OFFICIAL PROCEEDINGS

Meeting of Nigerian Regulators on Information Integrity in the Context of the Upcoming Elections

DATES	VENUE
12–13 May, 2026	Four Points by Sheraton, Lagos, Nigeria

CONFERENCE OVERVIEW

This document constitutes the official proceedings of and recommendations from the two-day meeting convened to address the growing challenges of information integrity in Nigeria's electoral landscape. The meeting brought together senior regulators, policy stakeholders, and technical experts to deliberate on coordinated frameworks for combating misinformation, disinformation, and electoral interference.

Discussions spanned regulatory policy, cross-agency coordination, digital platform accountability, and capacity-building strategies to safeguard the integrity of public information ahead of the upcoming elections.

Key Thematic Areas Covered

I Regulatory frameworks for countering electoral misinformation	II Cross-agency coordination mechanisms and data sharing protocols
III Digital platform accountability and content moderation standards	IV Capacity building and public awareness on information integrity
V Legal and enforcement mechanisms for information offences	VI International best practices and comparative regulatory models

REPORT COMPILED BY

Rosemary Alor & Ayomide Eweje

Contents

Executive Summary

The Nigeria Regulators Meeting on Information Integrity in the Context of Upcoming Elections took place in Lagos on May 12-13, 2026, bringing together government officials, regulatory bodies, civil society, and international partners, including UNESCO, GIZ, and NDI. The purpose of the dialogue was to gain familiarity with the Guide for Regulators to Implement the Information Integrity Model Policy Framework in West Africa and the Sahel, and adapt it to Nigeria's legal, social, and digital landscape, with particular attention to the 2027 electoral cycle. The initiative positioned Nigeria as the first West African nation to apply the guide at a national level; with over 150 million internet users and upcoming high-stakes elections, the country is poised to prioritize the Guide's focus on safeguarding democratic processes, public trust, and human rights against misinformation, disinformation, and hate speech.

Like the Guide, the discussions in Lagos were grounded in the Praia Policy Framework for Information Integrity in West Africa and the Sahel, adopted in Cabo Verde in 2025, which emphasizes an ecosystemic view of information as a public good, and the Abidjan Voluntary Protocol (2024). The framework advocates moving away from punitive measures toward resilience-based governance and is structured around four regulatory pillars: transparency, proportionality, human rights compliance, and platform accountability; and five ecosystem pillars, including public access to information, media and information literacy, platform engagement, and multi-stakeholder collaboration. These principles were operationalized through voluntary tools, such as model codes of practice, standard operating procedures for high-risk scenarios, and inter-regulatory coordination frameworks.

A major recurring theme of the discussions was the growing impact on election narratives of the content circulating on and approaches used by digital platforms, including AI-generated content, algorithmic manipulation, online harassment, hate speech, voter suppression, and foreign influence. Participants noted that the speed and virality of disinformation continue to outpace institutional responses, especially where there are technical gaps, weak monitoring systems, limited expertise, and delayed reactions from both regulators and platforms. There were also strong concerns about public trust. Discussions highlighted how misinformation and disinformation can weaken confidence in elections, discourage participation, deepen insecurity, and further marginalize groups such as women and persons with disabilities. Participants agreed that protecting information integrity is directly linked to protecting democratic stability, human rights, freedom of expression, and public trust.

A core element of the dialogue was mapping Nigeria's distributed regulatory landscape, highlighting the roles of INEC, NBC, NITDA, NDPC, NCC, ONSA, Federal Ministry of Justice, Police Cybercrime Units, NHRC, and ARCON. The mapping identified three critical overlap zones requiring coordinated action and clarity: platform governance, data access versus privacy, and elections and crisis response. Participants emphasized the importance of joint protocols, rapid-response teams, and pre-designated lead agencies to reduce operational friction and ensure swift, unified responses during high-risk periods, particularly elections.

