

Project Members: Célia Barhoumi, Laurane Yara, Louise Alima Bodian, Yoko Tanaka

Partner: Mr. Antoine Barbry (Organisation internationale de la Francophonie (OIF))

Academic Supervisors: Dr. Jérôme Duberry

Applied Research Project: Final Report

Word Counts (excl. references): 10474 words

AfriNIC:

Digital Sovereignty and Governance in Africa

AI statement: All writing in this inception report is our own. AI tools were used only for grammar checking, translation of texts and transcripts, bibliography generation, and producing our interview transcripts. Additionally, AI was used to produce anonymised summaries of interview content to help identify broader themes and categories. All AI-generated outputs were carefully reviewed to ensure accuracy and to support the integrity of our research (12/05/2026)

Contents

I - Introduction	4
II - Literature Review	5
2.1. Introduction	5
2.2. The Political Economy of Critical Internet Resources: The Commodification of IPv4	5
2.3. The Jurisdictional Paradox: Legal Vulnerabilities of the Multistakeholder Regime	6
2.4. Geopolitical Perspectives in the Global South: Multistakeholderism vs. Digital Sovereignty	7
III - Theoretical framework	8
3.1. The Political Economy of Critical Resources: Commodification	8
3.2. The Jurisdictional Paradox and "Lawfare"	8
3.3. Institutional Capacity and the Failure of Consensus	8
3.4. Power Asymmetry and Digital Neocolonialism	9
3.5. Research Hypotheses	9
IV - Methodology	9
4.1. Data Collection	9
4.2. Data Analysis Methods	10
4.3. Reliability and Validity of Our Research	11
4.4. Limitations	11
V - Findings	12
Section 1 - IPv4 Scarcity and the Governance of Number Resources	12
5.1.a. Scarcity of IPv4 Addresses and Corporate Greed	12
5.1.b. IPv6 Transition Failure	13
5.1.c. IPv4 Transfer Policies as a Resilient Mechanism	14
Section 2 - Systemic vulnerability of AfriNIC	15
5.2.a. Legal Fragility and Jurisdictional Mismatch	15
5.2.b. Internal Governance Failures	16
5.2.c. Board Instability and Institutional Capture	17
Section 3 - Sovereignty Debate - Multistakeholderism vs Multilateralism	18
5.3.a. Structural critique of Multistakeholderism: Neocolonial Asymmetries	18
5.3.b. The Sovereignty Awakening in African Governance Dynamics	19
5.3.c. MSH vs. ML	20
VI - Discussion	21
6.1. Legal vulnerability and Structural tension within the MSH model (H1)	21
6.2 IPv4 as a Market Commodity and Private Capture (H1)	21
6.3. Institutional Capacity and the Limits of Consensus (H2)	22
6.4. Power Asymmetry and Digital Colonialism (H2)	23
VII - Conclusion	24
VIII - References	25
7.1. Primary sources	25
7.2. Secondary sources	26
IX - Annexes	28

Annex 1: Visual Stakeholder Mapping	28
Annex 2: Recommendations	29
Annex 3: Interviewee IDs	31
Annex 4: Deductive Coding Framework (Precoding)	32
Annex 5: Codebook	34
Annex 6: Informed Consent and Ethical Consideration	54
Annex 7: Acronyms	57

I - Introduction

The governance of critical digital infrastructure in Africa is currently defined by a fundamental friction. The global “multistakeholder” (MSH) model, which conceptualises the internet as a borderless network, is increasingly at odds with African nation-states asserting “digital sovereignty” to regain control over their digital spaces (Pohle & Santaniello, 2024). While the internet is global in reach, its actual management remains regional. In Africa, this responsibility falls to AfriNIC (African Network Information Centre), the registry charged with allocating IP addresses across the continent.

AfriNIC’s trajectory began long before its formal ICANN accreditation in 2005. Its origins lie in the late 1990s, specifically a pivotal 1998 meeting in Cotonou where African professionals convened to “reclaim agency” over the continent’s digital resources (Vitus, 2025). Their objective was explicit: to end reliance on external registries and to construct a sustainable, community-led structure capable of adapting global policies to African realities. For over a decade, AfriNIC operated as a private entity, serving as the institutional embodiment of this regional autonomy (AfriNIC, n.d.).

Operationally, the organisation serves the entire African continent, distributing IP addresses and ASNs regionally. Legally, however, it is anchored in Mauritius, where it is headquartered and incorporated as a company limited by guarantee. This distinction is crucial: despite its continental mandate, AfriNIC’s corporate governance is bound by Mauritian domestic law and lacks international immunity (Vitus, 2025). This specific legal geography has become the focal point of the organisation’s recent destabilisation.

This subject is urgent because AfriNIC has been paralysed by an unprecedented governance crisis since 2022. The organisation has been forced to function without a board following a barrage of lawsuits initiated by Cloud Innovation Limited, a Seychelles-registered broker controlled by Chinese entrepreneur Lu Heng (Mueller, 2021). Originally stemming from a dispute over the misuse of scarce IPv4 addresses, the conflict escalated into a campaign of “lawfare” (Vitus, 2025). This strategy successfully utilised Mauritian courts to freeze AfriNIC’s bank accounts and block its elections, effectively holding the registry hostage (The Register, 2023).

Ultimately, the paralysis at AfriNIC forces us to look beyond the immediate legal battles and question the stability of the global internet governance system itself. Asking this is crucial because there is currently a blind spot in the academic discussion: while extensive theory exists on how the global MSH model *should* work, there is very little empirical research on what happens when its decentralized, private-law architecture fails to protect a continental guardian of digital commons from corporate lawfare. To address this gap, our research is guided by the following central question: *What does the AfriNIC crisis illustrate about the challenges of regional internet governance in Africa?*

To answer this question, this thesis is structured as follows. Section 2 reviews the existing literature on the political economy of IP addresses, jurisdictional paradoxes, and geopolitical perspectives relevant to the AfriNIC crisis. Section 3 outlines the theoretical framework and our central hypotheses. Section 4 details our qualitative methodology, based on expert interviews and document analysis. Section 5 presents our empirical findings regarding the commodification of IPv4, AfriNIC’s legal and internal fragilities, and the debate on digital

sovereignty under multistakeholderism. Finally, Section 6 provides a comprehensive analysis of these results, answering our hypothesis.

II - Literature Review

2.1. Introduction

Academic literature increasingly documents a profound structural transition in Internet governance. While the Internet's underlying architecture was historically perceived as a neutral, technical coordination system driven by engineering consensus, contemporary scholarship overwhelmingly analyzes it as a highly contested geopolitical and economic arena. To contextualize the AfriNIC institutional crisis, this literature review examines three intersecting academic debates. First, it explores the political economy of critical internet resources, specifically analyzing how literature accounts for the market commodification of the IPv4 protocol (Weber & Heinrich, 2011; Livadariu, Elmokashfi & Dhamdhare, 2017). Second, it reviews the complex jurisdictional paradoxes and systemic legal vulnerabilities inherent to the privatized multistakeholder (MSH) regime (Mueller, 2010; Kettemann, 2020). Finally, it addresses the geopolitical discourse concerning the Global South, where scholars increasingly contrast the liberal MSH model with emerging demands for state-centric digital sovereignty and intergovernmental oversight (Flonk, Jachtenfuchs, & Obendiek, 2020; Pohle, Santaniello, & Nanni, 2025).

2.2. The Political Economy of Critical Internet Resources: The Commodification of IPv4

Studies on the allocation of Internet resources argue that early network architecture treated IP addresses as a boundless “digital commons”, managed collaboratively and distributed freely by Regional Internet Registries (RIRs) based on demonstrated technical need (Weber & Heinrich, 2011; Dulong de Rosnay & Stalder, 2020). However, as the explosive growth of the global network led to the depletion of the IPv4 protocol's address space, scholars began analyzing the institutional inertia that prevented a seamless technological transition.

While the engineering community developed the IPv6 standard to provide virtually infinite addressing space, its global adoption lagged significantly (Livadariu et al., 2017). Scholars attribute this failure not to technical flaws, but to governance limitations. Mueller, Kuerbis, and Asghari (2013) posit that the MSH model, reliant on voluntary industry consensus, lacked the centralized coercive authority necessary to mandate a costly infrastructure migration. In the absence of regulatory mandates, internet service providers and corporations opted to artificially prolong the utility of IPv4, effectively transforming a basic routing identifier into a highly coveted resource characterized by absolute scarcity (Weber & Heinrich, 2011).

This scarcity triggered a fundamental shift in the political economy of the Internet. Researchers observe the rapid emergence of an IPv4 secondary transfer market, transforming addresses from a collaboratively managed public resource into a fully tradable financial commodity (Livadariu et al., 2017). Huston (2026) documents the exponential rise in the financial value of IPv4 blocks, noting how this attracted speculative investors driven by monetization rather than network operation. Expanding on this, Mueller et al. (2013) suggest

that economic actors became willing to pay premium prices for address blocks primarily to secure robust, exclusive property rights and bypass the stringent "needs-based" assessments historically enforced by RIRs.

Crucially, literature argues that the MSH framework was structurally unprepared for this financialization. As early as 2011, Weber and Heinrich warned that assigning monetary value to a common routing resource would inevitably incentivize hoarding, allowing well-funded actors to establish monopolistic positions while pricing out smaller entities, particularly in developing regions. Ultimately, scholars observe that to prevent a total loss of visibility over network routing and the rise of untraceable "shadow markets," RIRs were cornered into amending their foundational regulations to formalize and legitimize these monetized transfers, thereby institutionalizing the commodification of the registry system (Mueller et al., 2013; Livadariu et al., 2017).

2.3. The Jurisdictional Paradox: Legal Vulnerabilities of the Multistakeholder Regime

As the financial stakes surrounding internet resources escalated, academic literature increasingly focused on the "jurisdictional paradox" at the core of the MSH regime. Mueller (2010) theorizes a fundamental tension between the borderless, transnational nature of digital networks and the strictly territorial authority of the modern nation-state. To navigate this friction, global governance mandates were delegated to private technical entities like RIRs. However, Mueller (2010) notes that these institutions could never entirely transcend physical geography; they remain legally tethered and subject to the local corporate laws of the specific countries where they are incorporated.

Kettemann (2020) provides a definitive legal analysis of this vulnerability, attributing it to the absence of a comprehensive international treaty framework for internet infrastructure. He argues that because the global system lacks a recognized, unified normative order, the governance of critical internet resources inevitably defaults to fragmented, and often ill-equipped, national legal systems. Scholars argue that this regulatory gap creates severe institutional vulnerabilities. DeNardis (2014) posits that private governance bodies, lacking international diplomatic immunity, frequently become surrogate battlegrounds for broader commercial and political conflicts.

Furthermore, literature highlights the fragility of the MSH consensus model itself. Hill (2016, 2017) argues that "bottom-up" MSH governance functions effectively only in "win-win" scenarios where stakeholders share a common operational goal. When financial interests diverge significantly, as seen in the IPv4 market, the assumption of collaborative consensus collapses, exposing the MSH model as an "industry self-regulation" mechanism lacking the enforcement capabilities of formal governmental oversight (Hill, 2016).

Private actors actively exploit this normative vacuum. Raymond and DeNardis (2015) conceptualize this practice as "forum shopping," detailing how commercial entities instrumentalize favorable local courts to bypass, challenge, or neutralize global governance policies. Literature heavily emphasizes how this legal asymmetry disproportionately impacts the Global South. Holden and Van Klyton (2016) argue that despite its theoretical emphasis on equal, multistakeholder dialogue, the MSH framework generates systemic structural barriers for African institutions. Compounding this structural disadvantage, Phokeer et al. (2021) observe that African technical actors have historically been compelled to focus their limited resources on expanding physical connectivity. This necessary focus on technical

resilience, they argue, has created a detrimental blind spot regarding legal and governance resilience, leaving African registries structurally underequipped to defend themselves against aggressive, well-funded administrative litigation and corporate *lawfare*.

2.4. Geopolitical Perspectives in the Global South: Multistakeholderism vs. Digital Sovereignty

Consequently, scholars increasingly analyze these jurisdictional and economic vulnerabilities through a critical geopolitical lens. Flonk, Jachtenfuchs, and Obendiek (2020) conceptualize the current governance landscape as a structural clash between an established “liberal sphere”, which advocates for privatized, multi-actor governance, and an emerging “sovereigntist sphere” demanding state control. Historically, the liberal sphere has dominated. DeNardis (2014) notes that the United States actively championed the privatized ICANN model specifically to prevent intergovernmental organizations, such as the ITU, from asserting authority over the Internet's logical layer.

However, critical literature increasingly deconstructs this liberal architecture. Hill (2016) critiques the ICANN-led model as a mechanism designed to preserve Western technological and economic hegemony under the guise of private self-regulation. Kwet (2019) takes this critique further, utilizing the theoretical framework of “digital colonialism” to argue that Western actors maintain asymmetrical, imperial control over the Global South by dictating the governing rules of digital architecture, thereby keeping developing nations in a state of perpetual dependency.

In response to these systemic vulnerabilities and the perceived failure of the MSH model to protect regional interests, literature notes that African states are increasingly drawn toward alternative governance paradigms. Pohle, Santaniello, and Nanni (2025) view the rising demands for “digital sovereignty” not merely as authoritarian overreach, but as a defensive political reaction against the inability of privatized technical institutions to secure critical infrastructures from foreign corporate capture. Within this context, scholars analyze the growing influence of the Chinese governance model. Shen (2018) details the deployment of Beijing’s “Digital Silk Road,” while Gravett (2020) emphasizes China’s export of the “Internet sovereignty” ideological framework, which asserts the supreme right of the sovereign state to regulate its cyberspace. For African governments feeling legally and financially powerless against private corporate interference, literature suggests this state-centric approach offers a highly appealing mechanism for reclaiming political and legal control over digital resources.

