that the frequent and broad application of such measures carries demonstrable, serious, and often unintended consequences. These actions can disproportionately impact economic stability, hinder humanitarian efforts, and constrain fundamental digital freedoms, necessitating the urgent establishment of clear international best practices and human-rights-based safeguards to ensure digital governance is consistently resilient and rights-respecting.

Building on successful models from African nations like Rwanda's digital resilience strategies during crises, the framework can promote proportional responses that protect both security and access.

The consequences of this tactic are far-reaching. Economically, these blackouts cripple digital trade, disrupt essential e-services, halt financial transactions, and sever access to crucial global markets, leading to significant, quantifiable losses in GDP. For a continent heavily invested in leapfrogging traditional development stages through digital transformation, such disruptions undermine years of progress and erode investor confidence.

From a policy and rights perspective, the practice of restricting digital access, such as through digital restrictions, introduces significant complexity to the realization of a people-centered Information Society. While recognizing the legitimate concerns regarding public security and order, it is imperative that all stakeholders acknowledge the profound and systemic consequences of such actions. Specifically, the interruption of communication channels can have a measurable chilling effect on fundamental digital rights, including the rights to freedom of expression and peaceful assembly. Furthermore, it risks impeding the timely dissemination of vital, life-saving information during emergencies and undermines the capacity for transparent governance and inclusive civic dialogue. The international community must therefore prioritize developing robust, rights-based, and proportional frameworks to address security challenges without compromising the core principles of digital openness, transparency, and human development.

The Economic Impact of Non-Performance

Beyond the political and civil costs, the economic repercussions of digital restrictions are immediate and substantial, particularly in countries with low connectivity that rely heavily on mobile digital infrastructure. The financial damage is staggering, with estimates suggesting that even a temporary, one-day disruption can cost a typical low-connectivity nation as much as **$3 million per day**.

These costs accrue rapidly because the shutdowns cripple several vital sectors of the modern African economy:

- **Mobile Money and Banking:** Africa is a global leader in mobile money transactions. A shutdown halts person-to-person transfers, salary payments, and essential financial services, immediately affecting daily commerce for millions.
- **E-commerce:** Online retail and marketplace platforms become inoperable, leading to lost sales, delivery failures, and damage to consumer trust.
- **Small and Medium-sized Enterprises (SMEs):** Many SMEs rely on digital communication, cloud services, and online marketing. A loss of connectivity can halt operations, leading to payroll issues, supply chain disruptions, and long-term business failure.

While disruptions pose challenges, many African governments have demonstrated resilience by investing in alternative communication tools, which could be scaled continent-wide. References and inferences from the field must be reflected in the diacissions up ahead.

As detailed by the Global Network Initiative (2025) and the World Economic Forum (WEF, 2025), a commitment to refraining from digital restrictions is no longer merely a civil rights issue; it is a fundamental prerequisite for maintaining **economic stability** and fostering a resilient digital economy in Africa. Protecting the free flow of data is, therefore, a dual imperative that safeguards both civil liberties and the continent's trajectory toward sustained economic growth.

8.2. Proposal: Focused Inclusion of underserved populations (Para 14, 26)

Intervention: The Zero Draft is encouraged to provide dedicated support for the digital inclusion of underserved populations .

Rationale: The forthcoming Zero Draft, in its capacity as a foundational document, must place significant emphasis on the principle of digital equity by explicitly committing to and detailing dedicated support mechanisms aimed at fostering the digital inclusion of underserved populations . This is not merely an aspirational goal but a necessity to ensure that the transformative potential of the digital age is realized by all segments of society, leaving no one behind.

To achieve this, the document ought to outline specific, actionable strategies, including:

1. **Targeted Infrastructure Investment:** Prioritizing the expansion of affordable, reliable digital infrastructure (including broadband access and mobile connectivity) into geographically isolated, low-income, and marginalized areas where underserved populations reside.
2. **Affordable Access and Devices:** Proposing state backed guarantees, financing schemes, or public-private partnerships to reduce the cost of digital devices (smartphones, tablets, computers) and internet services for low-income households and individuals with disabilities.
3. **Digital Literacy and Skills Training:** Designing and implementing culturally sensitive, accessible digital literacy programs tailored to the specific needs of different underserved populations —such as the elderly, persons with disabilities, indigenous populations, refugees, and those with limited educational backgrounds—to build the confidence and skills required to navigate and utilize digital tools safely and effectively.
4. **Accessible Content and Services:** Mandating the adherence to international accessibility standards (e.g., WCAG) for all government and publicly funded digital platforms and services, ensuring information and functionality are usable by individuals with diverse abilities.
5. **Multilingual Support:** Ensuring that digital government services and critical online information are available in multiple languages to overcome linguistic barriers for certain underserved populations .
6. **Safety and Trust:** Incorporating measures to protect vulnerable users from online exploitation, misinformation, and cyber-security threats, coupled with educational campaigns on safe online practices and digital rights.

By dedicating explicit provisions to these areas, the Zero Draft will solidify its commitment to bridging the digital divide and ensuring that digital technologies serve as a catalyst for social and economic empowerment for all, particularly those who face systemic barriers to participation.

- **Use Case and Rationale: Elaborated Text on Digital Access and Inclusivity in Africa**

The imperative for robust digital access across Africa is underscored by both humanitarian needs and the long-term goal of fostering inclusive national development, a concept frequently highlighted in regional policy discussions such as the WSIS Africa Perspectives (2025).

Use Case: Humanitarian Aid and Crisis Response - The Digital Lifeline in Vulnerable Regions

In regions acutely affected by protracted and sudden-onset humanitarian crises digital connectivity transcends its typical role as a convenience, becoming a critical, life-saving

infrastructure. Its availability is foundational for minimizing mortality and morbidity and ensuring the continuity of human dignity amidst upheaval.

I. Enhancing Operational Efficiency for Relief Agencies

Digital infrastructure is essential for the effective coordination and execution of both international and local aid efforts. Relief agencies rely on it for:

- **Supply Chain and Logistics Management:** Real-time data sharing via mobile and satellite networks allows agencies to track the movement of food, medicine, shelter materials, and personnel from global hubs to remote distribution points. This optimizes resource allocation, minimizes waste, and ensures the timely delivery of critical provisions to the most vulnerable populations.
- **Dissemination of Critical Public Health Information:** Digital channels, including SMS, social media platforms, and community-based digital radio, enable the rapid and broad dissemination of vital public health and safety warnings. This includes information on disease outbreaks (e.g., cholera, measles), preventative measures, vaccination schedules, and safe zones—a function crucial for containing epidemics in congested displacement camps.
- **Secure and Reliable Communication Channels:** Reliable digital systems maintain secure communication links between field teams, headquarters, and governmental partners. This security is paramount for protecting sensitive information, coordinating complex multi-agency operations, and ensuring the safety of aid workers in volatile environments.