Participating institutions presented their existing detailed roadmaps for operational readiness. INEC committed to proactive information integrity management, structured platform engagement, and transparency in the Electoral Result Management System (IReV). NBC focused on co-regulation, real-time monitoring, and local content promotion. NITDA established an Election Monitoring Situation Room and direct escalation channels with tech platforms, while NHRC deployed automated complaint-handling systems and civic monitoring initiatives. ARCON shifted election monitoring toward regulating political advertising, and law enforcement agencies emphasized cyber threat attribution and judicial support.

The dialogue also highlighted structural challenges, including overlapping mandates, limited technical capacity, global platform opacity and latency, inadequate moderation in local languages,

and systemic polarization within the creator economy. To address these, the dialogue recommended a unified National Coordination Council (NCC) model, scenario-specific lead protocols, standardized rapid-response teams, strategic platform engagement, strict human rights adherence, regional collective bargaining through ECOWAS and the African Union, and nationwide media and information literacy (MIL) campaigns.

Participants emphasized that incorporating fact-checkers, independent journalists, researchers, and civil society groups into regulatory frameworks is critical to achieving real-time detection and containment of misinformation. They can support regulators by monitoring harmful narratives, providing evidence, supporting public education, tracking implementation, and acting as watchdogs throughout electoral processes.

Regional cooperation emerged as another key outcome. Speakers from ECOWAS, UNESCO, Article 19, and regulatory bodies emphasized that African countries would achieve better results by engaging digital platforms collectively instead of acting alone. Discussions also explored the importance of standardizing regulatory practices across the region, strengthening expertise, improving data governance, and building stronger relationships with platforms through continental and regional structures.

Overall, the workshop provided a comprehensive blueprint for establishing coordinated, rights-respecting, and proactive governance of Nigeria's digital information ecosystem, ensuring electoral integrity, public trust, and resilience against emerging digital threats ahead of the 2027 elections.

The dialogue was organised by NDI, GIZ, UNESCO, ECOWAS, Media Rights Agenda, and Techsocietal, with financial support from the Government of Canada, the EU, and Germany (through BMZ).

Key Recommendations

Some of the key recommendations from the sessions are as follows:

i. Consistent with the Praia Policy Framework for Information Integrity in West Africa and the Sahel, efforts to combat harmful information practices in Nigeria should adopt rights-based, multi-stakeholder approaches, in accordance with international human rights standards, and should involve stakeholder groups like civil society organisations, fact-checking organizations, independent media, and academic and research institutions, among others.

ii. Combating disinformation, misinformation, hate speech and other harmful content in the digital sphere cannot rely only on restrictive regulation but should also involve transparency, institutional accountability, media, information and digital literacy programmes; independent research; inter-agency coordination rather than isolated responses, platform engagement, and regional coordination.

iii. Regulators should ensure that the measures they are taking to address the harmful effects of disinformation serve legitimate aims, are necessary and proportionate, to avoid undermining information integrity themselves and eroding public trust. They should accordingly ensure that responses to disinformation follow due processes of law, are justified, evidence-based, guided by a risk assessment framework, and constitute the least restrictive means available.

iv. In the Nigerian context where no single agency has regulatory authority, and responsibilities relating to platform governance are distributed across multiple institutions, including media regulators, the data protection authority, INEC, the telecommunications regulator, cybersecurity institutions, and the access to information oversight body, a mandate mapping of regulatory bodies in the information ecosystem is an important tool to avoid duplication of efforts, reduce institutional friction, identify gaps, streamline platform engagement, strengthen election and crisis preparedness, and effectively protect human rights.

v. During periods of high vulnerability, such as elections, armed conflict, public health emergencies, and political crises, effective coordination among these actors is even more essential to ensure coherent engagement with digital platforms, rapid response mechanisms, transparency, and respect for human rights.