Regarding the AfriNIC institutional crisis, Mueller (2025) situates the event precisely at the intersection of these competing geopolitical models. He analyzes the intergovernmental alliance Smart Africa and its CAIGA project as a direct consequence of MSH failure, representing a coordinated attempt to introduce a council of sovereign state regulators over AfriNIC’s embattled technical community. Crucially, Mueller (2025) highlights a profound institutional paradox: ICANN signed a Memorandum of Understanding to support this governmental transition. Mueller critiques this move, arguing that by supporting an organization explicitly promoting state-led digital sovereignty, ICANN fundamentally contradicts its own bottom-up, non-state ethos in a bid for regional political legitimacy. Furthermore, he frames this as a geopolitical double standard tinged with Western paternalism, asserting that the global MSH community would never grant similar

intergovernmental oversight or state intervention if the European registry (RIPE-NCC) faced a similar legal crisis.

III - Theoretical framework

This section establishes the analytical lenses through which the AfriNIC crisis is examined. Rather than viewing the event as an isolated administrative failure, this study approaches it as a systemic breakdown resulting from the friction between private governance and public resources. By operationalizing concepts of political economy, jurisdictional theory, and power dynamics, this framework establishes the causal mechanisms necessary to test our research hypotheses.

3.1. The Political Economy of Critical Resources: Commodification

The first pillar of the framework addresses the transformation of technical identifiers into financial assets. Drawing on the work of Weber and Heinrich (2011), this study utilizes the concept of Commodification.

The core mechanism here is the shift from a “needs-based” allocation model, central to the early Internet’s “digital commons” ethos, to a market-based reality driven by absolute scarcity. When IPv4 addresses became finite, they acquired a speculative value that incentivised “capture” strategies by private actors (Mueller et al., 2013). This concept is crucial to explain why the exhaustion of resources creates a pressure that the current multistakeholder (MSH) registries were not designed to withstand.

3.2. The Jurisdictional Paradox and "Lawfare"

To analyze why a regional institution could be paralyzed by a single company, this framework relies on Mueller’s (2010) Jurisdictional Paradox. This theory highlights the tension between the borderless nature of digital networks and the strictly territorial nature of the law.

Because there is no “international law of the Internet” (Kettemann, 2020), governance defaults to fragmented national corporate laws. This creates a vacuum where “forum shopping” and Lawfare (Raymond & DeNardis, 2015) become viable strategies. Private entities can instrumentalize local courts to bypass global technical policies. This theoretical pillar directly informs whether the lack of an international legal framework is the primary structural vulnerability of regional registries.

3.3. Institutional Capacity and the Failure of Consensus

The third pillar examines the internal limits of the MSH model. Hill (2016) argues that the MSH model functions as an “industry self-regulation” mechanism that relies on Consensus.

However, this framework posits that consensus-driven governance is fragile when faced with high-stakes financial conflicts. In the Global South, where institutions often lack the “institutional thickness” or financial buffers of their Northern counterparts, this lack of coercive power becomes a fatal flaw. This concept allows us to analyze whether the MSH model is structurally incapable of resolving deep-seated conflicts when stakeholders no longer share a common “win-win” objective.

3.4. Power Asymmetry and Digital Neocolonialism

To contextualize the crisis within the Global South, the framework incorporates theories of Power Asymmetry and Digital Neocolonialism (Kwet, 2019). This lens deconstructs the MSH “equal footing” myth, arguing that Western-designed governance rules often place African institutions at a structural disadvantage.

As Holden and Van Klyton (2016) observe, institutions in developing regions often lack the legal and financial resilience to defend themselves against wealthy, transnational private litigators. This framework is used to explore how the MSH model’s design may inadvertently facilitate the exploitation of Global South registries.

3.5. Research Hypotheses

Building upon the theoretical mechanisms described above, this study proposes the following hypotheses to answer the research question of *What does the AfriNIC crisis illustrate about the challenges of regional internet governance in Africa?*:

- **Hypothesis 1 (H1):** The AfriNIC crisis highlights a structural tension within the multistakeholder model. The lack of an international legal framework leaves regional registries structurally vulnerable to IPv4 market commodification.
- **Hypothesis 2 (H2):** The crisis demonstrates that the consensus-driven multistakeholder model lacks the institutional capacity to resolve deep conflicts in the Global South.

IV - Methodology

To examine these hypotheses, this study employs a qualitative case study approach centred on the AfriNIC crisis. According to Yin (1989), a case study is an empirical investigation of a contemporary phenomenon in its real-life context, using multiple sources of evidence. In line with this definition, three methodologies are applied to address the research question. The analysis is structured around three sub-questions designed to address the research objectives. First, the study asks: what factors contributed to the AfriNIC crisis, and how does this case reveal the complex interplay between legal, institutional, and geopolitical dynamics within broader debates on multistakeholderism, Internet governance, and digital sovereignty? By unpacking these interacting factors, the paper demonstrates how the AfriNIC case illustrates the risks and limitations of multistakeholder governance models in managing critical digital infrastructure. Second, the study examines the converse dimension: how does the AfriNIC crisis also reveal the resilience of multistakeholder governance? Finally, building on these analyses, the study explores what lessons can be drawn for diplomats and policymakers seeking to protect digital commons and strengthen regional digital sovereignty.

4.1. Data Collection

For data collection, this study combines desk research, stakeholder mapping, expert interviews, and document analysis.

First, desk research and stakeholder mapping lay the foundation for the case study. Drawing on literature reviews and publicly available media sources on the AfriNIC crisis (secondary sources), the study develops an initial understanding of stakeholder dynamics and the key factors contributing to the crisis. According to Cryns et al (2025), stakeholder mapping focuses on the relationships between stakeholders and analyses the nature and influence of stakeholders on environments, organisations, and projects. Therefore, in this study, stakeholder mapping is employed to identify, categorise, and analyse the actors involved in both the AfriNIC crisis and the broader Internet governance architecture. This process informs the selection of interview participants and relevant documents for analysis. A visual representation of the stakeholder mapping is provided in Annex 1.

Building on these initial findings, semi-structured interviews are conducted to generate deeper insights into the research questions. Semi-structured interviews offer sufficient flexibility to approach different respondents while still covering the same data-collection areas (Noor, 2008). Accordingly, the interviews aim to capture contextual knowledge, interpretative perspectives, and professional assessments that cannot be obtained through desk research alone. They also serve to validate preliminary findings and deepen the analysis of the political and technical implications of the crisis. Of the 72 interview candidates contacted, a total of nine expert interviews were conducted.

Regarding the sampling strategy, the study employs a combination of purposive and snowball sampling. Campbell et al (2020) illustrate that purposive sampling is used to select respondents who are most likely to yield appropriate and useful information. Aligning with this definition, purposive sampling is used to select participants based on their expertise, as identified through stakeholder mapping and secondary source analysis. Importantly, the study includes not only direct stakeholders in the AfriNIC crisis but also broader Internet governance experts to provide more generalisable insights. In addition, snowball sampling is useful when it is difficult to access individuals with the target characteristics identified through purposive sampling (Naderifar et al, 2017). Thus, this study employs snowball sampling by asking interviewees to recommend other relevant experts. Participants were primarily contacted via email through organisational websites and professional networks such as LinkedIn. A full list of interview participants is provided in Annex 3.

In parallel with the interviews, the study conducts document analysis of key legal, policy, and institutional documents produced by relevant stakeholders. These documents are identified through both initial desk research and recommendations from interviewees. The document set includes both primary and secondary sources relevant to the case.

4.2. Data Analysis Methods

For the interviews, this research employs qualitative content analysis of the interview transcripts using a hybrid coding technique. According to Kaur et al (2025), qualitative content analysis is used to analyse textual data derived from semi-structured interviews. While deductive coding supports the application and extension of existing theories, inductive coding facilitates the identification of emerging themes and unique insights (ibid). To effectively analyse the interview transcripts, this study adopts a hybrid coding approach that integrates both deductive and inductive coding methods.

First, a deductive coding framework was developed based on the literature review, focusing on five analytical dimensions: systematic vulnerability of the MSH model, digital sovereignty, digital colonialism in privatised MSH, the commodification of IPv4 addresses, and institutional challenges and resilience (see Annex 4). The interview transcripts and relevant documents were then coded according to these categories and their associated subthemes. Through an iterative coding process, additional patterns and emerging themes were identified inductively (see the codebook in Annex 5). Furthermore, document analysis is used to support the explanation and interpretation of the arguments presented in the interviews. By combining these methodologies, this research develops a well-structured case study that provides a multidimensional understanding of the AfriNIC crisis. It also aims to generate relevant recommendations for diplomats and policymakers seeking to protect digital commons and strengthen regional digital sovereignty in Africa.

4.3. Reliability and Validity of Our Research

Through semi-structured interviews and document analysis, this research demonstrates strong internal validity by capturing in-depth perspectives from relevant actors. The AfriNIC case study further provides rich contextual insight, enabling more robust causal inferences within the specific setting. Moreover, the interpretive and context-dependent nature of this qualitative analysis, combined with the diverse academic and cultural backgrounds of the research team, contributes to the reliability of the findings. This is further strengthened through multiple rounds of coding applied to both interview transcripts and official documents, ensuring consistency and analytical rigour.

In addition, this study demonstrates a high level of credibility and transparency. Credibility is strengthened through the triangulation of multiple sources, including primary data such as interview transcripts and legal or policy documents, as well as secondary sources such as academic literature and publicly available media materials. Moreover, the research ensures transparency and enhances replicability by systematically documenting the coding process and developing a detailed codebook for the analysis of interview transcripts.

4.4. Limitations

However, several limitations remain. First, this study has low external validity because the findings cannot be generalised to other Regional Internet Registries or contexts, as it adopts a single-case approach. While the analysis of the AfriNIC crisis may reveal broader geopolitical dynamics, the lack of stakeholder perspectives from other regions constrains the generalisability of the findings.

Second, potential biases may arise during the research process. Given the dominance of Western frameworks in the literature, there is a risk of reproducing cultural and analytical biases. Our interpretations may also be influenced by personal biases shaped by our educational and cultural backgrounds. While the diversity of the research team enabled access to documents and the conduct of interviews in both French and English, language barriers may still limit access to relevant multilingual documentation on the AfriNIC crisis. Additionally, cultural and linguistic factors may have influenced the selection of interviewees. Another related limitation concerns information bias. Reports and statements issued by governments, organisations, or private entities may reflect institutional or national interests, potentially resulting in one-sided narratives. To mitigate these risks, the research team

remained critically aware of such biases throughout the research process and made efforts to incorporate diverse sources of information and a broad range of interview participants.

Finally, given the highly politicised and legally contentious nature of the AfriNIC crisis, there is a risk that certain research activities, such as interviews and document collection, may be perceived as taking a particular stance or as handling sensitive information. Furthermore, this may have affected the selection of stakeholders. This could potentially expose the researchers to legal challenges or formal complaints. To mitigate these risks, the study adopts strict anonymisation procedures, applies confidentiality agreements for interviewees, and maintains a clear and transparent academic framing of its objectives and analytical scope. Annex 5 includes the informed consent form administered prior to the interviews, along with an outline of the ethical considerations applied throughout the research process.

V - Findings

Section 1 - IPv4 Scarcity and the Governance of Number Resources

Our findings primarily demonstrate that the initial trigger of the AfriNIC crisis stems from the scarcity of IPv4 address resources, with subsequent economic incentives being driven by non-regional actors. However, they also highlight AfriNIC's limited internal incentives to transition to IPv6, given the continued dominance and global interoperability of IPv4. A deeper examination of IPv4 transfer policies further reveals the resilience and limitations of AfriNIC's regulatory framework under pressure from non-regional economic actors.

5.1.a. Scarcity of IPv4 Addresses and Corporate Greed

Our interviewees indicate that the AfriNIC crisis was triggered by the scarcity of IPv4 addresses. One expert from the technical community explains that "IPv4 becomes a valuable resource to be traded," since most of the internet still operates on IPv4, creating strong incentives for economic actors to acquire and resell these addresses on secondary markets (**INT-07**). Given that other RIRs had already exhausted their IPv4 pools, strong economic incentives persisted, making AfriNIC particularly attractive as the entity controlling the remaining IPv4 resources (**INT-04**). Interestingly, however, a digital rights advocate argues that IP resources were not perceived as valuable assets by African members, despite the scarcity of IPv4 addresses (**INT-08**). This lack of awareness and preparedness regarding the economic value of IP resources further contributed to the emergence of the AfriNIC crisis (**INT-08**).

In situations where IP addresses, supposedly treated as public goods, become commodified private resources, a global internet governance scholar argues that a fundamental flaw of the MSH model lies in the assumption that such critical addressing resources can be effectively governed by the private sector within an MSH system (**INT-02**). Indeed, an academic expert argues that the rising value of IPv4 addresses is beginning to undermine established systems of allocation and governance, with effects extending into the emergence and expansion of black market activities (**INT-01**). In this context, high-value transfers have given IPv4 addresses a market value that exceeds the fees charged by

registries, according to another expert from academia (**INT-06**). Consequently, he notes that this tension generates “a need for transfers of addresses from lower to higher value uses to respond to supply and demand in different parts of the world,” effectively turning IPv4 allocation into a global market (**INT-06**).