II. Providing a Crucial Lifeline for Displaced Communities

For refugee and internally displaced communities, digital access serves as a fundamental human right and a tool for self-reliance and protection. It enables them to:

- **Registration and Assistance Access:** Digital identity verification and registration systems streamline the process for displaced persons to receive targeted assistance, including food vouchers, cash transfers, and essential non-food items, improving accountability and reducing fraud.
- **Family Tracing and Reunification:** Connectivity provides a critical means for individuals separated by conflict or disaster to locate family members and re-establish contact, which is essential for emotional well-being and rebuilding social networks.
- **Access to Basic Services and Educational Resources:** Digital platforms offer immediate access to telemedicine consultations, remote mental health support, and critical educational resources, such as online courses and remote learning modules. This ensures that children and adults can continue their education and acquire new skills, maintaining hope and preparing for future self-sufficiency.

III. The Imperative for Resilience and Security

Ensuring reliable, universally accessible, and secure communication systems is paramount to mitigating the devastating, long-term impact of ongoing conflicts and natural disasters in these vulnerable areas. This requires investing in resilient infrastructure that can withstand physical damage, prioritizing network security to protect sensitive data, and developing solutions that are affordable and user-friendly for people with low digital literacy. Ultimately, digital connectivity is a non-negotiable component of a modern, effective, and rights-based humanitarian response.

Rationale: Achieving Comprehensive Digital Inclusivity for Sparse, Geographically Challenged, and Indigenous Populations

Digital inclusion is no longer a peripheral social initiative but a cornerstone of sustainable national development, moving far beyond mere crisis intervention. Its successful execution is fundamentally critical, especially for nations grappling with complex geographical hurdles and diverse demographic landscapes. To bridge the widening digital chasm, comprehensive programs focusing on expansive digital literacy and robust infrastructure development must be strategically implemented. These initiatives must align explicitly with global commitments, such as those articulated in Paragraph 26 of relevant international frameworks and the Sustainable Development Goals (SDGs), to ensure that historically marginalized and remote groups are not systematically excluded from the benefits of the digital economy.

The case of a nation like Namibia, which epitomizes the challenge with its vast, arid, and sparsely populated regions alongside distinct indigenous communities (e.g., San, Himba), provides a crucial blueprint. Standard, one-size-fits-all digital strategies are insufficient here. Instead, **tailored and culturally competent initiatives are absolutely essential.**

These bespoke programs must concentrate on three critical pillars:

1. **Addressing the "Last-Mile" Connectivity Challenge:** This involves innovative solutions that move beyond conventional fiber optics, such as utilizing satellite broadband, high-altitude platform stations (HAPS), and community-owned micro-grids for connectivity. The focus must be on cost-effective, resilient, and energy-efficient infrastructure that can operate effectively in remote environments.
2. **Providing Culturally and Linguistically Appropriate Digital Skills Training:** Digital literacy must be delivered not only in local languages but also through methodologies that respect and integrate traditional knowledge systems. This includes training community leaders as digital champions and developing localized, relevant content (e.g., e-health, agricultural technology, vocational

skills) that immediately translates digital competence into tangible social and economic benefits.

3. **Ensuring Access to Affordable Devices and Digital Public Goods:** Subsidies, public-private partnerships, and innovative financing models are needed to make smart devices accessible to low-income households. Furthermore, promoting open-source tools and Digital Public Goods (DPGs) ensures that basic digital services—like online education platforms and civic engagement portals—are affordable, trustworthy, and interoperable.

This proactive, multi-faceted approach transforms digital inclusion from a theoretical policy goal into a verifiable, lived reality. By overcoming geographic and cultural barriers, indigenous and geographically sparse populations gain full, equitable access to global economic opportunities, essential educational resources, and meaningful civic participation. This level of comprehensive digital integration is the engine for socio-economic transformation, ensuring that the digital dividend is shared equitably across the continent (WSIS Africa Perspectives, 2025).

---

9. Pillar IV: Finance and Investment: Closing the Digital Funding Gap

The aspirations for an equitable Information Society, as outlined in the WSIS+20 Zero Draft, are fundamentally constrained by a systemic digital funding crisis across Africa. The continent requires an estimated $3 billion annually in sustained ICT investment to effectively bridge the infrastructure gap (AIFAT, 2025). This colossal financial deficit is exacerbated by the fact that nearly half of all African nations face high debt burdens, often exceeding critical sustainability thresholds, severely limiting the fiscal space available for essential public investments in infrastructure and digital skills (AIFAT, 2025). Addressing this structural funding deficit is paramount, necessitating a transformation of the high-level commitments of the Zero Draft (Paragraphs 72, 73, and 76) into prescriptive, actionable financial mechanisms.

9.1. Proposal: Endorsing Innovative and Blended Financing Models (Para 76)

Intervention: Stakeholders are encouraged to consider strengthening Paragraph 76 to move beyond general calls for private sector participation and mandate the exploration and scaling of blended financing models that strategically leverage public and private capital for digital development.

Elaboration and Rationale: Traditional commercial investment is often deterred by the low-return, high-risk nature of last-mile and rural connectivity projects. Blended finance—the strategic use of concessional public funding from Multilateral Development Banks (MDBs) and Development Finance Institutions (DFIs) to de-risk private investment—is essential for closing this gap. The WSIS+20 outcome ought to encourage the development of specialized Regional Digital Infrastructure Funds. These

funds would pool risk and provide guarantees, effectively addressing market failures and ensuring predictable returns for private operators engaged in projects vital for universal access. This structured approach, supported by organizations advocating for digital cooperation, is critical for mobilizing the scale of private capital required (Carnegie Endowment, 2025; Digital Convergence Initiative, 2025). Without such proactive financial innovation, new infrastructure will remain concentrated in already profitable urban centers, leaving rural and underserved populations perpetually excluded.

Blended Finance and Innovative Financial Mechanisms for Universal Digital Access

The persistent challenge of achieving universal digital connectivity, particularly in last-mile and rural areas, is fundamentally a financial one. Traditional commercial investment models are often deterred by the inherently low-return, high-risk profile associated with these complex and geographically dispersed connectivity projects. To bridge this significant gap—a chasm often referred to as the 'investment desert'—a paradigm shift towards innovative financial mechanisms is essential.