vi. Furthermore, effective response to information integrity challenges during elections also requires preparedness, clearly defined thresholds for regulatory action, crisis communication, development of early warning systems, and standard operating procedures, proactive engagement with platforms ahead of elections, and a multifaceted approach that includes regulation, public communication, platform accountability, and systemic preparedness. Plans for these should be put in place well ahead of any such situation arising.

vii. In this regard, the Office for Strategic Preparedness and Resilience (OSPRE) may also be engaged in advance to enhance the coordination of early warning and response mechanisms in relation to information integrity on digital platforms.

viii. To enhance coordination, there is a need for structured mechanisms such as established codes of practice, cooperation frameworks among regulators, and escalation matrices to ensure consistent messaging. In addition, although all institutions share responsibility for protecting citizen rights, accountability must nonetheless be clearly assigned within a coordinated system.

ix. In the context of misinformation and disinformation during election periods, multiple engagement approaches with platforms should be considered in a coordinated manner,

including requesting takedown or quarantine of harmful content, adding community notes or labels to potentially harmful electoral content, and ensuring official electoral information is widely distributed through official channels.

x. Additional measures to be considered include strengthening collaboration with independent media, influencers, other government agencies, and fact-checkers, as well as leveraging experiences from other countries and regional bodies to improve electoral preparedness and regulate misinformation.

xi. Effective responses also require training for the regulators, enabling platform features such as misinformation flags, structured election guidelines, observatories, and pre-planned communication strategies, which should be accompanied by coordinated, multi-stakeholder engagement and proactive planning rather than isolated institutional action. Platform moderation mechanisms should also be sensitive to content produced in local languages.

xii. Regulators should also strive to ensure that public office is not used to spread false or manipulated information and that government officials are upholding the highest standards of transparency, accuracy, and responsibility, particularly during crises, elections, and conflicts, and that actions by State actors that incite discrimination, hostility, or violence are addressed in accordance with international human rights law.

xiii. Other actors that can play important roles should also be engaged on the issue, including the Judiciary; the National Assembly, which can oversight regulatory bodies; the National Orientation Agency, which can carry out public enlightenment campaigns, including on media and information literacy; the Nigerian Press Council, which regulates newspapers; and digital platforms owners, such as blogging sites, to educate them on the dangers of misinformation and disinformation.

xiv. Furthermore, content creators and producers should also be engaged to deter them from focusing only on income-generation and to help them understand the dangers of misinformation and disinformation.

xv. There were calls for real-time monitoring systems, rapid response teams, and joint election monitoring situation rooms to track misinformation, hate speech, cyber threats, and harmful narratives before, during, and after elections. Participants also recommended clear standard operating procedures for responding to online harms and crisis situations.

xvi. Capacity building was repeatedly identified as a priority. Participants recommended regular training for regulators, journalists, fact-checkers, and other stakeholders on emerging technologies, AI tools, digital investigations, platform governance, data analysis, and election-related disinformation.

xvii. Participants recommended proactive public communication by institutions such as INEC and other regulators to provide accurate and timely information throughout the electoral cycle. Media and information literacy campaigns were also encouraged, with emphasis on regional contexts, local languages, women, young people, and persons with disabilities.

xviii. On the regional level, participants encouraged ECOWAS, ACRAN, UNESCO, and other regional bodies to continue developing coordinated approaches for platform governance, data protection, election monitoring, and engagement with digital platforms. They also encouraged the development of regional observatories and stronger collaboration with the African Union.

I. Introduction

In the contemporary digital era, information integrity has emerged as a fundamental pillar of national security, democratic stability, and public trust. As Africa's largest democracy, Nigeria anchors the region's most influential digital arena, hosting over 150 million internet users. While this massive digital expansion has significantly expanded civic spaces and democratic participation, it has simultaneously introduced profound systemic risks. Coordinated disinformation campaigns, polarizing hate speech, and the rapid rise of technologically engineered threats such as artificial intelligence (AI) and deepfakes now present sophisticated challenges to the fabric of public discourse.