In the context of AfriNIC, Cloud Innovation is repeatedly identified as a key economic actor. One academic expert indicates that Cloud Innovation received a substantial number of block allocations, thereby strengthening its position, expanding its influence, and reinforcing its control over the ecosystem (**INT-01**). This actor is reported to have transferred approximately 6.2 million IPv4 addresses originating from the African continent into secondary markets, reinforcing its position as a central beneficiary of the AfriNIC crisis, arguably to the exclusion of other actors (**INT-01**). Indeed, Lu Heng, CEO of Cloud Innovation and its partner company LARUS Ltd, has publicly highlighted the significant economic potential of the IPv4 address market and advocates greater awareness and involvement in policy processes governing IPv4 assets (Blue Tech Wave 2024). He further argues that RIRs fail to adequately recognise ownership rights and instead impose artificial restrictions on market liquidity (ibid).

One expert from the tech community characterises the behaviour of certain economic actors in commodifying IPv4 addresses as “corporate greed,” whereby actors seek to exploit “an opportunity of having access to very valuable IPv4 addresses” while “engaging in a kind of lawfare” to circumvent AfriNIC’s policies governing their use (**INT-07**). Notably, LARUS Ltd is actively involved in RIR management, providing expertise in navigating the regulatory and allocation frameworks that govern IPv4 addresses, thereby positioning itself strategically within this emerging market (Blue Tech Wave, 2024).

Importantly, one expert emphasises that such resource exploitation is not limited to Cloud Innovation, but can be undertaken by any economic actor driven by similar incentives (**INT-07**). Moreover, our interviews suggest that this pattern of behaviour is not new. As early as a decade ago, another African expert from the tech community mentioned that certain actors were already seeking to exploit and influence decision-making processes within different RIRs to advance their own interests (**INT-05**). Consequently, he argues that other RIRs, such as APNIC and LACNIC, have also experienced tensions and challenges within their meetings and policy development processes (**INT-05**).

5.1.b. IPv6 Transition Failure

In the face of this AfriNIC crisis, experts suggest that the situation could have been avoided if the transition to IPv6 had been successfully implemented, given that IPv6 does not face the same scarcity constraints as IPv4. However, in reality, demand for IPv4 addresses in Africa remains persistently high despite these circumstances, and several factors continue to hinder AfriNIC’s ability to effectively facilitate the transition to IPv6.

One expert from the technical community notes that there is significant “path dependency” in network operations, whereby stakeholders continue to rely on IPv4 because it remains the globally interoperable standard (**INT-07**). He goes on to say that if AfriNIC were to operate exclusively on IPv6, it would not be fully interoperable with the entire internet, as not all networks currently support IPv6 (**INT-07**). Therefore, during the transition to IPv6, AfriNIC must operate both IPv4 and IPv6 simultaneously, a configuration known as “dual stack.” On the other hand, since maintaining a dual-stack setup is costly, many network operators opt

for the cheaper alternative of continuing to rely on IPv4, thereby creating a “chicken-and-egg problem” (INT-07). This reflects a situation in which “no one wants to move to IPv6 until everyone else does,” which, in turn, sustains the demand for and market value of IPv4 addresses (INT-07).

In the case of AfriNIC, this challenge is not new. As early as a decade ago, there was limited recognition of the strategic importance of IPv6 for the future of internet governance. One expert with an engineering background noted that, at the time, there was a prevailing belief that “AfriNIC will not need IPv6 because there’s so much IPv4 sitting unused” (INT-09). This perception contributed to a delayed transition, further entrenching reliance on IPv4 within the region.

Simultaneously, there are other strong incentives for African actors to continue relying on IPv4 addresses, as this aligns with their economic viability and existing technical capacities for internet development. One expert from the tech community explains that restricting IPv4 addresses to regional use, rather than allowing global sales, was intended to maintain lower prices by limiting demand to African entities and preventing inflation under global market exposure (INT-07). He mentions that this reflects the benefits of regionally grounded governance arrangements, where policies are adapted to local conditions to support affordable internet development in line with regional capacities (INT-07). However, the AfriNIC crisis complicates this logic, as Cloud Innovation’s diversion of addresses into black markets has inflated IPv4 prices beyond the fees charged by registries, according to the expert in academia (INT-06).

5.1.c. IPv4 Transfer Policies as a Resilient Mechanism

Although many experts emphasise the role of external economic actors and corporate greed in commodifying scarce IPv4 resources, one interviewee from an engineering background notes that he sees no issue in commodifying the IPv4 addresses “if proper protocol and agreement were done and we made them available to others for money to develop the African continent, to develop institutions in Africa” (INT-09). However, he argues that problems arise if it is being misused or misappropriated for economic gain, without any benefits being reinvested back into the African continent. This highlights the importance of AfriNIC maintaining robust IPv4 transfer policies (i.e., Number Resource Transfer Policies) to safeguard against exploitation by actors driven by corporate greed (INT-09).

Draft 3 of this policy permits IPv4 address transfers under specific conditions, including: (1) between AfriNIC members, (2) from legacy holders to AfriNIC members, and (3) between AfriNIC and other regions, provided that reciprocal intra-RIRs policies are in place (AfriNIC 2026). In the event of a breach, the entity bound by the RSA must remedy the violation and/or return the affected resources to AfriNIC, with failure allowing AfriNIC to terminate the agreement. In the case of Cloud Innovation, the alleged RSA breach became the starting point of a prolonged legal dispute (AfriNIC, 2022).

Indeed, in response to the AfriNIC crisis, the newly ratified Number Resource Transfer Policy in February 2026 is expected to serve as a mechanism to prevent malpractice by economic actors. In an AfriNIC member update published on 12 March 2026, AfriNIC outlined the benefits of the new transfer policy for the organisation and its members, including enabling controlled and transparent IPv4 redistribution by establishing a regulated framework for

legitimate transfers, reducing informal or unregistered transfers by minimising the risk of undocumented or “underground” transactions that could compromise legal certainty and registry integrity, and preserving routing stability by ensuring that transfers are properly recorded and validated (AfriNIC, 2026). However, the ratification of this policy has also triggered further litigation, including *Skyconnect v AfriNIC and Annor* on 9 March 2026 (African Dialogue on Internet Governance, 2026), thereby contributing to the ongoing governance and legal uncertainty in African internet governance.

Section 2 - Systemic vulnerability of AfriNIC

The empirical data gathered from the interviews, cross-referenced with AfriNIC’s legal and institutional documents, indicate that the crisis was not solely the result of external market pressures. Rather, it was rooted in deep internal structural flaws that pre-existed the conflict with Cloud Innovation. These systemic vulnerabilities fall into three main categories: a weak and mismatched legal framework, fragile internal governance structures, and a chronically dysfunctional Board of Directors.

5.2.a. Legal Fragility and Jurisdictional Mismatch

A major issue identified in the research is the fundamental incompatibility between AfriNIC’s continental mandate and its local legal status.

Several interviewees pointed to AfriNIC’s registration under Mauritian company law as the root of this problem. One regional internet governance expert described it as a “fundamental limitation,” noting that managing a globally connected infrastructure under a local legal framework creates an inherent structural weakness (**INT-01**). An international governance scholar reinforced this, arguing that standard commercial law is simply not designed to handle disputes over critical global public goods. When such a law is applied to these situations, it produces poorly adapted outcomes and legal dead ends (**INT-02**). A regional policy expert went further, suggesting that the choice of Mauritius as a host country was itself problematic, noting that the legal environment there offers limited accountability, and that had AfriNIC been headquartered elsewhere, the crisis might not have unfolded in the same way (**INT-04**).

A key consequence of this jurisdictional mismatch is the absence of any independent international arbitration mechanism. Another regional governance expert noted that without such a mechanism, AfriNIC was left exposed to “forum shopping,” the practice of selecting the most favorable local court to file legal challenges (**INT-01**). The Mauritius Supreme Court ruling (2022 SCJ 253) provides concrete evidence of this. The document details how Cloud Innovation filed at least nine separate injunctions after AfriNIC attempted to terminate its membership in July 2021, a tactic the court even scrutinized as a potential “abuse of process.” This relentless legal pressure eventually led to winding-up petitions and frozen bank accounts. A digital rights advocate similarly emphasized that independent dispute resolution mechanisms are essential, and that the current system relies too heavily on members themselves to set and enforce protective rules, which proved insufficient in this case (**INT-03**).

The regional policy expert also pointed to the absence of a strong continental legal framework as a structural gap (**INT-04**). Had the African Union or a regional internet governance body established well-defined legal regulations, he argued, the crisis could have

been prevented or at least contained. In its absence, AfriNIC had no supranational legal shield to fall back on.

The consequences of this legal fragility were concrete and severe. A regional tech community veteran noted that litigation by external actors essentially paralyzed AfriNIC over several years **(INT-05)**. He also highlighted that legal loopholes within the institutional framework made it theoretically possible for a hostile entity to take control of a regional internet registry, a vulnerability that was actively exploited in this case **(INT-05)**. A governance expert added a financial dimension to this: AfriNIC simply lacked the financial resilience to sustain a prolonged legal war of attrition. Once its bank accounts were frozen, the organization's ability to function was critically undermined **(INT-01)**.

5.2.b. Internal Governance Failures

Beyond the legal framework, interviewees consistently identified serious internal governance failures as a second major category of vulnerability. These failures existed within AfriNIC's foundational documents, its policy processes, and its organizational culture.

A senior technical expert with direct institutional knowledge drew a clear distinction between AfriNIC's policy development process, which he described as strong and functional, and its governance structures, which he identified as the real source of the problem **(INT-03)**. He specifically pointed to two key documents, the Resource Services Agreement (RSA) and the Bylaws, as the texts that allowed the crisis to unfold **(INT-03)**. These documents contained gaps and ambiguities that external actors were able to exploit. This insider also noted that the CEO's contract was allowed to expire without a clear transition plan, creating a governance vacuum at a critical moment **(INT-03)**.

A critical regulatory loophole was the Number Resources Transfer Policy. A review of AfriNIC's Policy Manual (Section 5.7) confirms this, reflecting the institution's struggle to clearly regulate intra- and inter-regional address transfers as IPv4 resources dried up. An academic expert in internet governance corroborated this, noting that well before Cloud Innovation became involved, there were already corrupt elements within AfriNIC **(INT-06)**. Individuals within the organization had been improperly allocating IP addresses and profiting from it. When AfriNIC attempted to recover those addresses from Cloud Innovation, it triggered the legal escalation that followed. The regional tech veteran similarly pointed to internal malpractice, noting that policies were broken and that the organization had already been compromised from within before the external crisis erupted **(INT-05)**. The senior technical expert added that the internal legal dispute actually started before Cloud Innovation escalated the matter externally **(INT-03)**. Members began filing legal cases against AfriNIC first, which weakened the organization's position and opened the door to further external intervention.

A regional policy analyst identified additional internal vulnerabilities linked to the broader African governance environment **(INT-04)**. He noted that divisions inside AfriNIC allowed external actors to exploit disagreements between members. He also pointed to corruption as a compounding factor, describing how a third party attempted to approach and corrupt member countries in order to destabilize the board and take control of the organization. In addition, the regional tech veteran pointed to linguistic and regional fragmentation as a structural feature that hindered cohesive decision-making **(INT-05)**. The divisions between

Francophone, Anglophone, and Lusophone Africa created communication barriers that affected the organization's internal coherence and its ability to respond collectively to threats.

A structural governance problem identified by several interviewees is the absence of sufficient participation in AfriNIC's internal processes. The senior technical expert noted that only five to ten members typically participate in elections, which means that decisions affecting the entire continent are made by a very small group (INT-03). This asymmetry of participation weakens the legitimacy and resilience of governance outcomes. A global internet policy expert also noted that the former board had been criticized for failing to act on warning signs early enough, and that there were questions about whether certain decisions had been approved that should not have been (INT-07).

The data also reveals a broader clash between technical realities and political ambitions. This same policy expert observed that while AfriNIC's core function is technically straightforward, managing a database, the community attempted to enforce protectionist policies to keep IPv4 addresses strictly within Africa. This regional protectionism collided directly with global market forces (INT-07).

5.2.c. Board Instability and Institutional Capture

The final vulnerability highlighted across the interviews is the structural weakness, manipulation, and paralysis of AfriNIC's Board of Directors.

The election process itself, as dictated by the AfriNIC Bylaws, was a major point of contention. A regional telecommunications pioneer described the Board's design as the organization's "biggest loophole", criticizing the fact that members are appointed on the basis of regional representations rather than professional merit (INT-05). He argued that this system severely undermined accountability and opened the door to patronage. He described an internal culture in which appointments were used to reward personal connections rather than competence. This lack of oversight occasionally resulted in the appointment of "ghost" members who never attended meetings (INT-05).

An academic scholar added another dimension to the board's fragility: electoral fraud (INT-06). He noted that Lu Heng appeared to have been bribing individuals to vote in particular ways during board elections, which represents a direct manipulation of AfriNIC's governance from the outside. This kind of interference was made possible precisely because the board election process lacked sufficient safeguards against external influence (INT-06).

The ultimate proof of this institutional collapse is the Communiqué from the AfriNIC board of Directors and the Receiver, which confirms the organization was placed under receivership because it could not even gather a quorum to govern. While there are current efforts to rebuild, evidenced by the recent publication regarding the Appointment of Nomination Committee 2026, questions about long-term resilience remain. As one academic expert questioned, it is still unclear whether a newly elected Board will possess the "very professional corporate management skills and legal protections" required to fend off future crises (INT-06). A policy analyst nuanced this slightly, arguing that in most cases the composition of the board does not significantly affect day-to-day operations, but acknowledged that in moments of conflict or political tension, board composition can become a decisive factor that creates problems where none previously existed (INT-07).