The Crucial Role of Blended Finance

Blended finance represents the strategic cornerstone of this new financial approach. It involves the coordinated and catalytic use of concessional public or philanthropic funding from Multilateral Development Banks (MDBs) such as the World Bank, the African Development Bank, and the Asian Development Bank, alongside specialized Development Finance Institutions (DFIs). The primary objective of deploying this public capital is not to replace private investment, but rather to strategically de-risk it. By assuming the initial, highest-risk layers of a project's capital stack, blended finance instruments—including first-loss guarantees, subordinated debt, and viability gap funding—effectively enhance the risk-adjusted returns to a level acceptable for private operators and institutional investors. This de-risking function is indispensable for unlocking the scale of private capital required to meet universal access goals.

Developing Specialized Regional Digital Infrastructure Funds (RDIFs)

A critical structural recommendation for the upcoming WSIS+20 outcome is the vigorous encouragement and establishment of specialized **Regional Digital Infrastructure Funds (RDIFs)**. These funds are designed to overcome systemic market failures by creating a pooled investment vehicle that standardizes risk assessment, aggregates diverse connectivity projects, and provides necessary credit enhancements.

- **Risk Pooling and Mitigation:** By grouping multiple smaller, last-mile projects under a single fund structure, the overall idiosyncratic risk is diversified and mitigated. This 'portfolio effect' makes the investment proposition more attractive to larger institutional investors, such as pension funds and sovereign wealth funds, which typically require a certain level of scale and diversification.

- **Guarantees and Credit Enhancement:** RDIFs are ideally positioned to issue standardized performance guarantees and credit wraps. These mechanisms assure private operators of predictable returns on their investment, which is crucial for infrastructure projects with long payback periods. This stability is vital for attracting private operators to projects in markets they might otherwise deem too volatile or risky.
- **Addressing Market Failures:** The establishment of RDIFs is a direct intervention to correct the market failure where the social return on universal access infrastructure significantly outstrips the private financial return. They act as a crucial intermediary, leveraging public mandate to crowd-in private efficiency and capital.

Strategic Imperatives for Digital Cooperation

Organizations advocating for robust digital cooperation, as highlighted by reports from the Carnegie Endowment (2025) and the Digital Convergence Initiative (2025), must champion this structured financial approach. Without such proactive financial innovation and the establishment of dedicated instruments like RDIFs, new digital infrastructure will inevitably remain concentrated in existing profitable markets—namely, densely populated urban centers. This continued concentration deepens the digital divide, leaving rural, remote, and underserved populations in a state of perpetual exclusion from the economic, educational, and social opportunities afforded by the digital economy. Therefore, mobilizing the financial scale and implementing the structural innovation of blended finance and specialized funds is not merely a preference, but a critical prerequisite for achieving the ambitious goal of truly universal and equitable access to information and communication technologies.

9.2. Proposal: Linking Debt Instruments to Digital Development (Para 72)

Intervention: The continent urgently proposes that the final document acknowledges the potential of innovative debt management strategies, specifically exploring frameworks that link debt relief or refinancing to verifiable, results-oriented commitments for digital infrastructure investment (Paragraph 72).

Rationale and Elaborating on the Digital Development Dividend and Debt Sustainability

The integration of debt sustainability with digital development represents a pioneering financial mechanism critical for nations facing the dual challenges of high sovereign debt and the urgent need for digital transformation. This concept is particularly relevant for resource-rich countries, such as Angola, which often possess substantial natural resource wealth yet struggle with heavy debt burdens that severely restrict domestic fiscal space. These financial constraints preempt the allocation of the necessary capital

for large-scale, nationwide digital infrastructure rollouts (WSIS Africa Perspectives, 2025).

The proposed solution—the **Digital Development Dividend (DDD)**—is a strategic financial engineering approach. It mandates a contractual link between any fiscal savings derived from sovereign debt restructuring, relief, or innovative debt-for-development swaps, and their guaranteed earmarking for specific Information and Communication Technology (ICT) projects. This goes beyond general budgetary support; it requires legally binding commitments ensuring that the financial headroom created by debt relief is demonstrably and exclusively channeled into the digital sector.

The DDD mechanism serves several vital purposes:

1. **Ensuring Project Finance Certainty:** It guarantees a predictable and non-volatile source of funding for capital-intensive digital projects, such as fiber optic backbone networks, satellite connectivity for remote areas, and the establishment of national data centers. This predictability is crucial for attracting private sector co-investment and for effective long-term project planning.
2. **Transforming Liabilities into Strategic Assets:** By deliberately linking the reduction of a financial liability (debt) to the creation of a long-term strategic asset (a robust digital foundation), the DDD transforms a short-term fiscal crisis into a catalyst for structural economic change. This approach fosters a sustainable, digitally-enabled path toward economic diversification and resilience.
3. **Enhancing Accountability and Governance:** The contractual nature of the earmarking introduces a higher degree of transparency and accountability into the debt relief process. Creditors and citizens alike can track the tangible outcomes of the debt savings, ensuring that the funds are not diverted to non-productive uses but rather applied to projects that generate measurable developmental impact.
4. **Fostering Digital Economic Resilience:** Ultimately, the successful deployment of these funds into digital infrastructure—promoting digital literacy, e-government services, and digital financial inclusion—is foundational to future economic stability. This strategic investment enables African nations to capture the value of the digital economy, mitigating future reliance on volatile commodity prices and strengthening overall sovereign resilience (AIFAT, 2025).

In essence, the Digital Development Dividend is an innovative financial instrument designed to break the vicious cycle where financial distress indefinitely postpones the indispensable investments needed for digital progress, thereby accelerating Africa's pursuit of comprehensive digital transformation.

9.3. Proposal: Prioritizing Climate-Resilient and Sustainable ICT Investment (Para 73)

Intervention: All financial commitments related to infrastructure (Para 73) must explicitly prioritize investments in climate-resilient and sustainable digital systems to future-proof the sector against escalating environmental risks and ensure long-term operational viability.

Use Case and Consequence: Addressing Climate Resilience and Energy Independence in African ICT Infrastructure

The escalating frequency and severity of extreme weather events across the African continent demand a paradigm shift in the planning and execution of ICT infrastructure development. This necessitates moving beyond standard construction to embrace international resilience standards for critical communication networks. For instance, in countries highly vulnerable to hydro-meteorological hazards like cyclones and catastrophic flooding the imperative is to ensure infrastructure can withstand these shocks. Maintaining operational communications during and immediately following a crisis is not merely a technical requirement but a humanitarian one, enabling effective disaster response, coordination of relief efforts, and timely public warnings (WSIS Africa Perspectives, 2025). The adoption of these rigorous resilience standards must be a non-negotiable condition for all new infrastructure projects in high-risk zones.