To proactively address these challenges ahead of the 2027 electoral cycle, the Nigeria Regulators Meeting on Information Integrity in the Context of Upcoming Elections was convened in Lagos, Nigeria, on May 12-13, 2026.

II. Meeting Objectives

- Nigerian regulators gain familiarity with the Guide for Regulators to Implement the Information Integrity Model Policy Framework in West Africa and the Sahel and its relevance to Nigeria's digital governance landscape.
- Nigerian regulators review key recommendations made during the Praia Conference on Information Integrity and subsequent regional consultations held in Pretoria, with a view to contextualising them for national implementation.
- Nigerian regulators identify priority risks to information integrity within Nigeria's digital ecosystem, particularly in relation to elections, vulnerable populations, and crisis contexts.
- Nigerian regulators and relevant stakeholders agree on practical, context-specific mechanisms for the implementation of selected elements of the Guide within existing institutional mandates.
- Relevant Nigerian regulatory institutions strengthen inter-agency coordination and collaboration in matters relating to digital platform governance and information integrity.
- Nigerian stakeholders reflect on their position as regional leaders promoting a harmonized and human rights-focused approach to platform governance and information integrity.

III. Context of the Meeting

UNESCO, in collaboration with regional partners, developed a Guide for Regulators to Implement the Information Integrity Model Policy Framework in West Africa and the Sahel following extensive consultations across the region. The document aligns with the UNESCO Guidelines for the Governance of Digital Platforms and responds to a number of international instruments, as outlined in the Guide's introduction.

The draft Guide was prepared ahead of the September 2025 Praia Conference on Information Integrity and aimed to provide regulators with practical guidance on implementing the Policy Framework adopted by participating governments. Following the Praia Conference, further technical consultations were held with regulatory institutions and civil society stakeholders across the region, including during the February 2026 meeting of West African regulators in Pretoria, South Africa, convened ahead of UNESCO's Internet for Trust event.

While the Pretoria consultations enabled valuable regional input into the draft Guide, and Nigerian representatives contributed at a network level to the guide's review, Nigerian regulatory institutions were unable to participate in the Pretoria event. Given Nigeria's significant digital footprint and its

central role in shaping the region's information ecosystem, it was essential that Nigerian regulators analyse the Guide in light of Nigeria's legal, institutional, and socio-political context.

Nigeria's existing legislative and policy framework relevant to digital governance, including provisions relating to data protection, cybersecurity, broadcasting, telecommunications, and electoral integrity, provides an important foundation for the implementation of the Model Policy Framework. However, institutional mandates remain distributed across multiple agencies, underscoring the need for strengthened coordination and operational clarity in addressing risks to information integrity on digital platforms.

This meeting therefore provided a dedicated national forum for Nigerian regulators to engage with the draft Guide and recommendations emerging from Praia and Pretoria, with a view to identifying priority implementation pathways within Nigeria's regulatory environment. Particular emphasis was placed on preparedness for high-risk periods, including electoral processes and crisis situations, as well as on safeguards for vulnerable groups and mechanisms for transparency and data access.

IV. Participants

The following institutions with mandates relevant to digital platform governance and information integrity were invited to attend the event. Those with asterisks were unable to attend.

Nigerian regulatory institutions

- Advertising Regulatory Council of Nigeria (ARCON)
- Federal Competition & Consumer Protection Commission (FCCPC)*
- Federal Ministry of Communications, Innovation and Digital Economy*
- Federal Ministry of Information and National Orientation
- Federal Ministry of Justice
- Independent National Electoral Commission (INEC)
- National Broadcasting Commission (NBC)
- National Human Rights Commission (NHRC)
- National Information Technology Development Agency (NITDA)
- Nigeria Data Protection Commission (NDPC)*
- Nigerian Communications Commission (NCC)*
- Nigerian Police Force Cybercrime Unit
- Office of the National Security Adviser (ONSA)*

Legislative committees

- House of Representatives Committee on Freedom of Information*

- House of Representatives Committee on ICT
- House of Representatives Special Committee on Media and Public Affairs*
- Senate Committee on ICT and Cybersecurity*