Interestingly, interview data suggest that these pressures are not exclusive to AfriNIC. Other RIRs are not exempt from these challenges (**INT-05**). As one expert from the tech community notes, their policy development processes have also experienced tensions arising from external economic actors and corporate interests over the past decade (**INT-05**). Similarly, another scholar observed that similar patterns of litigation and policy contestation have occurred across all regional internet registries worldwide (**INT-06**). Furthermore, according to an expert from the tech community, the AfriNIC episode has actively catalyzed discussions around reforming the ICP-2 framework, the foundational document governing the creation and recognition of RIRs, a process that is currently ongoing (**INT-05**).

Section 3 - Sovereignty Debate - Multistakeholderism vs Multilateralism

5.3.a. Structural critique of Multistakeholderism: Neocolonial Asymmetries

The different findings suggest that the MSH model operates within a structurally unequal global order, in which African actors face significant limitations in participation, representation, and influence.

In this regard, a regional policy expert in Internet governance highlighted a persistent gap between the Global North and South in terms of digital development and internet governance capacity (**INT-04**). According to this perspective, limited internet access across parts of the African continent directly constrains participation in governance processes, effectively excluding large segments of the population from decision-making structures. This asymmetry is not only infrastructural but also institutional, reinforcing unequal representation within global governance forums.

Furthermore, a deeper structural critique emerges from historical analyses of internet governance. One academic expert argued that the architecture of the system, including the establishment and geographical distribution of RIRs, was shaped by Western political interests and colonial legacies (**INT-02**). In this context, the role of the United States is highlighted, as it promoted and effectively imposed a privatised and largely unregulated model of internet governance on the global system, despite resistance from other states that were compelled to adopt it. Expanding on this argument, the same expert further described the selection of RIRs' headquarters, and even the existence of only five RIRs, as arbitrary and reflective of historical power dynamics, noting that they are predominantly located in English-speaking countries or former colonies (**INT-02**). This interpretation then reinforces the claim that contemporary governance asymmetries are rooted in geopolitical and historical processes rather than neutral institutional design.

Similar dynamics can be found in more recent developments. One academic expert noted that ICANN has historically pursued a strategy of “global engagement”, aimed at building relationships with international organisations and strengthening its institutional presence across governance forums (**INT-06**). Within this context, ICANN collaborated with Smart Africa, a partnership of African states and international actors such as the AU, through a Memorandum of Understanding aimed at strengthening internet governance capacity across Africa. However, an internet governance scholar questions ICANN's neutrality. ICANN

underestimated the inherently political nature of Smart Africa, whose state-led priorities may not align with the role that ICANN is expected to play in the region (INT-06). As a result, this criticism eventually pushed ICANN to retreat from the initiative (INT-06). At the same time, another expert emphasised that African stakeholders remain heavily dependent on Western institutions, including ICANN, for financial support, which in turn constrains their autonomy in international negotiations and reinforces structural power imbalances (INT-01).

Nevertheless, on the other hand, a policy expert emphasised that ICANN's decision to decentralize policy development for IP address allocation by delegating it to RIRs was originally intended to prevent excessive centralization of power (INT-07). This institutional design, implemented thirty years ago, remains relevant today. In this regard, he argues that framing AfriNIC as subject to "colonization" by ICANN would be inaccurate (INT-07). Specifically, the IANA, which is responsible for the global coordination and distribution of IP address resources, allocates large address blocks to RIRs, which in turn manage their distribution at the regional level. This governance structure was therefore designed to empower regional communities and allow them to define allocation policies based on local needs rather than being subjected to a fully centralised global system (INT-07).

Consequently, while one expert argues that AfriNIC maintains technical and operational autonomy due to the decentralised nature of global internet architecture (INT-07), other perspectives point instead to structural constraints that limit its effective independence (INT-01; INT-02; INT-06). In this prospect, another participant emphasized that the AfriNIC crisis revealed a mismatch between global governance frameworks and African realities (INT-04). From this perspective, externally developed models may not be adequate to address local needs. As a result, there is a necessity to find African solutions for African problems. Several participants therefore stress the need for African-centred governance approaches, stating that a possible solution would be for African stakeholders to be more involved in and take responsibility for the decision-making process, assuring that infrastructures and governance are built at the same time. Such an approach would enhance ownership, reduce dependency on external actors, and support the long-term resilience of internet governance systems across the continent (INT-08; INT-09).

5.3.b. The Sovereignty Awakening in African Governance Dynamics

Digital sovereignty in Africa regained importance, especially after the AfriNIC crisis. One interviewee remarks that the crisis exposed the risks associated with reliance on privatized global infrastructure lacking sufficient political backing (INT-01). This realization has prompted a broader sovereignty awakening, encouraging African states to reconsider their role in the governance of critical digital resources.

Several experts demonstrate that the crisis exposed international constraints on African digital sovereignty. A regional internet governance expert notes that the continent lacked cohesion in its response to the AfriNIC crisis, highlighting a broader absence of regional solidarity (INT-01). Furthermore, an international governance scholar reinforces this argument by emphasizing the political diversity and recurring conflicts among African governments, which complicate coordinated action and collective responses (INT-06).

Structural inequalities within the continent further contribute to this fragmentation. Uneven levels of economic and technological development result in differing priorities and capacities among states **(INT-03)**. As a result, African digital sovereignty remains inherently fragmented, reflecting both internal diversity and external pressures **(INT-03)**.

5.3.c. MSH vs. ML

In the context of constraints on African digital sovereignty during the AfriNIC crisis, the tension between multistakeholder (MSH) and multilateral (ML) governance emerged as a central theme throughout the findings.

On the one side, some experts argue that stronger state involvement is necessary to prevent the monopolization of critical internet resources and to provide political backing during crises. From this perspective, resource management should be anchored in national sovereignty and coordinated through intergovernmental mechanisms **(INT-02; INT-09)**. In line with this stance, a regional governance expert highlighted the relevance of the AU on the continent, arguing it should provide both legal and technical support to AfriNIC **(INT-09)**. This view reflects a growing interest in strengthening regional institutional frameworks to support digital sovereignty.

However, a key concern raised by multiple experts is that increased state-led involvement could disempower AfriNIC by shifting real decision-making power into the hands of governmental actors, particularly through initiatives such as Smart Africa. One academic expert argues that introducing a political overlay through initiatives such as CAIGA would undermine the effectiveness of the registry by disrupting established bottom-up processes **(INT-06)**. Global internet policy expert further emphasizes that ML governance is inherently political, as it involves negotiations between states over IP address allocation **(INT-07)**. In contrast, the MSH model distributes decision-making authority across a diverse set of actors, reducing the risk of politicisation **(INT-07)**. From this perspective, shifting toward an ML system could introduce geopolitical considerations into technical decision-making processes, potentially leading to fragmentation of the internet **(INT-07)**.

Hence, the majority of our interviewees expressed strong support for the MSH system as the preferred governance framework. Several participants argued that the strength of the MSH model lies precisely in its bottom-up and non-governmental nature, which limits direct political interference in technical decision-making processes **(INT-03; INT-07)**. An academic expert further argued that this approach is valued because its strength in Africa lies in AfriNIC's continental responsibility and agency; as a result, the integration of different policies does not need to rely on agreements between nation-states **(INT-06)**.

Despite these differences, a common ground emerges around the need for a balanced, hybrid approach. A governance expert stated that "the crisis has also balanced the conversation between technical governance and political authority" **(INT-01)**. As said by a digital rights advocate, the future of internet governance in Africa may lie in a collaborative model, where governments, technical communities, private actors, and civil society work together toward a shared objective, which is expanding access to and development of digital infrastructures across the continent **(INT-08)**. Therefore, the objective is not necessarily to

replace the MSH system, but rather to complement it with greater institutional and political support.

VI - Discussion

6.1. Legal vulnerability and Structural tension within the MSH model (H1)

The findings provide strong empirical support for Hypothesis 1. The absence of an international legal framework did leave AfriNIC structurally vulnerable - not only to IPv4 commodification but more broadly to any sustained legal pressure by well-resourced private actors.

The literature had already identified this risk theoretically. Mueller (2010) described the jurisdictional paradox at the heart of the MSH model, and Kettemann (2020) warned that the absence of an international treaty framework forces governance to default to fragmented national legal systems. The AfriNIC case confirms this empirically. AfriNIC's incorporation under Mauritian company law became a decisive structural weakness. The organization held a continental mandate but had no legal protection beyond the domestic framework of a small island state. This mismatch was not a minor administrative detail; it was a foundational design flaw that went unaddressed for years.

What our research adds to the existing literature is the role of internal failures in amplifying this legal vulnerability. H1 frames the problem primarily as an external one. Our findings suggest the picture is more complex. The legal vulnerability was exploited precisely because internal governance failures had already weakened the organization from within. Poorly drafted bylaws, a weak RSA, corrupt address allocations preceding the crisis, and the absence of independent arbitration mechanisms all created entry points for external exploitation. As a former Chairman of the Board of Directors of AfriNIC noted, the legal dispute started internally before Cloud Innovation escalated it. The structural legal vulnerability was necessary but not sufficient to produce the crisis. It was the combination of external legal exposure and internal institutional fragility that made AfriNIC unable to defend itself.

6.2 IPv4 as a Market Commodity and Private Capture (H1)

The commodification of IPv4 addresses made this vulnerability acute. As IPv4 exhaustion has progressed and addresses acquired significant market value, the conditions for consensus-based governance have deteriorated. The scarcity of IPv4 transformed what had been a collaboratively managed resource into a financially attractive target. In this regard, as Weber and Heinrich (2011) suggested, the needs-based allocation model of the IPv4 digital commons has transferred into a market-driven commodity.

Firstly, our findings demonstrate that the emergence of the IPv4 transfer market, along with the fragility of existing transfer policies, has significantly exacerbated the commodification of IPv4 addresses, driving increasing profitability as their market value rises. This supports the argument advanced by Livadariu et al. (2017), who identify the development of IPv4 transfer markets as a fundamental shift, transforming IP addresses from a previously free and widely accessible resource into a fully tradable commodity.

This increasing tendency of transforming the IPv4 resources into the market-driven commodity triggers capture strategies employed by private actors, driven by the increasing market value of IPv4 addresses. Findings show that the persistence of IPv4 is more strongly driven by AfriNIC's structural dependency on IPv4 address resources, particularly in relation to the Cloud Innovation, as well as internal malpractices within AfriNIC preceding the current AfriNIC crisis. This AfriNIC's dependency on Cloud Innovation's IPv4 resources, evidenced by the contentious transfer of approximately 6.2 million addresses, highlights the risk of monopolisation by a single economic actor. This concentration of address ownership reflects broader structural vulnerabilities within the governance framework. As Weber and Heinrich (2011) warn, certain actors may seek to hoard IP address resources in order to establish monopolistic positions or artificially inflate prices, thereby excluding less affluent participants. This concern is clearly manifested in the ongoing legal disputes and contestation over IP address ownership observed during the AfriNIC crisis.

6.3. Institutional Capacity and the Limits of Consensus (H2)

Hypothesis 2 argues that the consensus-driven MSH model lacks the institutional capacity to resolve deep conflicts in the Global South. Our findings provide nuanced support for this claim while also complicating it.

Hill (2016) argued that MSH governance functions effectively only in win-win scenarios. The AfriNIC case illustrates this clearly. Once IPv4 addresses acquired significant market value, a single actor with sufficient financial resources could bypass community-developed policies through litigation, rendering the bottom-up policy process irrelevant. No amount of community consensus could counter a strategy of sustained lawfare backed by deep pockets. The emergence of the IPv4 transfer market, combined with fragile transfer policies, significantly exacerbated this dynamic. As Livadariu et al. (2017) identify, this represents a fundamental shift in IP addresses, moving from a freely distributed resource to a fully tradable commodity, and the MSH model had no effective mechanism to manage that transition.

However, framing this purely as a failure of the MSH model risks obscuring important distinctions. An internet policy expert argued that the governance function of AfriNIC is, in most circumstances, well-adapted to its purpose, and that the crisis did not fundamentally shift the calculus in favor of a multilateral alternative. Most of the interviewees maintained that the MSH model remains the most appropriate framework, provided that internal governance structures are sufficiently robust. Mueller et al. (2013) contend that the MSH framework is structurally ill-equipped to restrain aggressive commodification, but our research suggests this limitation is not inherent to the model itself, but rather to the institutional weakness of the organizations implementing it.

In addition, legal loopholes have created incentives for market actors to intervene in IPv4 transfer policies and, more broadly, in internet governance processes. This perspective indicates that the vulnerabilities of the MSH model do not primarily stem from its reliance on voluntary participation and consensus-based decision-making. Rather, they arise from institutional dependencies, governance failures, and regulatory gaps that enable strategic manipulation by market actors.

What the AfriNIC case demonstrates more precisely is that the MSH model's capacity to resolve conflict depends heavily on the institutional strength of its component organizations. In the Global South, where institutions often lack legal protection, financial buffers, and deep technical and legal expertise, this dependency becomes a structural problem. The model assumes a level of institutional thickness that does not always exist. H2 is therefore confirmed not as a general indictment of the MSH model, but as a diagnosis of its uneven performance across different institutional contexts.