Furthermore, this comprehensive proposal incorporates a vital component focused on achieving energy independence for ICT services through dedicated financial support for solar-powered solutions. This is specifically targeted at nations grappling with chronic, systemic power deficits but also applicable to vast swathes of off-grid or poorly serviced rural areas continent-wide. The deployment of energy-independent, green ICT infrastructure serves a crucial triple objective:

1. **Climate Change Mitigation and Adaptation:** By utilizing renewable solar energy, the continent directly contributes to global climate change goals by reducing reliance on fossil fuels and generator power, thereby lowering the carbon footprint of the burgeoning digital economy.
2. **Enhanced Network Reliability:** In regions where the national grid is erratic, unreliable, or entirely non-existent, a standalone solar power system drastically enhances the reliability and uptime of network access points, data centers, and telecommunication towers. This operational stability is fundamental for the sustained growth of digital services.
3. **Economic and Social Inclusion:** Guaranteeing stable and accessible digital services, even in remote and off-grid communities, ensures that the benefits of the digital economy—such as mobile banking, e-health, e-learning, and market access—are universally available. This stability is a key prerequisite for digital inclusion and ensures economic activities can continue uninterrupted,

irrespective of grid failures (African Perspective Note, 2025).

In essence, the strategy proposes an integrated approach where climate resilience and energy sustainability are not optional add-ons, but foundational pillars for building a robust, inclusive, and future-proof digital Africa.

9.4. Proposal: Fostering Public-Private-Community Partnerships (PPCPs)

Intervention: The Zero Draft ought to promote a more nuanced understanding of partnerships that includes community engagement in the planning, financing, and maintenance of digital projects, moving beyond traditional public-private models.

Elaboration and Rationale: **Deepening the Commitment: From PPPs to Inclusive Public-Private-Community Partnerships (PPCPs)**

Achieving genuine, sustained economic growth and securing high, long-term investment returns in the digital development sector necessitates a fundamental shift away from conventional, top-down approaches. True digital transformation requires models that explicitly and robustly champion **local ownership** and meticulously **tailor solutions to specific regional, cultural, and socio-economic needs.** The limitations of standard Public-Private Partnerships (PPPs), which often focus primarily on financial metrics and operational efficiency without deep local integration, become pronounced in the complex and diverse landscapes of rural and underserved areas.

Therefore, the critical evolution lies in the aggressive promotion and deployment of **Public-Private-Community Partnerships (PPCPs)**. This expanded framework deliberately integrates the community as an active, decision-making third partner, moving beyond mere beneficiary status. This structure ensures several critical outcomes:

1. **Local Relevance and Solution Fit:** By involving community leaders, civil society organizations, and local businesses in the planning, design, and execution phases, PPCPs guarantee that digital solutions (e.g., last-mile fibre, community Wi-Fi, localized applications) are not merely imported but are **locally relevant**, directly addressing immediate needs such as access to market information, localized education, and primary healthcare.
2. **Sustainability and Resilience:** Crucially, PPCPs establish **locally sustainable maintenance and operational structures.** This model moves system maintenance and first-line support from a remote, expensive corporate function to a decentralized, local enterprise. Community members are trained and employed to manage the infrastructure, reducing dependency on external resources and ensuring rapid, cost-effective service continuity, which is vital for rural infrastructure longevity.
3. **Risk Mitigation and Investment Stability:** This inclusive, **decentralized governance model dramatically reduces the risk profile of rural infrastructure deployments.** The single biggest failure point for such projects

is often a lack of community buy-in and accountability. PPCPs resolve this by fostering:

- **Community Buy-in:** Active participation translates into a sense of collective ownership and protection of the asset.
- **Accountability:** Local management structures introduce immediate, transparent accountability mechanisms to the end-users.
- **Stable Consumer Base:** When infrastructure is seen as a community asset, adoption rates are higher, and the consumer base is more stable, generating predictable revenue streams essential for long-term viability.

This integrated approach is not merely a social consideration; it is a **critical, proven financial strategy** for the long-term success, financial stability, and scalability of high-impact digital initiatives across the continent (as highlighted in the *WSIS Africa Perspectives, 2025* report). By internalizing the social and operational costs of non-inclusion, PPCPs deliver superior return on investment and more equitable development outcomes.

---

10. Pillar V: Digital Public Infrastructure (DPI) and Innovation

Intervention: The continent recognizes DPI as a key enabler for scaling digital transformation and bridging sectoral divides (AIFAT, 2025).

Rationale: **The Foundational Role of Digital Public Infrastructure (DPI) in Africa's Strategic Development Agenda**

Digital Public Infrastructure (DPI) has firmly established itself not merely as a technical priority, but as a recognized cornerstone of Africa's overarching strategic vision for **accelerated economic development** and deeper **regional integration**. The widespread continental consensus explicitly recognizes DPI as a fundamental and foundational **enabler**, positioning it as central to achieving modern socioeconomic objectives.

This critical recognition stems from DPI's **proven and scalable capability** to drastically increase the pace, reach, and depth of digital transformation initiatives across virtually all sectors. This is deemed essential for the realization of **inclusive economic growth** that benefits all segments of society, a primary goal of African Union's Agenda 2063.

Key Strategic Mechanisms and Impact:

Furthermore, DPI is championed as a vital and **critical mechanism** for systematically and effectively bridging the significant **sectoral divides** that currently impede comprehensive progress. By providing secure, interoperable, and standardized technological foundations, DPI fosters greater **efficiency, transparency, and accountability** across the public and private spheres. This transformative impact is most evident in key sectors:

- **Finance:** Driving financial inclusion through instant, low-cost payment systems.
- **Healthcare:** Enabling seamless digital health records, telemedicine, and targeted public health interventions.
- **Education:** Expanding access to quality learning resources and digital credentials.
- **Governance:** Improving public service delivery, enhancing citizen engagement, and combating corruption.

Formal Continental Alignment and Endorsement:

The strategic importance of DPI is not merely a policy aspiration but is a formally documented and robustly supported continental alignment. This consensus is formally endorsed and guided by key intergovernmental bodies and frameworks. A prime example is the explicit recognition and detailed support provided in foundational documents, notably highlighted in reports such as the **Africa Integrated Framework for Action on Technology (AIFAT, 2025)**. Such frameworks codify DPI as an indispensable element for building a cohesive, competitive, and digitally sovereign Africa. The momentum behind DPI is thus rooted in high-level political commitment and a shared understanding of its indispensable nature for future prosperity.

10.1. Proposal: Endorsing Africa-Centric DPI (Para 35, 56)

Intervention: African stakeholders encourage the Zero Draft to explicitly support the development of **Africa-centric DPI**, based on principles of interoperability, openness, and security (AIFAT, 2025).

Rationale: African stakeholders are strongly encouraging that the Zero Draft explicitly includes provisions to support the comprehensive development of Africa-centric Digital Public Infrastructure (DPI). This push emphasizes the need for a framework that is tailored to the continent's unique needs, socio-economic context, and diverse regulatory environments.