Civil society and media experts

- Accountability Lab
- Article 19
- Centre for Journalism Innovation and Development (CJID)
- Digi Africa Lab
- FactsMatterNG
- International Foundation for Electoral Systems (IFES)*
- International Press Centre (IPC)
- Media Rights Agenda (MRA)
- Media and Information Literacy and Intercultural Dialogue Foundation (MILID Foundation)
- Paradigm Initiative
- Socio - Economic Rights And Accountability Project (SERAP)
- Tech Societal
- TechHer
- Yiaga Africa

ECOWAS Commission directorates

- ECOWAS Commission, Directorate Communication
- ECOWAS Commission, Directorate Digital, Post, and Economy*
- ECOWAS Commission, Directorate IT*
- ECOWAS Commission, Directorate Political Affairs*

V. Opening

5.1 Welcome Remarks

Charles Ebuebu, Director-General of NBC and Representative of ACRAN

The Director General of the National Broadcasting Commission (NBC) and representative of the African Communications Regulatory Authorities Network (ACRAN) noted that information integrity efforts must align with Nigeria's constitutional guarantee of freedom of expression, cultural diversity, and lived experience with disinformation and hate speech.

He highlighted Nigeria's position as Africa's largest democracy, noting that the country's over 150 million internet users make its information ecosystem highly influential across the continent. He further observed that although laws such as the Cybercrime Act, the NBC Act, and the NITDA Act are already in place, regulatory mandates remain fragmented across different agencies. He stressed the need for institutions to move beyond operational silos and embrace stronger inter-agency synergy and collaboration.

Mr. Charles Ebuebu linked the dialogue to preparations for Nigeria's 2027 electoral cycle, emphasizing the importance of taking proactive measures against disinformation, misinformation, and hate speech well ahead of the elections to protect democratic stability and public trust. He stated that ACRAN and NBC are committed to harmonizing regulatory approaches, sharing early-warning mechanisms, and strengthening platform governance and democratic discourse across Africa.

> *"Let us rise to the occasion, not as competing agencies, but as co-stewards of Nigeria's information integrity… Coordination is no longer a virtue; it is indeed a necessity."*
>
> -- Charles Ebuebu, Director-General of NBC and Representative of ACRAN

5.2 Goodwill Remarks

Carlos Rojas-Arbulu (High Commission of Canada to Nigeria), Lilian Seffer, GIZ Nigeria & ECOWAS and Francis Ezekiel, Directorate of Communication, ECOWAS Commission.

The goodwill remarks featured a unified front of international and regional partners, each emphasizing that Nigeria's digital landscape is the "most significant arena" in Africa. All speakers advocated for a "rights-based approach," ensuring that platform governance does not infringe upon constitutional guarantees like freedom of expression.

Carlos Rojas-Arbulu (Canada) opened the narrative by framing the current era as a critical juncture where the digital landscape is evolving at "remarkable speed," particularly due to the complexities of AI. He noted that Nigeria's information ecosystem has regional consequences, meaning the "Lagos design" for regulation will likely inform standards in cities like Accra and Nairobi. He added that the work in Nigeria aligns with Canada's Africa Strategy, launched in 2025.

Lilian Seffer (GIZ) posited that disinformation is not merely a technical glitch but a symptom of low institutional trust – for information integrity to take hold, there must be a bridge between platform governance and credible public communication. She highlighted that GIZ's support is rooted in the belief that "learning and flexibility" are essential as digital governance is an ever-evolving field.

Francis Ezekiel (ECOWAS) reported that ECOWAS has moved beyond theory into massive action, having already trained over 500 journalists to detect and combat misinformation. He detailed how ECOWAS is modernizing its policies to address the "negative impact" of social media and AI on peace and stability. His narrative centred on collective resilience, pointing to the establishment of the region's first National Response Centre in The Gambia as a template for what Nigeria and others can achieve.