6.4. Power Asymmetry and Digital Colonialism (H2)

The vulnerability of the MSH model can be attributed not only to limitations in institutional capacity but also to entrenched power asymmetries between the Global North and the Global South within the global internet governance architecture. Kwet (2019) argues that Western-designed governance frameworks systematically position African institutions at a structural disadvantage; consequently, the MSH model, in a global context, fails to ensure equal footing for African stakeholders.

Consistent with this, our findings indicate that the pronounced dependence of African stakeholders, particularly AfriNIC, on Western, US-led institutions such as ICANN is deeply problematic. This dependency reflects not only the limited compatibility of Western governance models with African socio-political and economic realities, but also a persistent digital and technical capacity gap between the Global North and South. Moreover, reliance on ICANN for financial support risks skewing agenda-setting processes, whereby issues prioritised by ICANN stakeholders are more likely to dominate, thereby marginalising locally relevant concerns within the African context.

Nevertheless, as one expert emphasised, this dynamic should not be interpreted as evidence that the US-based ICANN dominates Africa or constitutes a form of digital colonisation (**INT-07**). African stakeholders retain ownership over the technical layer of internet governance through their role as an independent RIR, exercising authority in policy development and implementation. In this respect, the claim by Holdern and Van Klyton (2016) that the design of the MSH model may inadvertently facilitate the exploitation of Global South registries is not fully supported in this case. However, their observation that Global South RIRs often lack sufficient legal and financial resilience remains valid.

Furthermore, the pressures exerted on AfriNIC must be analyzed not as an isolated regional failure, but as a symptom of a structural shift in global internet governance. As Weber and Heinrich (2011) and Livadariu et al. (2017) demonstrate, the global exhaustion of IPv4 addresses has transformed these routing resources, initially conceived as a collaboratively managed digital commons, into highly lucrative and tradable financial assets. This commodification has introduced aggressive market dynamics into the RIR system. However, as Raymond and DeNardis (2015) analyze, the MSH model was structurally designed for technical coordination, not to regulate high-stakes economic conflicts involving private actors. Consequently, AfriNIC's vulnerabilities reflect a systemic friction between consensus-based governance and the financialization of infrastructures.

Crucially, our interview data confirms that this friction is not confined to Africa; it represents a universal vulnerability across the RIR system. A regional telecommunications pioneer explicitly noted that actors driven by personal gain have been attempting to "manipulate the

processes within different RIRs" (INT-05). Furthermore, an international governance scholar stressed that the specific corporate pressure exerted by Cloud Innovation is "not only an Afrinic problem, but a problem of all registries" (INT-06). He warned that if such an actor "managed to break Afrinic, it will go and break the other registries" (INT-06). These insights demonstrate that the aggressive patterns of corporate capture seen in Mauritius are symptomatic of a global threat to the entire MSH framework.

It is in light of these empirical data that the collapse of AfriNIC can be accurately reevaluated. The critical divergence between the administrative collapse of AfriNIC and the survival of Western registries (such as ARIN or RIPE NCC) is explained by their differing institutional capacities. As Kettemann (2020) explains, in the absence of a strong supranational legal framework, internet governance depends on national legal systems. Western RIRs benefit from protective legal environments and deep financial reserves. Conversely, Holden and Van Klyton (2016) emphasize that African internet governance institutions often operate with severe capacity constraints. AfriNIC therefore found itself forced to defend a global digital commons against a global market threat, relying solely on the vulnerable commercial law of a small island state.

Finally, this dynamic illustrates the power asymmetry inherent in the current technological architecture. As Kwet (2019) argues, the global digital system structurally disadvantages the Global South by exposing it to the disproportionate power of massively resourced multinational corporations. Therefore, our findings demonstrate that presenting the AfriNIC crisis as a simple "failure of African governance" is empirically inaccurate. Rather, the crisis exposes a systemic flaw in the global MSH model: it exports consensus-based rules without providing Global South institutions with the equitable structural and legal shields necessary to withstand these corporate assaults.

Taken together, these findings suggest a more nuanced conclusion for H2. Rather than attributing the crisis solely to a lack of institutional capacity, the evidence indicates that while formal governance authority is retained by African stakeholders, structural constraints, including asymmetries in capacity and resources embedded within the broader governance architecture, limit their ability to effectively manage and resolve complex conflicts. Therefore, H2 is partially confirmed, as the consensus-driven MSH model's conflict-resolution capacity is contingent upon uneven institutional conditions shaped by power asymmetries within the global governance architecture.

VII - Conclusion

This research set out to answer one central question: *What does the AfriNIC crisis illustrate about the challenges of regional internet governance in Africa?* Drawing on nine expert interviews, a wide body of academic literature, and the analysis of key legal and institutional documents, this study has shown that the crisis was neither accidental nor simply the product of one bad actor. It was the outcome of layered and interconnected structural failures that had been accumulating for years before they became visible. Critically, it would be a misreading of this evidence to frame the AfriNIC crisis as an "African crisis." The

vulnerabilities it exposed are systemic features of the global multistakeholder (MSH) model, not regional pathologies. The AfriNIC case is therefore best understood as an early stress test of governance structures that are globally distributed but unevenly protected.

The findings confirm both hypotheses, though with important nuances. Regarding H1, AfriNIC's incorporation under Mauritian company law, combined with the absence of any independent arbitration mechanism, left it exposed to sustained “lawfare” by a well-resourced private actor. Yet the crisis was not solely an external one. Internal failures, including poorly drafted bylaws, corrupt address allocations, board instability, and low member participation, pre-existed the conflict with Cloud Innovation. Regarding H2, the bottom-up consensus model proved insufficient once IPv4 addresses had acquired significant financial value and a single actor could afford to litigate indefinitely. However, this should not be read as a wholesale indictment of the MSH model, which the majority of interviewees maintained remains the most appropriate governance framework for internet resources. What the AfriNIC crisis reveals is that the model's effectiveness is contingent on institutional strength, a condition that cannot be taken for granted where legal protections are thin, financial buffers are limited, and power asymmetries with better-resourced external actors are pronounced.

This study's single-case design necessarily limits its generalisability, and a comparative analysis of the five Regional Internet Registries would be a valuable next step. Further research into the evolving IPv4 transfer market would also be timely, particularly in light of AfriNIC's newly ratified Number Resource Transfer Policy (February 2026) and the litigation it has already triggered. Finally, the potential role of the African Union in providing a supranational legal and political framework for regional internet governance deserves deeper scholarly attention.

For practitioners and policymakers, the AfriNIC crisis carries lessons that extend well beyond the repair of one organisation. A detailed set of recommendations is provided in Annex 2. Ultimately, the AfriNIC crisis is a reminder that the multistakeholder model is not self-sustaining. It requires institutions strong enough to withstand pressures it was never designed to anticipate, and a global community willing to ensure that the burden of that resilience does not fall unevenly on those least equipped to bear it.

VIII - References

7.1. Primary sources

African Dialogue on Internet Governance. (2026). *Skyconnect, Cloud Innovation, and the long proxy war against Africa's internet registry.*
<https://www.afrodig.org/skyconnect-cloud-innovation-and-the-long-proxy-war-against-africas-internet-registry/>

AfriNIC. (2024). *Bylaws of the African Network Information Centre.*

- AfriNIC. (2022).** *Court update: Cloud Innovation Ltd vs AFRINIC (SCR 5C/30/21).* <https://afrinic.net/20220215-court-update-cloud-innovation-ltd-vs-afrinic-scr-5c-30-21>.
- AfriNIC. (2026).** *AFRINIC member update: Organisational stability and ongoing legal challenges.* AFRINIC.
- AfriNIC. (2020).** *IPv6 programme.* <https://afrinic.net/ipv6-programme>
- AfriNIC. (2018).** *Resource Services Agreement (RSA).*
- AfriNIC. (2020).** *Policy Manual (Section 5.7).*
- AfriNIC. (2026).** *Number Resource Transfer Policy.* Ratified February 2026.
- AfriNIC. (2026).** *AFRINIC Member Update: Organisational Stability and Ongoing Legal Challenges.* Published March 12, 2026.
- AfriNIC Board of Directors & Receiver. (n.d.).** *Communiqué.*
- African Telecommunications Union & African Network Information Centre (ATU & AfriNIC). (2021).** *African Telecommunications Union and AFRINIC collaborate to enhance efficient and secure internet connectivity in Africa.*
- Supreme Court of Mauritius. (2022).** *Cloud Innovation Ltd v. African Network Information Centre (AfriNIC) Ltd.* 2022 SCJ 253.
- Supreme Court of Mauritius. (2026).** *Skyconnect v. AfriNIC and Annor.* Filed March 9, 2026.

7.2. Secondary sources

- Blue Tech Wave. (2024).** *IPv4 market: A \$60T opportunity hiding in plain sight, says LARUS CEO.* Access from: <https://btw.media/en/ipv4-market-a-60t-opportunity-hiding-in-plain-sight-says-larus-ceo>.
- Campbell, S., Greenwood, M., Prior, S., Shearer, T., Walkem, K., Young, S., Bywaters, D., & Walker, K. (2020).** *Purposive sampling: Complex or simple? Research case examples.* *Journal of Research in Nursing*, 25(8), 652–661.
- Cryns, M., van Hassel, E., & Vanelislander, T. (2025).** *Stakeholder identification and mapping in peripheral European inland waterway ecosystems.* *Journal of Shipping and Trade*, 10, 11.
- DeNardis, L. (2014).** *The Global War for Internet Governance.* Yale University Press.
- Dulong de Rosnay, M., & Stalder, F. (2020).** *Digital commons.* *Internet Policy Review*, 9(4).
- Flonk, D., Jachtenfuchs, M., & Obendiek, A. S. (2020).** *Authority conflicts in Internet governance: The liberal sphere and its challengers.* *Review of International Studies*, 46(3), 364-386.

- Gravett, W. (2020).** Digital neo-colonialism: The Chinese model of internet sovereignty in Africa. *African Human Rights Law Journal*, 20(2), 411-440.
- Hill, R. (2016).** *Internet Governance: The Last Gasp of Colonialism, or Imperialism by Other Means?* Inosphere.
- Holden, J., & Van Klyton, A. (2016).** Exploring the tension and asymmetries in Multistakeholder Internet Governance. *Journal of Information Policy*, 6, 140-168.
- Huston, G. (2026).** IP addresses through 2025. *APNIC Blog*.
- Kaur, K., Abu-Qamar, M. Z., Rashidi, A., McKay, N., & Saunders, R. (2025).** *Applying hybrid coding and reflexivity in qualitative content analysis: An exemplar.* *Global Qualitative Nursing Research*, 12.
- Kettemann, M. C. (2020).** *The Normative Order of the Internet: A Theory of Rule and Regulation Online.* Oxford University Press.
- Kwet, M. (2019).** Digital colonialism: US empire and the new imperialism in the Global South. *Race & Class*, 60(4), 3-26.
- Livadariu, V., Elmokashfi, A., & Dhamdhere, A. (2017).** On IPv4 transfer markets: Analyzing the secondary IPv4 market. *ACM SIGCOMM Computer Communication Review*, 47(3), 19-27.
- Mueller, M. (2010).** *Networks and States: The Global Politics of Internet Governance.* MIT Press.
- Mueller, M., Kuerbis, B., & Asghari, H. (2013).** Dimensioning the elephant: An empirical analysis of the IPv4 number market. *Info*, 15(6), 44-56.
- Mueller, M. (2025).** *ICANN fosters some not-so-smart ideas for AFRINIC.* Internet Governance Project.
- Naderifar, M., Goli, H., & Ghaljaei, F. (2017).** *Snowball sampling: A purposeful method of sampling in qualitative research.* *Strides in Development of Medical Education*, 14(3).
- Noor, K. B. M. (2008).** Case study: A strategic research methodology. *American Journal of Applied Sciences*, 5(11), 1602–1604.
- Phokeer, A., Chege, K., Chavula, J., Elmokashfi, A., & Gueye, A. (2021).** *Measuring Internet Resilience in Africa (MIRA).* AFRINIC & Internet Society.
- Pohle, J., Santaniello, M., & Nanni. (2025).** *Unthinking Digital Sovereignty: A Critical Reflection on Origins, Objectives, and Practices.* *Policy & Internet*, 16: 666-671.
- Raymond, M., & DeNardis, L. (2015).** Multistakeholderism: anatomy of an inchoate global institution. *International Theory*, 7(3), 572-616.
- Shen, H. (2018).** Building a Digital Silk Road? Situating the Internet in China's Belt and Road Initiative. *International Journal of Communication*, 12, 19.
- Yin, R. (1989).** *Case study research.* Sage Publications.