The proposed Africa-centric DPI must be firmly rooted in a set of core principles to ensure its success and widespread adoption. Specifically, stakeholders, as highlighted in the African Internet Forum and Africa Tech (AIFAT) report from 2025, are advocating for the following:

1. **Interoperability:** The DPI must be designed to seamlessly connect and communicate across different systems, platforms, and national borders within Africa. This ensures a unified digital market and facilitates cross-border services, trade, and data exchange.
2. **Openness:** A commitment to open standards, open-source technology, and open APIs is essential to foster innovation, prevent vendor lock-in, and ensure that the infrastructure is accessible, adaptable, and owned by African nations and communities.
3. **Security:** Robust security and privacy safeguards must be built into the foundation of the DPI. This includes resilient cybersecurity measures to protect critical data and infrastructure, as well as adherence to data protection laws to build and maintain public trust.

The development of such an infrastructure is viewed as critical for accelerating digital transformation, promoting financial inclusion, improving public service delivery, and empowering citizens across the continent, ensuring that Africa's digital future is self-determined and sustainable.

- **Use Case and Rationale:** Digital Public Infrastructure (DPI), encompassing foundational elements such as digital identity (ID), interconnected payment systems, and robust data exchange platforms, is increasingly recognized as a critical accelerator for economic integration and trade across the African continent. This recognition is particularly salient in the context of the **African Continental Free Trade Area (AfCFTA)**, where seamless digital systems are deemed essential for realizing the full potential of intra-African commerce and cooperation (Carnegie Endowment, 2025).

The deployment of integrated DPI not only facilitates economic goals but also translates into significant improvements in the efficiency and reach of public service delivery. The experience of nations like **Rwanda** provides a compelling case study, where advanced, integrated e-government services have streamlined citizen interactions with the state, setting a benchmark for the continent (WSIS Africa Perspectives, 2025). Such digital sophistication allows governments to deliver services more effectively, from health and education to taxation and social protection.

Building upon these foundational elements, the development of **sectoral DPIs** is poised to drive targeted improvements in specific economic and social sectors (refer to **Para 71** for further details on sectoral DPIs). These applications leverage the underlying ID, payment, and data exchange layers to create specialized digital ecosystems. For instance, in the agricultural sector—a cornerstone of many African economies—sectoral DPIs can be deployed to streamline services for smallholder farmers. The successful integration of digital technologies across various sectors, particularly agriculture, is a transformative trend being championed by many African nations. The experiences of countries such as **Malawi** and **Ethiopia** serve as compelling examples, showcasing the profound impact these digital tools can have on modernizing farming practices and improving rural livelihoods.

In these contexts, digital solutions have been instrumental in significantly enhancing **agricultural extension services**. Mobile applications and interactive voice response (IVR) systems, for instance, are enabling agricultural experts to reach a far greater number of smallholder farmers with targeted, context-specific advice. This includes best practices for soil management, pest and disease control, and optimal irrigation techniques.

Furthermore, these digital platforms are revolutionizing farmers' **access to markets**. By providing real-time price discovery and connecting producers directly with potential buyers, they eliminate layers of intermediaries, leading to better prices for produce and reducing post-harvest losses. Digital marketplaces and e-commerce platforms are becoming vital infrastructure for a more transparent and efficient agricultural value chain.

A critical function of these technologies is the provision of **timely weather and planting information**. Using sophisticated data analytics and satellite imagery, digital systems can deliver hyper-localized forecasts and advisory notes directly to farmers' phones. This crucial information allows farmers to make data-driven decisions about when to plant, irrigate, and harvest, thereby mitigating risks associated with erratic weather patterns and ultimately boosting yields.

Finally, the adoption of digital tools has proven highly effective in ensuring a **more efficient and transparent subsidy distribution**. By using digital identification and mobile money platforms, governments can directly disburse farming inputs, seeds, or financial aid to verified beneficiaries. This system minimizes leakage, reduces corruption, ensures that subsidies reach the intended recipients promptly, and facilitates better tracking and evaluation of government support programs (Digital Convergence Initiative, 2025; WSIS Africa Perspectives, 2025). The overall effect is a significant step towards greater food security and economic resilience in the agricultural sector.

Ultimately, the strategic, layered deployment of DPI—from foundational components to sector-specific applications—is seen as vital for fostering sustainable development, improving governance, and achieving the ambitious goals of continental integration.

10.2. Proposal: Youth and Gender Entrepreneurship (Para 13, 38)

Intervention: The document is encouraged to facilitate investment and regulatory environments that support youth and women-led digital entrepreneurship (**Para 38**).

Rationale: Recognizing the immense potential of inclusive digital transformation, a core recommendation is the active encouragement of an enabling environment for investment and regulatory frameworks that specifically champion youth and women-led digital entrepreneurship. This initiative goes beyond simple support, aiming to dismantle systemic barriers and foster an ecosystem where these demographic groups can thrive in the digital economy.

To achieve this, the following elements are critical:

- **Targeted Investment Mechanisms:** Establishing dedicated funds, venture capital, and angel investor networks that prioritize startups and digital businesses founded by young people and women. This includes providing seed funding, technical assistance, and access to financial literacy programs tailored to their unique needs.
- **Regulatory Modernization:** Reviewing and reforming existing business registration, licensing, and taxation policies to be more accessible, affordable, and flexible for nascent, digital-first ventures. Special attention must be paid to reducing the bureaucratic burden and eliminating biases that disproportionately affect women and youth starting businesses.
- **Capacity Building and Mentorship:** Launching comprehensive programs that

offer digital skills training, business management courses, and access to mentorship networks with established entrepreneurs. These programs ought to address the specific challenges faced by youth and women, such as access to networks and work-life balance.

- **Access to Digital Infrastructure:** Ensuring equitable access to affordable, high-speed internet and essential digital tools, especially in underserved regions, as a foundational prerequisite for any digital enterprise.

By focusing on these areas, the document aims to harness the innovative spirit of youth and the economic empowerment of women, thereby driving inclusive economic growth and accelerating digital transformation (**Para 38**). This systematic approach ensures that the benefits of the digital economy are widely distributed and that diverse perspectives contribute to the future of digital innovation.

- **Use Case and Rationale: Empowering Women for Africa's Digital Economy: A Strategic Imperative for Inclusive Growth**

The integration and empowerment of women within the technology and business spheres are universally recognized as not just a moral necessity but a fundamental economic imperative for sustained African development. This viewpoint has been firmly adopted as a strategic national priority by some African nations, including **Egypt** and **Senegal** (as highlighted in *WSIS Africa Perspectives, 2025*). These governments have publicly acknowledged that the deliberate exclusion of women from the digital economy represents a significant ceiling on national productivity and a barrier to achieving truly inclusive growth. Their commitment goes beyond rhetorical policy statements, translating into concrete actions designed to systematically dismantle entrenched structural and socio-cultural barriers that hinder women's full participation.