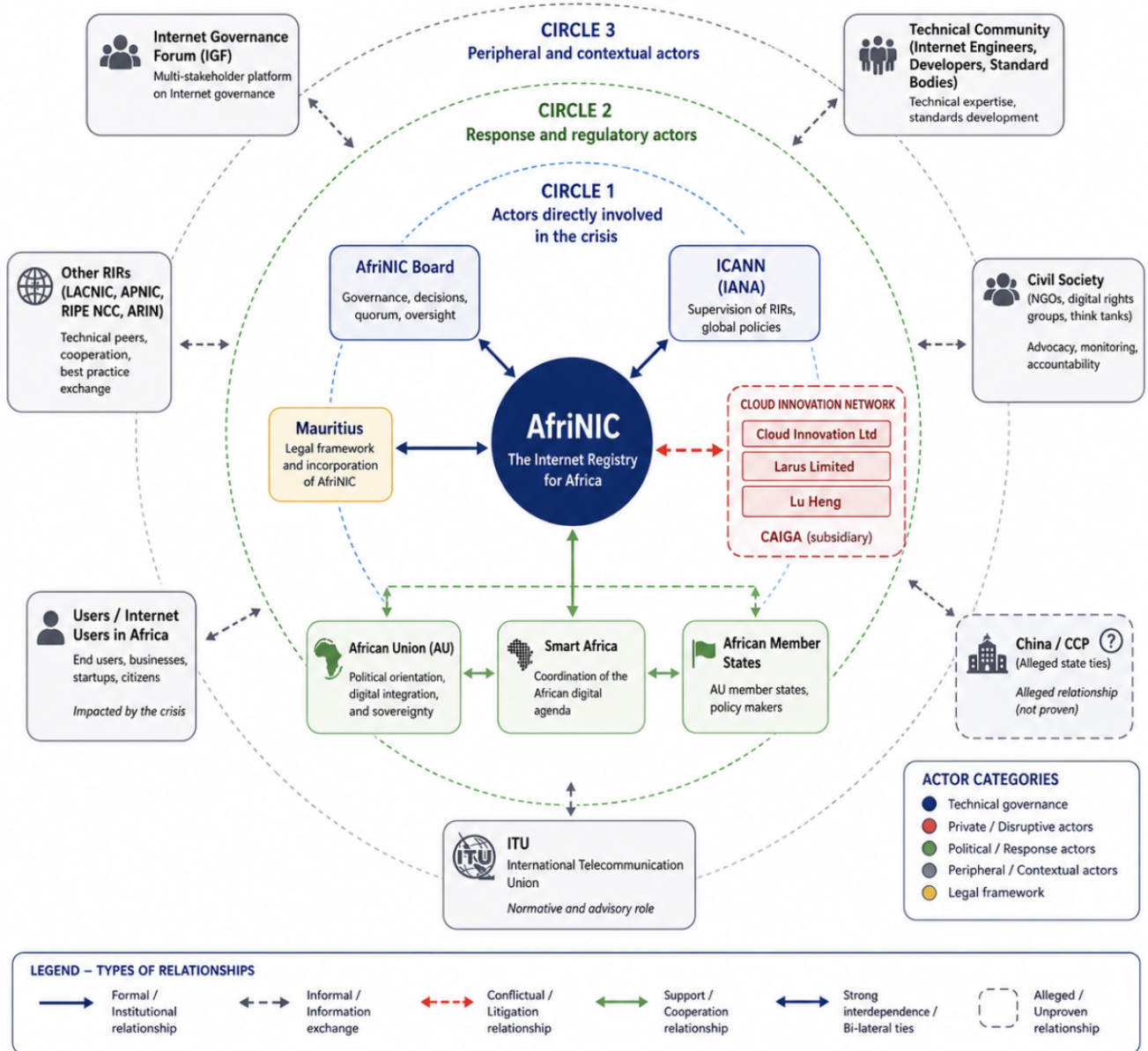
Weber, R. H., & Heinrich, U. N. (2011). IPv4 address exhaustion and the new Internet protocol (IPv6). *Computer Law & Security Review*, 27(4), 400-408.

IX - Annexes

Annex 1: Visual Stakeholder Mapping

STAKEHOLDER MAPPING – THE AFRINIC CRISIS

Mapping actors, relationships and dynamics



Annex 2: Recommendations

Drawing on the interviews and our analysis, this paper proposes a set of recommendations that reflect the multifaceted nature of the crisis, encompassing economic, legal, governance, and MSH model dynamics.

To address corporate greed arising from IPv4 scarcity, several interviewees emphasise the need to strengthen IPv4 transfer policies, particularly concerning out-of-region transfers of number resources. One expert argues that the AfriNIC crisis partly originated from the absence of “a coherent, defensible policy regarding people from other regions getting addresses and using them outside **(INT-06)**.” In response, another expert stresses that revisions to the bylaws and the Resource Services Agreement (RSA) are necessary to address these governance gaps **(INT-03)**.

One expert further emphasises the importance of accelerating the IPv6 transition in the face of the depletion of IPv4 resources and to support the growth of the African digital economy **(INT-09)**. This is echoed in a 2021 MoU between the African Telecommunications Union and AfriNIC, which highlights stronger IPv6 strategies as rising device use and IoT growth increase demand, while IPv4 exhaustion limits connectivity (ATU & AfriNIC 2021). In addition, another expert advocates for greater state involvement in technical design, arguing that if states had managed the internet from the outset, they could have enforced stricter security standards and required the new internet protocol (IPv6) to be backwards-compatible with IPv4, potentially mitigating the current address shortage **(INT-02)**.

As our findings show, the AfriNIC crisis was not solely the result of external market pressures from economic actors, but was also rooted in an internal institutional fragility. In particular, AfriNIC’s registration under Mauritian company law reflects a weak legal framework that constitutes a fundamental limitation. In response, several experts argue for relocating AfriNIC’s headquarters outside Mauritius to avoid reliance on local commercial laws that are ill-suited to governing a global public resource **(INT-04; INT-09; INT-01)**. One expert further suggests moving its legal base under the African Union, rather than maintaining its current structure as a Mauritius-based private company **(INT-04)**.

Moreover, addressing internal governance failures, particularly board instability and risks of institutional capture, is critical to enhancing the organisation’s transparency and accountability. Several experts advocate for strengthening internal oversight mechanisms to mitigate corruption and prevent the monopolisation of IP address resources by internal actors **(INT-05; INT-06; INT-04)**. Concurrently, reinforcing external oversight is equally important. In this regard, the establishment of an independent international arbitration mechanism has been proposed as a means to prevent corporate actors from exploiting domestic legal systems to paralyse AfriNIC’s operations **(INT-01)**. Finally, improving internal governance structures and leadership capacity within AfriNIC is essential for ensuring long-term institutional stability and effectiveness **(INT-01; INT-06)**.

As outlined in the discussion, this paper argues that the MSH model remains the most suitable governance framework, although it reveals institutional weaknesses when confronted with the increasing commodification of number resources. To address these limitations, one expert suggests that political backing from a multilateral organisation, specifically the African Union, is necessary to provide formal support to AfriNIC, while refraining from encroaching on its core technical and operational functions **(INT-01)**. In this regard, another expert emphasises that promoting a balanced and collaborative approach among diverse stakeholders is essential to preventing the politicisation of technical governance **(INT-08)**.

Finally, although the AfriNIC crisis is regionally contained, it requires both African ownership and external support. Greater engagement from African policymakers is essential, alongside openness to collaboration. In this context, coordination with other RIRs remains particularly valuable (**INT-02**).

Annex 3: Interviewee IDs

Interview ID	Professional Background / Anonymized Expertise	Date of Interview
[INT-01]	Regional Internet Governance Expert & Digital Rights Advocate	March/April 2026
[INT-02]	Global Internet Governance Scholar & Academic	March/April 2026
[INT-03]	Senior Technical Insider & Regional Tech Veteran	March/April 2026
[INT-04]	Regional Policy Expert	March/April 2026
[INT-05]	Regional Telecommunications Pioneer & Tech Community Veteran	March/April 2026
[INT-06]	International Governance Scholar & Academic Expert	March/April 2026

[INT-07]	Global Internet Policy Expert & Policy Analyst	March/April 2026
[INT-08]	Digital Rights Advocate	March/April 2026
[INT-09]	Academic Expert & Regional Governance Expert	March 2026

Annex 4: Deductive Coding Framework (Precoding)

Themes/Codes	Subcodes (example)	Explanation of the codes
Systematic vulnerability of the MSH model in the African context	Political/ governance level fragility - Unequal representation/ asymmetry of participation, - Sidelined the local realities - Lack of governance resilience - technical resilience/lack of technical resilience - Lack of coercive mechanisms through voluntary participation and consensus	Explaining the structural contradiction between the West and the Global South.
	Legal fragility / jurisdictional vulnerability of the MSH model - Lack of international legal immunity	Explaining how legal fragility leads the internet community to drag itself into commercial conflict. Explaining the incompatibility between the borderless nature of networks and the territorial

		jurisdictional authority of the nation-state.
Digital sovereignty (African context)	State-led digital Sovereignty - Governance vacuum - Chinese model of internet sovereignty / digital neocolonialism - Multilateral governance model (e.g., ITU/ SmartAfrica)	Explaining how the African community form their digital sovereignty with internal and external influences.
Digital colonialism in privatised MSH	- Western predominance/ technology hegemony (towards the Global South), i.e., ICANN - Industry self-regulation - ECONOMIC EXTRACTIVISM> also related to market-driven digital neocolo) - Institutional paradox of ICANN	Explaining the unequal dynamics imposed by the liberal ICANN model and economic extractivism.
	Politicisation of Technical Governance - Institutional paradox of ICANN (MoU for SmartAfrica, although it should be a bottom-up institution) - Western Paternalism	Explaining the increase in intertwining between tech governance and political governance.
The commodification/financialisation of IPv4 addresses	- IPv4 scarcity / increased financial value of IPv4 - The rise of IPv4 transfer markets/ emerging private economic actors	Explaining the commodified scarce IPv4 address resources under the multistakeholder internet governance.
Institutional Challenges and Resilience	Institutional Collapse of RIR - Inability to adopt their policies - Emergence of	Explaining Afrinic or other RIRs' institutional vulnerability and how they maintain their resilience amid crisis.

	shadow markets - Legal challenges Institutional resilience of RIR - Revision of policies	
--	--	--

Annex 5: Codebook

Relevant Themes	INT number	Code Name	Description	Examples of Coding
Internal and historical structural flaws/ Legal Fragility	INT-05	Regional Board Structure Weakness	The governance structure of AfriNIC was designed around regional representation rather than merit, which weakened institutional effectiveness and accountability.	"Board members have to be appointed on the basis of region, not on the basis of merit... This regional thing is Afrinic's biggest loophole.
	INT-05	Patronage and Informal Power Networks	Informal networks and patronage practices influenced appointments and decision-making within AfriNIC, undermining transparent governance.	"This structure has also been manipulated... Let me give my friends positions so that I can control them."
	INT-03	Afrinic internal structure failure	the crisis started because of a structural flaw within Afrinic, not within the MSH model	"the problem AfriNIC faces. It's mainly from the from the from the from the RSA resource service agreements and the by law. Those are the two key documents that need to be addressed."
	INT-05	Weak Board Oversight	Weak institutional oversight and a lack of active participation within the board allowed governance failures to emerge over time.	"A lady was appointed to the board... and she never attended a single meeting. A ghost was appointed to the board."
	INT-05	Institutional Fragmentation	Linguistic and regional divisions within Africa	"You had Francophone Africa, Anglophone Africa, Lusophone Africa, North

			influenced institutional design and decision-making, contributing to structural governance weaknesses.	Africa... the language barrier became the key dividing factor."
	INT-05	Internal Mismanagement and Malpractice	Internal governance failures, including fraud and poor oversight, contributed to the crisis.	"Policies were broken, malpractice happened... we ended up in a situation where Africa was compromised."
	INT-04	Internal division within AfriNIC	Internal disagreements and divisions within the organisation created opportunities for external actors to intervene.	"There were divisions inside AfriNIC and this allowed a third party to divide the members."
	INT-03	Afrinic internal governance failure	Afrinic's problem is on the governance side, the policy side is strong and functional	"the policy side is very, very strong. There is no problem on the police side. The problem we had is mainly like on the go, on the governance side" ... "You let you leave the CEO contract to end; it gets a vacuum"
	INT-09	governance failure	aside from AfriNIC's governance failure, even the continent has difficulties managing the governance, compared to the other continents	"like the rest of the continent Europe, not they have more formalized institutions, and these issues don't usually come up, but you have Africans with all the institutional problems. Governance level through the this continental level "
	INT-06	Voting fraud	when the interviewee talks about the voting fraud for the election for the AfriNIC Board	"Now, maybe if he had done some fraudulent things regarding the elections—he seems to have been bribing people to vote a certain way for the board election—that might be a cause for ending his membership.

				But it would have to be based on a direct violation of the rules within AfriNIC's governing documents, not just "we don't like you, we want to get rid of you."
	INT-03	Afrinic internal dispute	the legal dispute started internally, before the externalisation of the case by Cloud Innovation	"the members start opening legal, legal cases against AfriNIC. I think that's where the problem started. "
	INT-08	Lack of independent dispute resolution	International immunity would be efficient, but the system, in order to work, also needs more participation from the members	"Legalization or jurisdiction can be, uh, supportive to better address what afrinic is facing. But the core issues are, is how members. Okay. Set rules to protect, uh, to reinforce the, uh, the the, the, the, the, the registry to better address the needs of the members".
	INT-07	Vigilance in enforcing policies/ lack of enforcement	To what extent the Afrinic is vigilant in enforcing the policies matters as the previous Board member in AfriNIC conducted the internal malpractice	"to what extent the board of those organizations are vigilant in enforcing the policies that the communities have created. And I think that has been some critique in the AfriNIC case that, I mean, I don't know all of the ins and out, but I know that there was some critique of the former board that wasn't acting on this earlier, or might have approved something that they shouldn't have approved."

	INT-07	Not a board issue	most of the time, who becomes the board does not matter for this issue.	"And in I would probably argue that in 99% of the cases, it might not matter who's on the board. It might not matter at all if it's someone from the government or if it's someone from the community, but that 1% of the time, there might be a geopolitical consideration by that board, and that will happen if it is coming from, let's say if you have a representative from Nigeria, and suddenly there's a conflict between Nigeria and Kenya. And then suddenly, oh, Nigeria has a representative on this entity that has a say in who gets to have access to IP addresses or not. Suddenly, you created a problem that wasn't there to begin with. So I think it's it's creating more problems than solving them, to have these sort of multilateral institutions involved, and that what really needs to happen is more of a I think what we're seeing in AfriNIC is sort of lessons by the community itself in terms of how it's organizing."
	INT-04	Corruption vulnerabilities	Governance environments affected by corruption increased institutional fragility.	"In Africa beyond legislation there is also the problem of corruption, and this allowed a third party to divide the members."

	INT-06	IPv4 Fraud before the AfriNIC crisis 2021	Internal malpractice in organising the addresses was happening even before the 2020s Afrinic crisis.	"As far as AfriNIC was concerned, well before Cloud Innovation, there were corrupt elements within AfriNIC who were giving addresses to people and making money off of it. They tried to clean that up, and then I think they overstepped when they tried to get the addresses back that they had given out to Cloud Innovation. That would have destroyed Cloud Innovation's business, so that's when he initiated this legal war."
	INT-06	Fragility of the new Board	Fragility in terms of legal and financial resources. Solving this fragility is needed to fight against the external actors.	"But I also think they might not have the legal and financial resources to adequately fight against somebody like Lu Heng. They need to have some very professional corporate management skills and legal protections. I just don't know how well this new board is going to function. It's too new."
	INT-04	Third-party infiltration	An external actor attempted to manipulate AfriNIC's governance structures in order to take control.	"A third party tried to approach member countries, trying to corrupt them and destabilize the AfriNIC board."
	INT-04	Institutional fragility	Weak institutional safeguards made the organisation vulnerable to governance manipulation.	"They tried to destabilize the AfriNIC team board in order to take control."
	INT-01	Local Legal Vulnerability	AfriNIC's reliance on local Mauritian law created a structural vulnerability for a continental	"Managing a globally connected infrastructure under a local company law is a fundamental limitation... yet it depends on the national laws of

			infrastructure.	that association."
	INT-01	Ineffective Dispute Mechanisms	The absence of independent arbitration mechanisms leads to forum shopping and the exploitation of local courts.	"One core vulnerability we observed in this crisis is the lack of independent dispute resolution mechanisms... This leaves the door open to domestic disputes and creates opportunities for forum shopping and legal fragmentation."
	INT-02	Unsuitable Jurisdictional Framework	Using standard private/commercial law to regulate critical global internet resources creates endless legal vulnerability.	"By refusing to acknowledge that this is a public good requiring specific rules, inappropriate laws are used... we end up in a system where we try to apply ordinary laws to disputes, but ordinary laws apply poorly."
	INT-01	Financial Fragility of RIRs	The regional registry lacked the financial resources to defend itself against well-funded private litigation.	"Cloud Innovation actually seized the bank accounts and appointed receivers. How can you survive that with very limited financial resilience? Those limitations invite evolution."
Economic pressure and IPv4 scarcity	INT-02	Technical Failure (IPv6)	The technical community (IETF) failed to make IPv6 backwards compatible, which directly created the artificial scarcity of IPv4.	"The entire slowness of the transition to IPv6 comes from the fact that you have to build a new network from scratch. It was obvious foolishness; they should have made it backward compatible... They were the 'Internet cowboys'."
	INT-05	Resource capture incentive	Economic incentives linked to digital resources motivated attempts to control AfriNIC.	"The third party entered the system mainly to take control of the IPv4 resources available."
	INT-02	Speculative Value of IP Blocks	IPv4 blocks became highly valuable financial assets, especially in regions with	"Now, it is clear that there is a strong financial interest in acquiring IPv4, especially in a continent (Africa) where there are

			historical scarcity like Africa.	relatively few due to historical colonial exploitation. In Africa, it becomes very interesting to grab a nice block and sell it later."
	INT-08	IP addresses are not assets	Even though IPv4 addresses are scarce, they did not become an asset	"IPv6, IPv4, IPv6 numbers are not considered as an asset for, uh, Afrinic members that has been issued, uh, IPv4 according to, uh, the registration services agreement that has been signed between, uh, uh, Afrinic members and afrinic. "
	INT-09	IP addresses should be sold if it's a benefit	IP addresses should be sold, and the revenues should be used for the continent's benefit. Then, if needed by Africa's populations, they should return to the continent. This process should be regulated by detailed policies.	"when the numbers were sitting down, not being used, others needed them. If proper protocol and agreement was done and we made them available to others for money to develop African continent, to develop institutions in Africa, I don't see anything wrong with it, because all these years that we're not using it, the number was sitting down if others were using it appropriately, in a legal way, and paying something for it, I did not see anything wrong with it at all".
	INT-06	Profitability of IPv4 // Commodification	IPv4 is profitable and tradable	"Scarcity of IPv4 addresses, but there's also kind of a dependency on IPv4 addresses, because the majority of internet kind of operates in IPv4 so that means that IP four addresses got a real they became very valuable, and they became effectively a resource that was being traded. So it became very attractive of getting hold of an IPv4 address and then

				selling it to someone, because it was a high demand for IPv4 addresses."
	INT-05	Strategic Manipulation of Governance Processes	Actors attempted to influence policy development processes in RIRs for financial gain linked to IP resources.	"Some really nasty people have been trying to manipulate the processes within different RIRs for their own personal gain."
	INT-04	Strategic value of IPv4	Remaining IPv4 resources controlled by AfriNIC created strong incentives for actors to capture them.	"The main point of the crisis was IPv4... they wanted to take control of the IPv4 addresses AfriNIC still has."
	INT-04	Late IPv4 exhaustion in Africa	AfriNIC remained attractive because it still controlled IPv4 resources while other RIRs had already exhausted theirs	"Other RIRs did not have this problem because they already exhausted their IPv4 resources."
	INT-02	Public Good vs. Commodification	Treating critical addressing resources as private commodities rather than public goods is a fundamental flaw of the MSH model.	"Therefore, it is a fundamental mistake to think that critical addressing resources can be managed by the private sector in a multistakeholder system... As soon as there is scarcity, yes, it becomes problematic."
	INT-07	Threat of External Economic Actors	When the interviewee explains about the economic actors who have the corporate greed to make a profit out of the IPv4 resources	"Where the African region saw, okay, the African region needs IPv4 addresses for the growth of the internet here. But then you had a player that came and they developed policies to that end, to try to safeguard that. And then a player came in and, you know, took advantage of the fact that, okay, they could get a hold of IPv4 addresses and then sell them in other regions to a

				high price."
	INT-07	Protection of Economic Viability on the Internet Governance for Afrinic	Preserving the market price of IPv4 is important for Afrinic to sustain the price and distributions	"And one of the reasons why the African community had these policies around IPv4 addresses being used in Africa and not being sold to the rest of the world, had to do with that also lowers the price of those right, like, because the demand is basically just African entities in that case, right? If you open it up globally, the prices will go up. So it was one of the ways of, sort of keeping the prices of IP for addresses low. And that speaks a little bit to the benefits of these governance arrangements where a given region given the needs of that region, in this case, a region that is effectively all developing countries, could ensure that they could have a sort of economic viability for their internet development that corresponded to their abilities, if you will, right? So they weren't subjected to these global market prices, but they could keep IPv4 addresses, sort of within reason, price wise, by having these limitations. "
	INT-07	Path Dependency for IP Address Management	Chicken and egg issues for the difficulty in transitioning into the IPv6. Because the African region is highly reliant on IPv4 assets, if there's no push to transition to IPv6, they will still be	"So that means that the IPv4 is kind of, there's a big chunk of path dependency here where people stick with IPv4, because the transition to IPv6 is quite expensive, as long as the Critical Mass is still on IP for it, it's kind of like this. Yeah, not a virtuous vicious cycle, but

			reliant on IPv4. This prolongs the issue of the lawfare.	close to, like, there's a bit of a chicken and egg problem, I guess, right? Like no one wants to go to IPv6 until everyone else is on IPv6. "
	INT-07	non-profitability of IPv6 addresses	Since there is no scarcity, it does not work like IPv4, which has a lot of values; therefore, the Afrinic Crisis would not happen	"IPv6 addresses are basically there's no cost of an IPv6 address because there's no scarcity."
	INT-07	Costly IPv6 / cost of the network operator/matter of technical realities	, there resistance of the transition drawn from the technical reality rather than the threat from external economic actors. A dual-stack situation with IPv4 and IPv6, or the complete transition, can generate expenses for operation. Therefore, IPv6 transition in general is not realistic	"If you're only running IPv6, you're not going to be interoperable with every part of the internet, because not everyone is running IPv six. So their alternative is to run what's known as a dual stack, where you have your network is both IPv4 and IPv6. That's very costly to implement."
	INT-07	resource exploitation/ market-driven governance / economic exploitation by the private sectors	what happens in AfriNIC crisis is in a way the resource exploitation.	"in what maybe might be the traditional version, where you have a European or American company that is sort of exploiting the African region. In this case, it's a Chinese company that is doing it. But I think it's colonial in the sense that you have a external actor taking advantage of of the situation and sort of exploiting the resources. In this case, the IP addresses are designed to be a resource for the African continent, and clearly you have a foreign actor here exploiting those resources for their private benefits. So it's colonial in

				that sense."
	INT-07	non-chinese issue	AfriNIC crisis is not only the issues generated by the Chinese economic actors.	"And in this case, one of those companies a Chinese it happened to be a Chinese company, but I could have seen this being done by an American company or a European company"
	INT-07	IPv4 policy matters/function of the policies matters	The importance of IPv4 policy to handle the issues of AfriNIC crisis.	"So the reason why this become an exploitation issue is because the policies here said that there was restrictions to it, but then those were overridden. So to the extent you would see exploitation in other regions, it would first requires that there are some restrictions on the sell of those IPv4 addresses globally."
	INT-07	IPv4 second-hand market	when the interviewee talks about the IP addresses second-hand market	, the second hand market is quite elaborate, and how it works in Europe. And that market, I think, is quite free in Europe, where you're basically, you're selling your IP before address someone buys it, and you just let ripe know, oh, they've now changed ownership.
	INT-07	IPv6 abundance	IPv6 is abundant, therefore it does not have much of the economic value compared to IPv4.	"So IPv6, there's no scarcity really like there's no real conflicts of who should get what, because everyone can get it. You know, there's no tragedy of the commons type of situation. So if you just think about them as like with a different technology, because the engineers would describe IPv four as a different technology in IPv6. So with a different technology, these governance arrangements

				wouldn't come about and the conflicts that we see wouldn't come about purely if you had a different technology, IPv6 and sort of abundance of it."
	INT-07	Who sets what IP policies matters;	the process of defining the IP policies and which clause to be included matters.	"Yes, it's not just "political versus operational", because even if IP addressing is somewhat political, the question is: what are the procedures and who are the stakeholders making the decision? If it is the members of AfriNIC, it's very well defined who has power and why decisions are made. The stakeholders have a very clear relationship to the outcome; they are accountable for the outcome. Whereas with the overlay of governments in Smart Africa, there's a disconnect between the actual stakeholder organizations using IP addresses and the governments. The governments are not really directly affected by how resources are allocated. It's more of a political game."
	INT-07	Breach of the policy (RSA) as a threat/ related to the external actors	The biggest issues are the ability to use numbers from Afrinic in different regions	"Of course, one of the biggest issues that started the whole fight was the ability of Cloud Innovation to use numbers they got from AfriNIC in different regions."
	INT-08	IPv4 resources should be governed by the Community	The distribution of IP addresses should be managed internally by the community, and a strong structure	"the IPv4 brokerage that we are observing in the region, uh, simply because, uh, we don't have policies that allow, uh, this kind of, uh, uh,

			needs to be put in place.	trading of IPv4, uh, within Afrinic service region". "IP resources should be governed by the communities. "
	INT-06	Issue of the Number resource transfer policy	Number resource transfer policies and how to organise the IPv4 transfer matters, especially for the out-of-region transfers of numbers.	"I would say they need to come up with a good resolution for the address transfer policy, particularly the question of out-of-region transfers of numbers. I think the source of the problem really is that they didn't have a coherent, defensible policy regarding people from other regions getting addresses and using them outside."
	INT-07	Comparison with the other RIRs	Comparison with the other RIRs in terms of IP economic exploitation and the policies.	"So the reason why this become an exploitation issue is because the policies here said that there was restrictions to it, but then those were overridden. So to the extent you would see exploitation in other regions, it would first requires that there are some restrictions on the sell of those IPv four addresses globally."
Sovereignty debate MSHvML	INT-02	Multilateral / State-centric Coordination	To avoid private monopolies, resource management should be rooted in national sovereignty and coordinated through intergovernmental bodies.	"To me, it is completely obvious: it must be managed first at the national level, and then at the international level. If you don't like the ITU, create another ITU!"
	INT-09	AU is the main actor	AU should be the main actor, both for the legal and technical aspects. AfriNIC must be	"the foundation should have been formed by an African Union, or AU, and then it will sit with the legal if you like" "AU must have