Dismantling Regulatory Barriers to Foster Entrepreneurship

A key component of accelerating economic growth and maximizing the potential of the female workforce is the cultivation of a business environment highly conducive to innovation and enterprise. **Tanzania** has emerged as a continental leader in this regard, setting a robust precedent by proactively addressing the complex, often opaque regulatory hurdles that disproportionately stifle nascent startup ventures. These challenges are particularly acute for businesses founded by young entrepreneurs and, critically, by women.

The country's strategy focuses on a comprehensive simplification of the business landscape. This involves:

- **Streamlining Business Registration:** Implementing digital, rapid, and transparent processes for company formation.

- **Reducing Bureaucratic Red Tape:** Eliminating unnecessary layers of administrative oversight and requirements.
- **Standardizing and Simplifying Tax Processes:** Creating predictable and easily understandable tax frameworks.

By implementing such efficiencies, nations drastically lower the financial and time-based barrier to entry. This simplification acts as a powerful catalyst, encouraging a substantial surge in entrepreneurial activity, especially among underserved demographics.

Strategic Investment in Local Innovation Ecosystems

Furthermore, guaranteeing sustained and robust economic expansion requires precise, targeted investment into local innovation ecosystems. African nations must make a strategic commitment to funding and scaling a network of local innovation hubs, incubators, and accelerators situated across the continent. This localized infrastructure is absolutely vital for nurturing and equipping the next generation of African tech leaders and business innovators.

These specialized centers provide essential, high-impact resources that are often inaccessible to local talent:

- **Professional Mentorship:** Connecting aspiring entrepreneurs with experienced industry veterans and successful founders.
- **Seed Capital and Access to Funding:** Providing the critical early-stage investment required to move from concept to market-ready product.
- **Access to International Networks:** Facilitating partnerships, market entry, and technology transfer beyond national borders.

This structured support system is instrumental in bridging the resource gap and transforming raw ingenuity into market-ready, scalable businesses.

Harnessing the Demographic Dividend

Ultimately, the focused effort on enhancing regulatory efficiency and providing robust financial and infrastructural support is positioning African countries to effectively harness their most profound competitive advantage: the demographic dividend. This dividend is characterized by the continent's rapidly expanding, predominantly youthful, and increasingly digitally native population. This massive cohort represents a powerful, untapped reservoir of energy, creativity, and ingenuity.

The energy and potential of this population, particularly among its female cohort, are poised to be the principal driver of unprecedented social and economic transformation in

the coming decades (*WSIS Africa Perspectives, 2025*). By strategically empowering women in the digital age, African nations are not merely fixing an inequality; they are activating a core engine for durable, continent-wide prosperity.

---

11. A Call for Southern Partnerships

The African intervention on the WSIS+20 Zero Draft stands as a clarion call for a fundamental recalibration of the global digital agenda, urging the international community to honor the spirit of a truly inclusive and development-focused Information Society. This proactive stance, encapsulated within the African Perspective Note (2025), is not a rejection of the draft, but rather a sophisticated invitation for a renewed, equitable, and actionable global partnership for the next two decades.

Africa's proposals are anchored in a set of critical, non-negotiable principles necessary for bridging the digital divide and fostering genuine digital empowerment across the continent:

1. **Affordability and Accessibility (Para 28, 62):** The continent emphasizes the need for concrete, measurable commitments to ensure that digital access is not a luxury but a fundamental right. This includes addressing the prohibitive cost of devices, reducing data tariffs, and expanding broadband infrastructure into underserved rural and marginalized communities. The intervention seeks clearer language that moves beyond aspirational goals to specific financial and technical support mechanisms for Least Developed Countries (LDCs) and landlocked nations.
2. **Digital Sovereignty and Data Governance (Para 94):** A core element of the African position is the assertion of national digital sovereignty. This calls for mechanisms that empower individual nations to exercise control over their own data ecosystems, digital policy-making, and technological choices, free from undue external influence. It stresses the imperative for international frameworks to respect national laws concerning data localization, cross-border data flows, and the development of sovereign cloud infrastructure, ensuring that the digital future aligns with national development objectives and security interests.
3. **Rights Protection and Governance Frameworks (Para 88):** Africa firmly advocates for robust, rights-based governance frameworks that safeguard human rights in the digital sphere. This encompasses freedom of expression, privacy, and protection against digital discrimination and surveillance. The intervention calls for clear commitments to combat the proliferation of harmful content, while simultaneously ensuring that regulatory measures do not stifle digital civic space or legitimate critique. The protection of underserved populations , including women, youth, and persons with disabilities, from online harm is a paramount concern.
4. **Development and Deployment of Digital Public Infrastructure (DPI):** The push for DPI development is central to Africa's long-term digital transformation. This involves securing global commitments for technical and financial support to build foundational digital systems—such as digital identity, interoperable payment systems, and data exchange layers—that can underpin public service delivery, boost economic inclusion, and foster home-grown innovation. This focus ensures that the technological architecture is citizen-centric and serves

broader sustainable development goals.

---

12. Conclusion: Forging an Equitable Digital Future

The WSIS+20 Review is a moral and developmental imperative for the global community. For African nations, the Zero Draft outcome document must serve as more than a reiteration of past aspirations; it must be a **pragmatic, financially backed roadmap** for achieving true digital equality and resilience. This comprehensive position, structured around the five pillars of Connectivity, Sovereignty, Finance, Rights, and Digital Public Infrastructure (DPI), reflects the unified will of the African continent to assert control over its digital destiny and align global efforts with the objectives of the **African Union's Agenda 2063** (African Perspective Note, 2025; AIFAT, 2025). The successful finalization of this document represents a pivotal opportunity to rectify historical inequalities and ensure the Information Society is genuinely inclusive.

12.1 A Call for Actionable Commitments

The continent's proposals are aimed at translating broad, high-level principles into measurable, impact-oriented action, which is essential for mobilizing resources and ensuring accountability:

- **Connectivity and Affordability:** By respectfully urging negotiators to adopt a **2% GNI affordability target** for mobile data, the outcome document can actively dismantle the single greatest economic barrier to entry for millions of citizens. This commitment extends beyond mere infrastructural access; it demands **meaningful connectivity**, defined by adequate speed, regularity, and access to the necessary tools and digital skills (ITU, 2022). Failure to address this cost disparity effectively will render new infrastructure investments redundant for the poorest 50% of the population, trapping entire communities in a cycle of digital exclusion and constraining socio-economic growth.
- **Sovereignty and Security:** The call to explicitly support **sovereign data governance** and capacity building is a direct response to the risks of data colonialism and external technological dependency. Exemplified by robust legal frameworks in countries like South Africa (**POPIA**) and Kenya, this action ensures that Africa's vast, high-value data resources primarily benefit the continent and are protected by internationally recognized, yet domestically controlled, legal and technical mechanisms (Pollicy, 2024; KICTANet, 2025). Furthermore, this initiative is crucial for bolstering national cyber resilience, especially in facing escalating cyber threats that disproportionately target developing digital economies.
- **Finance and Investment:** Recognizing the continent's systemic debt challenges and the substantial **$3 billion annual ICT funding gap** (AIFAT, 2025), the final text must embrace **innovative financing**. This requires more than simply calling for private sector participation; it necessitates concrete mechanisms through which Multilateral Development Banks (MDBs) and global financial institutions deploy **blended finance models** and, where appropriate, consider linking debt

instruments to resilient digital infrastructure investments. This linkage is vital to ensure long-term sustainability and stability, particularly for nations recovering from conflict or economic distress.

- **Trust, Human Rights and Digital Freedom:** The call for establishing clear international best practices and safeguards regarding digital restrictions, such as digital restrictions and censorship, is a **strategic imperative** to enhance the predictability and stability of the digital environment across the continent. Such a collective commitment offers a critical safeguard, as these restrictions can pose material challenges to sustained economic growth, impact the functionality of essential services, including mobile money and e-health, and constrain the efficiency of humanitarian operations. By prioritizing a firm, shared commitment to these rights-respecting frameworks, the global community can lay a vital foundation for a predictable and resilient digital future.
- **Digital Public Infrastructure (DPI):** By supporting an **Africa-centric, interoperable DPI model**, the WSIS+20 outcome can accelerate the continent's economic integration and transformation. This model, focusing on open-source, foundational digital systems (like digital identity and instant payments), will leverage digital platforms to scale services, critically facilitate the objectives of the **African Continental Free Trade Area (AfCFTA)**, and unlock the immense economic potential of youth and women-led entrepreneurship (Carnegie Endowment, 2025). The development of shared, secure DPI promotes efficiency, reduces transaction costs, and ensures that the foundation of the continent's digital economy remains adaptable and democratically accessible.

12.2 Appeal to Negotiators

This comprehensive position is submitted in the spirit of constructive engagement, partnership, and mutual respect for the sovereign decisions of all stakeholders. The inclusion of these targeted, evidenced-based proposals—which move beyond general statements to prescriptive action—is absolutely essential to ensure the WSIS+20 outcome is not viewed as a success merely in Geneva, but as a **transformative catalyst for genuine, equitable development across Africa and the wider Global South**. We could go even further. Focusing on a future which is emerging but not yet in official discourse : Fluid Institutions and Fluid Institutionaism. We have added an Annex (A) in this regard for the interested reader and we would then call it the Sixth Pillar. Annex B provides some immediate future pathways for consideration. These two annex have not been included in the primary text of this paper to maintain a seamless structural integrity of the narrative picture.

We urge the negotiating parties to embrace this opportunity by incorporating these amendments. Paving the way for a truly inclusive and equitable Information Society over the next two decades requires a commitment to addressing the deepest structural digital divides. The lasting success of WSIS+20 will ultimately be measured by its tangible positive impact on the communities and citizens that need its commitments the most.

References

1. African Perspective Note (2025) Note on An African Perspective for the WSIS+20 Zero Draft Outcome Document and Its Impacts on Data Security, Data Sovereignty, Innovation, Entrepreneurship, and Finance. [Unpublished Document].
2. AI for Africa ThinkTank (AIFAT) (2025) Africa's Strategic Positioning in the WSIS+20 Review: A Roadmap for Affordable and Accessible Digital Ecosystems. [Unpublished Document].
3. Carnegie Endowment (2025) Digital Public Infrastructure: A Practical Approach for Africa. Available at: https://carnegieendowment.org/research/2025/02/digital-public-infrastructure-a-practical-approach-for-africa?lang=en (Accessed: 18 October 2025).
4. Context by TRF (2025) Q&A: Africa's digital restrictions double in less than a decade. Available at: https://www.context.news/digital-rights/q-and-a-africas-internet-shutdowns-double-in-less-than-a-decade (Accessed: 18 October 2025).
5. Digital Convergence Initiative (2025) Advancing digital public infrastructure for social protection. Available at: https://spdci.org/resource/advancing-digital-public-infrastructure-for-social-protection/ (Accessed: 18 October 2025).
6. Digital Cooperation Organization (DCO) (2025) Digital Public Infrastructure. Available at: https://dco.org/wp-content/uploads/2025/06/DPI-Policy-Paper.pdf (Accessed: 18 October 2025).
7. Global Network Initiative (2025) The economic impact of disruptions to Internet connectivity A report for Facebook. Available at: https://globalnetworkinitiative.org/wp-content/uploads/GNI-The-Economic-Impact-of-Disruptions-to-Internet-Connectivity.pdf (Accessed: 18 October 2025).
8. International Telecommunication Union (ITU) (2022) The affordability of ICT services 2022. Available at: https://www.itu.int/en/ITU-D/Statistics/Documents/publications/prices2022/ITU_Price_Brief_2022.pdf (Accessed: 18 October 2025).
9. KICTANet (2025) Balancing Innovation and Data Sovereignty in Kenya. Available at: https://www.kictanet.or.ke/balancing-innovation-and-data-sovereignty-in-kenya/ (Accessed: 18 October 2025).
10. Lucidity Insights (2024) Mobile Broadband (2GB) Prices Relative to Gross National Income per Capita, 2022-2023. Available at: https://lucidityinsights.com/infobytes/mobile-broadband-prices-gni-per-capita-2022-2023 (Accessed: 18 October 2025).
11. Pollicy (2024) Introduction. Available at: https://pollicy.org/wp-content/uploads/2025/04/Policy-brief-28-Jan.pdf (Accessed: 18 October 2025).
12. Startup Graveyard Africa (2025) What is Digital Sovereignty, and How Are African Countries Approaching It?. Available at:

https://startupgraveyard.africa/blog/what-is-digital-sovereignty-african-countries-approach (Accessed: 18 October 2025).

13. World Economic Forum (WEF) (2025) How digital restrictions silently drain Africa's economy. Available at: https://www.weforum.org/stories/2025/06/how-internet-shutdowns-drain-african-economies/ (Accessed: 18 October 2025).
14. WSIS Africa Perspectives (2025) WSIS combined temp [Document containing African Perspectives and Relevant WSIS Zero Draft Articles]. [Unpublished Document].