			backed by the AU.	oversight responsibility of the legal and technical support "
INT-03	MSH is the ideal model	The bottom-up process needs to be maintained, limiting the prevalence of other stakeholders	"The multi stakeholder model has proven to be the most stable model for the internet's growth." "smart Africa, or any African governments, including African Union, or any others, there has to be. There has to help Afrinic as a stakeholder, not to make Afrinic as a subset " "work hand to hand, hand in hand with, uh, our bottom up process, our community consensus approach." "if CAIGA has, uh, aligned okay with, uh, what government, uh, organization can say that is okay."	
INT-07	MSH, as the designated internet model	The structure is mundane, and no need for the multilateral	"But when they're working on the standards, there's obviously going to be commercial interests involved in all of those things, but it's also in the context of being a community working towards something. "	
INT-06	African solidarity under the MSH	Integration of the African continent is completed through the AfriNIC, and there is no need for the Multilateral organisation to intervene	"But AfriNIC applies to the entire African continent. That's an example of why you don't want nation-states in charge; you want this non-profit contractual organization which applies to the whole continent. So you can get integration without having to go through nation-state agreements. Your jurisdiction is in fact the entirety of Africa. Any service provider or organization using IP addresses can join AfriNIC, and by that	

				means, the policy-making process within AfriNIC is in fact integrated across the whole continent."
INT-08	Collaborative approach	All members and stakeholders should participate and be involved, regardless of their status, to reach a common goal: internet accessibility		"When we meet with the government, uh, uh, motivating them, involving them in what afrinic is doing so that they can understand, uh, our ecosystem and how together, uh, we can facilitate adoption and the development of digital services in Africa. " "the internet is a common goal. Uh, we require, okay, uh, involvement of all the different parties, even if the youth, okay, men, women, etc., etc"
INT-01	State Intervention as Protective Mechanism	The crisis highlighted the need for political backing and coordinated regional voices (Smart Africa) to defend technical infrastructure, not to capture it.		"Smart Africa is bringing a blueprint to unify African voices when it comes to internet governance... throwing the trophy saying that African governments want to capture AfriNIC is not true."
INT-02	Private Monopoly Risks	Leaving critical infrastructure to the private sector without state regulation naturally leads to resource capture by the wealthiest actors.		"Leaving everything to the private sector when it comes to critical networks can be very dangerous... The equivalent on the Internet would be leaving the coordination of frequencies entirely to the operators. Obviously, what would happen? The richest would take everything."
INT-03	Asymmetry of participation	Not all the members participate equally in the decision-making process.		"the development, the speed is not at the same, the same rate, which, which, which means maybe the problem, the problem, the problems in ISP, is facing in South

				Africa, and then the probably is facing in Congo or in in in Sierra Leone are different. " ... "only five to 10 members contribute to participate in the election".
INT-01	Lack of Regional Solidarity	The crisis exposed the inability of the continent to defend its digital sovereignty cohesively.		"If one single RIR is fighting, you have silence, there is no solidarity. Africa cannot effectively exercise digital sovereignty at the level of individual states..."
INT-08	African responsibility	African stakeholders must take responsibility, be involved in the process of making the Internet accessible for all, and be prepared to solve any problem.		"I think that the continent must start building infrastructures and governance at the same time. Okay. That is very important. And this means exactly, uh, including a budget. A budget for legal prospection"
INT-01	Sovereignty Awakening	The crisis forced African states to realise the risks of relying on privatised global infrastructure without political backing.		"In Africa, it created a regional awakening. A regional awakening on digital sovereignty. It has made very visible the risk of relying on global infrastructure in a regionally fragile institution without official political backing..."
INT-06	African digital sovereignty	Fragmented digital sovereignty in Africa and the importance of acknowledging them		"Furthermore, regarding the idea of sovereignty: Africa is not a single state. There are 54 states in Africa. It would be nice if Africa were able to cooperate as a unified continent, but we're a long way away from that, unfortunately. We have a lot of conflicts among governments, a lot of diversity, and many of the governments are not democratic. Some of the policymakers in those governments would not be

				directly informed about the implications of different policy decisions regarding IP addresses."
	INT-07	non-geopolitical consideration	African Crisis is not the geopolitical concern as it is related to the technical governance layer.	"The model that we have today, the competing model that the other geopolitical spectra wants to have this to be about. They want to have this multilateral governance structure. The problem with that is that a multilateral governance structure is inherently political, right? Like you create a multilateral governance structure in order to manage politics between countries. You're making the issue to be a geopolitical issue if you have it as a multilateral governance structure, whereas when you have it as a private governance structure, the politics you cannot escape it. But it's not inherent to the system"
Neocolonialism	INT-07	No digital neocolonialism by ICANN	The policies and distribution of IP addresses are not decided by the greed of ICANN, but it is more African-centred	"but some 30 years ago, they decided, actually, it's much better if the access to these IP addresses, the policies for who gets to have what IP address, is developed by the local community or the regional community. So it's not a central, global, you know entity that decides how the African region should you know, offer access to IP addresses, or how the Latin American region should you know offer access to IP addresses. But they purposefully said, Okay, we're going to have these regional Internet registries that are going to

				be facilitating the users of the IP addresses. So the network operators, the network operators within a given region, that is the community of that region. So the AfriNIC is a African community of IP address users, if you will, right? And the whole system is based that those regional communities should set the policies within the regions for how those IP addresses are allocated."
	INT-06	ICANN override to AfriNIC	ICANN MoU with SmartAfrica override their responsibility on the continent and contributes to politicising the technical governance.	"I think in general, as a long-term pattern, ICANN is "running interference". This means they are trying to establish connections and essentially promote their organization among many different international organizations (like the ITU, the UN agencies, the IGF). They call it "global engagement", and they have a whole department for it. Essentially, it's just what we call "schmoozing"—getting to know people, getting in their good graces, maybe giving them money, so they won't be hostile to ICANN."
	INT-04	Global North-South digital gap	Structural technological inequalities shape the way internet governance operates globally.	"Between the West and the Global South we have a big gap in digital evolution and internet governance."
	INT-04	Connectivity inequality and limited internet access across African populations affects participation in governance	Limited internet access across African populations affects participation in governance discussions.	"Many people in Africa are still not connected, so you cannot talk to them about internet governance."

		discussions.		
	INT-07	African Ownership in Internet Governance	The idea that the internet / IP addresses operation has to be regionally managed	"Now, what Africa, the organization provides is really a very boring function. Like, what they do is just manage database that keeps track who got what IP address. That's that's their core function, offering this registry function, right? And the other piece is that they basically facilitate the policy making processes of the African community. So they, you know, they have staff that then organize these events and these processes where the network operators in the African region can come together and say, actually, when it comes to, let's say for, for example, when it comes to networks operated for nonprofit, they should have priority for getting IP addresses allocated. I'm not sure if that is a rule, but that would be an example of a rule, right? Okay, so the community would come together, develop those type of policies, and then after nick the organization would use them when they're allocating the IP addresses,"
	INT-04	Need for African governance strategies	African internet governance frameworks should be developed based on local needs and realities.	"African organizations should build their own strategy for internet governance according to African realities."
	INT-09	Involvement of Africans stakeholders	Africans must be the first to be interested in AfriNIC's future. Mauritius should not be the main	" need to look at establishing an entity, African regional registry, entity that is more African in nature than now." "Going forward, anything

			country; there should be equal participation between the different parties	that has to do with African continent, all the policy makers of the countries involved must be interested"
INT-04	Western governance model mismatch		Governance frameworks designed in Western contexts do not always reflect African realities.	"We cannot just take models from Western countries because our realities in Africa are different."
INT-02	US Unilateral Imposition		The United States imposed the privatised, unregulated internet model on the rest of the world against the will of other nations.	"The Clinton administration's decision was to take the Internet out of the US regulatory framework... But the problem is that they imposed this on everyone else. They very explicitly prevented the ITU and countries from taking up the matter."
INT-01	Power & Resource Asymmetry		African stakeholders depend heavily on Western institutions (like ICANN) for funding, limiting their independence in global forums.	"Africa in the global arena... currently, the continent faces an asymmetry of power, expertise, and legal influence. I tell you that to be able to go to Kigali, you have to go and take money from ICANN, over-relying on them for financial resources."
INT-02	Western Hegemony & Arbitrary Design		The architecture of internet governance and RIR locations was dictated by Western political interests and colonial legacies.	"What happened were political struggles. You will notice that it is no coincidence that the countries chosen to host the registries are all in the English-speaking zone or are former colonies. Why Mauritius rather than South Africa?"
INT-08	Interference of external actors		the members of the different RIRs should be the ones to define rules and be in charge of the governance of	"it is the responsibility, the responsibility of the members and the community of these RIRs to define the rules. And procedures that promote

			these RIRs	stability and strengthen the resilience of the registries".
	INT-03	A universal problem of all RIRs	It is not just an African problem; this crisis affected Afrinic, but it could affect all the other RIRs	"Cloud Innovation it's not only an Afrinic problem, but a problem of all registries. Which means that if it managed to break Afrinic it will go and break the other registries."
	INT-07	The role of RIRs as a capacity builder	The role of RIRs is to build capacity for the community.	"like you're still a role for the RIRs, even if you're only running IPv6. And the role for the RIRs are typically around capacity building, educations and those type of things. But these sort of, and it would probably still be policies for around the use of IPv six addresses, but these sort of more contentious issues wouldn't really be there if you were running IPv6".

Annex 6: Informed Consent and Ethical Consideration

1. Informed Consent form

<u>Interview Informed Consent Form</u> Research project title: “AfrinIC: Digital Sovereignty in Africa” Research Partner: Antoine Barbry (Organisation internationale de la Francophonie (OIF)) Academic Supervisors: Dr Jérôme Duberry Research Participants' names: Célia Barhoumi, Laurane Yara, Louise Alima Bodian, Yoko Tanaka
--

Dear [participant's name],

Thank you for accepting to participate in our study under the Master's programme of the Geneva Graduate Institute. This applied research project (ARP) is partnered with the International Organisation of the Francophonie (OIF). This study involves no financial contribution and is conducted independently.

What do you need to do?: You will be asked to complete a short interview that should take approximately 30-45 minutes.

What are the aims and possible benefits of the research?: This project aims to develop a well-structured case study that provides a multidimensional understanding of the AfriNIC crisis and examines how challenges in regional multistakeholder internet governance can impact digital ecosystems and raise tensions around digital sovereignty.

Voluntary Participation: Participation in this interview is entirely voluntary and does not include any form of compensation. Participants are free to decline to answer any question, pause at any time, or stop the interview altogether, without giving any reason. There are absolutely no negative consequences for choosing not to continue.

Usage of the Information and collected data:

- The transcript of the interview will be analysed by our researchers for this project.
- Participants can request a copy of their interview transcript and may make edits they deem necessary to ensure the effectiveness of any confidentiality agreement.
- The privacy and data of each participant will be treated confidentially.
- Any variation of the conditions above will only occur with your further explicit approval.

How will the research be published or shared?:

The findings of this research may be presented or published in a variety of media or forums, including academic papers, policy papers or our institute and/or partner's website. We will inform you when our research-related publications are issued.

For more information:

If you would like more information about this project or if you have any issues related to the project, please contact us via arp2025.afrinic@graduateinstitute.ch.

Consent

I,, consent to participate in the above research project. I understand that my involvement is voluntary and my responses will be confidential.

Ticking the 'Yes' box below indicates that, having read the information provided, you give your consent.

☐ Yes
☐ No

Ticking the 'Yes' box below indicates that, by allowing your interviews to be recorded, you give your consent.

☐ Yes
☐ No

*Any information shared will be used solely for the purposes of this research project. We will not disclose any identity unless the participant explicitly gives us permission to do so. Participants may also choose to speak off the record at any moment.
*The recordings will be deleted upon completion of this research.

Do you agree to have your name appear in the research outcome?

☐ Yes, I agree to have my name appear.
☐ No, I don't agree to have my name appear.

Participant signature: _____

Date: _____

Researcher signature: _____

Date: _____

2. Ethical Consideration

Given the highly politicized and legally contentious nature of the AfriNIC crisis, this research was conducted in strict adherence to academic ethical standards to protect all participants and researchers. The following ethical principles were applied throughout the data collection and analysis phases:

- **Informed Consent and Voluntary Participation:** Prior to all interviews, participants were provided with a detailed consent form explaining the research aims. Participation was entirely voluntary and involved no financial compensation.

Participants were explicitly informed of their right to decline any questions, pause the recording, or withdraw from the interview at any time without any negative consequences.

- **Confidentiality and Strict Anonymization:** Because the subject matter could potentially expose individuals to legal challenges or formal complaints, strict anonymization procedures were adopted. All private data is treated confidentially. Participant names and direct identifiers were removed and replaced with alphanumeric codes (e.g., INT-01) and generalized professional backgrounds. The research team committed to never disclosing a participant's identity unless explicit permission was granted by the individual.
- **Data Protection and Storage:** Any information shared by the participants was used solely for the analytical purposes of this specific research project. Audio recordings of the interviews were managed securely and will be permanently deleted upon the completion of the research.
- **Mitigation of Legal and Reputational Risks:** To safeguard both the interviewees and the research team against the sensitive nature of the corporate and legal disputes discussed, the study maintains a clear, transparent, and strictly neutral academic framing of its objectives and analytical scope

Annex 7: Acronyms

- **AfriNIC:** African Network Information Centre
- **AU:** African Union
- **IANA:** Internet Assigned Numbers Authority
- **ICANN:** Internet Corporation for Assigned Names and Numbers
- **IETF:** Internet Engineering Task Force
- **IP:** Internet Protocol
- **IPv4:** Internet Protocol version 4
- **IPv6:** Internet Protocol version 6
- **ITU:** International Telecommunication Union
- **MoU:** Memorandum of Understanding
- **ML:** Multilateralism
- **MSH:** Multistakeholderism
- **OIF:** Organisation internationale de la Francophonie
- **RIR(s):** Regional Internet Registry
- **RSA:** Registration Service Agreement