Annex A: Pillar VI: Liquid Institutions for Adaptive Digital Governance

Intervention: In an era marked by rapid technological disruption and evolving global challenges, African nations recognize the need for governance models that transcend rigid structures. Drawing on the principles of liquid institutionalism, this pillar advocates for the integration of adaptive, fluid frameworks into the WSIS+20 Zero Draft to foster resilient digital ecosystems. Such institutions, characterized by adaptability, agency, and agility, can address institutional voids in the Global South by leveraging AI and blockchain for dynamic decision-making (Mamun et al., 2025).

A6.1. Proposal: Embedding Liquid Institutionalism in Digital Policy (Para 97, 99)

Intervention: The continent proposes strengthening Paragraphs 97 and 99 to explicitly endorse liquid institutions as a foundational element for digital governance. This involves recognizing frameworks that emphasize adaptivity—allowing institutions to evolve in real-time with technological shifts; agentic action—empowering stakeholders to drive change through participatory mechanisms; and agility—enabling swift responses to crises like disinformation or cyber threats.

Rationale: Liquid institutionalism builds on established theories, such as those contrasting historical and rational choice institutionalism with more dynamic approaches, to create transformative knowledge ecosystems. For instance, in contexts like Bangladesh's real-time rumor tracking during crises or Nigeria's fintech innovations, these models have demonstrated potential to enhance national security and economic equity. By connecting to WSIS goals, liquid institutions can mitigate digital divides, ensuring that connectivity (Pillar I) and sovereignty (Pillar II) are not static but evolve with human rights protections (Pillar III) and innovative financing (Pillar IV). This alignment supports Africa-centric DPI (Pillar V) by fostering gamification and participatory engagement, where youth and women lead entrepreneurship in interoperable systems.

Use Case: In the Indian Ocean region, liquid institutions could facilitate South-South cooperation, underwriting innovation as alternatives to traditional aid. For example, adaptive governance in mobile financial services, enhanced by reinforcement learning, has reduced poverty by optimizing credit scoring and fraud detection, aligning with UN SDGs and Agenda 2063.

A6.2. Proposal: Capacity Building for Liquid Frameworks (Para 15, 56)

Intervention: African stakeholders encourage the Zero Draft to include provisions for international support in developing liquid institutional capacities, such as training programs and pilot initiatives. This would involve collaborating on ethical AI deployment, drawing from semantic differentials that highlight fluid models' strengths in agency and time orientation over rigid paradigms.

Rationale: By integrating liquid institutionalism, WSIS+20 can catalyze a narrative of resilient futures, addressing influence operations and information sovereignty. This extends previous explorations of fluid institutions in AI-driven development, promoting equity in the digital economy while safeguarding against vulnerabilities like disproportionate restrictions.

Works Cited

Bauman, Z. (2000) *Liquid modernity*. Polity.

Mamun, S.M., Umegbolu, O. and Matin, A.A. (2025) *Building resilient futures through fluid institutionalism: A strategic approach to influence operations and national security*. AI for Africa Thinktank.

United Nations (2025) *WSIS+20 zero draft outcome document*. United Nations General Assembly.

ANNEX B: Pathways into the Immediate Future – Proposed New Pillars for the Pan-African Diplomatic Position

This Annex outlines additional strategic pillars and focus areas designed to enhance the African diplomatic position on the WSIS+20 Zero Draft, ensuring the final outcome is comprehensive, future-proof, and fully aligned with the continent's long-term digital transformation and development goals (Agenda 2063).

Proposed Annex Pillar	Focus Area and Rationale	Strategic Proposal for WSIS+20 Text
1. AI, Emerging Technologies, and Ethical Governance	**Rationale:** To move Africa from a recipient of foreign technology to a **shaper and innovator** of new technologies, ensuring AI deployment is safe, ethical, and bias-free. A dedicated pillar is necessary given the rapid pace of technological change.	**Advocate for:** Mandating international commitments for **technology transfer** and **financial support for African AI Research Hubs**. Urge the adoption of **Africa-centric ethical AI principles** to prevent algorithmic bias, while prioritizing the use of AI for achieving the Sustainable Development Goals (SDGs) in critical sectors like agriculture and public health.
2. Digital Trade, Harmonization, and the Single Digital Market (SDM)	**Rationale:** The success of the African Continental Free Trade Area (AfCFTA) requires an integrated, secure, and legally coherent **Single Digital Market**. Policy fragmentation severely hinders cross-border e-commerce and investment.	**Advocate for:** Explicit inclusion of targets to **harmonize data protection, e-commerce, and digital taxation regulations** across African Regional Economic Communities (RECs). Insist on international support for developing **interoperable digital payment systems** and regional digital identity frameworks to facilitate seamless, secure continental trade.

Proposed Annex Pillar	Focus Area and Rationale	Strategic Proposal for WSIS+20 Text
3. Cybersecurity and Digital Resilience	**Rationale:** Digital sovereignty and the protection of critical national infrastructure (CNI)—such as finance, power, and telecommunications—depend on robust cybersecurity capacity. This is a foundational element of the AU's Digital Transformation Strategy.	**Advocate for:** A formal commitment to **strengthen national and regional Computer Emergency Response Teams (CERTs)** through dedicated funding and training. Propose the adoption of common **minimum cybersecurity standards** for CNI and increased international cooperation for **cyber diplomacy and capacity building** across African governments and judicial systems.
4. Monitoring, Evaluation, and Accountability (M&E)	**Rationale:** To ensure the WSIS+20 outcome is not merely a declaration but an enforceable roadmap. The lack of robust accountability mechanisms limits the implementation of global commitments.	**Advocate for:** The establishment of a **formal linkage between the WSIS+20 review and existing SDG monitoring frameworks** to track digital development progress quantitatively. Propose a requirement for a **dedicated, annual African Digital Progress Report** that includes multi-stakeholder participation (governments, civil society, private sector) to ensure transparent oversight and accountability for meeting defined targets.

Epilogue

As the echoes of these proposals fade into the annals of diplomatic discourse, let us pause to envision the horizon they illuminate. The WSIS+20 Outcome Document, if infused with the spirit of these pillars—Connectivity, Sovereignty, Finance, Rights, and Digital Public Infrastructure—will not merely close divides but forge unbreakable bonds of global solidarity. Yet, true transformation demands vigilance: the fluid institutions we advocate in our annexes remind us that governance must evolve with technology, adapting like water to the contours of change. To African negotiators and global partners alike, this is an invitation to legacy-building—a commitment to a digital ecosystem where every citizen thrives, unhindered by barriers of cost, control, or circumstance. In forging this equitable future, we honor not just the aspirations of today but the dreams of generations yet unborn, ensuring that Africa's digital dawn rises bright and boundless.

@AI FOR AFRICA 2025