VI. Presentations

6.1 Overview of the Praia Policy Framework for Information Integrity

Edetaen Ojo (Media Rights Agenda) & Michel Kenmoe (UNESCO)

The first session, facilitated by Michel Kenmoe of UNESCO and Edetaen Ojo of Media Rights Agenda, delivered a comprehensive review of the Praia Policy Framework for Information Integrity, officially adopted in Cape Verde on September 5, 2025. The presentation drew from the outcomes of the Regional Conference on Information Integrity in West Africa and the Sahel, held from September 35, 2025, at Techpark in Praia. Convened by UNESCO and the Government of Cape Verde, the conference addressed the escalating challenges posed by disinformation, hate speech, and AI-generated content across the region.

Michel Kenmoe opened the session by explaining that the framework originated from the need to view information integrity through an ecosystemic lens rather than focusing on the content of individual messages. He noted that while journalists once controlled the newsroom process, digital platforms have introduced algorithms and individual content creation that bypass traditional checks.

Following this, Edetaen Ojo detailed the specific commitments within the 19-page document. He explained that the framework is a comprehensive regional instrument designed to guide West African and Sahelian governments, regulators, and civil society in addressing disinformation, hate speech, and AI-generated threats. A central theme was the rights-based approach, emphasizing that efforts to combat information disorder must never violate freedom of expression, privacy, or media freedom. Ojo highlighted a strategic shift from punitive measures (criminal law and punishment) toward proactive measures such as Media and Information Literacy (MIL), to build long-term societal resilience.

The framework identifies five core pillars:

- Pillar 1: Shifting perception to an ecosystemic policy approach.
- Pillar 2: Ensuring proactive and committed access to information for the population.
- Pillar 3: Building population resilience through MIL institutes.
- Pillar 4: Developing the capacity to engage with and govern digital platforms.
- Pillar 5: Fostering intentional synergies and collaboration between all stakeholders, including researchers and fact-checkers

The Framework provides a rights-based, multi-stakeholder strategy to safeguard information integrity across West Africa and the Sahel, combining transparency, accountability, rapid-response mechanisms, and media literacy to address emerging digital threats while upholding freedom of expression and legal safeguards. The Framework calls for stronger transparency and accountability measures, including oversight of content moderation systems and assessments of algorithmic risks, observing that sensitive situations such as elections, armed conflicts, public health emergencies, and political instability require stronger safeguards, coordinated rapid-response mechanisms, and early warning systems.

"These threats have become systemic risks affecting democratic participation, electoral integrity, social cohesion, peace and security, and public trust."

-- Michel Kenmoe, UNESCO

"The fact that we are fighting information disorder or misinformation does not mean that human rights should be disregarded."

-- Edetaen Ojo, Media Rights Agenda

Discussion

Regulatory independence: Participants engaged in extensive discussions on how regulatory institutions could maintain credibility and accountability in politically sensitive environments while also addressing the spread of disinformation in local languages. Concerns were raised about how politically appointed agency leaders could be held accountable and be expected to hold accountable in turn those who nominated them.

Acknowledging that the framework could not instantly resolve entrenched political realities, Ojo explained that the framework establishes professional standards and institutional safeguards aimed at reducing such risks. He noted that the framework advocates creating strict professional codes of conduct that prohibit public officials from using their positions to spread false or manipulated information. He further emphasized the need for structural independence in regulatory agencies, particularly in relation to funding mechanisms and leadership arrangements. Edetaen Ojo also stressed the importance of legislative reforms that would guarantee transparent, merit-based appointments, as well as stronger parliamentary oversight systems capable of holding political appointees accountable to the public.

Linguistic realities of moderating digital content: Participants discussed the growing challenge of moderating disinformation in local African languages, especially on closed messaging platforms such as WhatsApp. Michel Kenmoe argued that while individual African countries often lack the influence needed to compel major platforms to invest in local language moderation, a united regional bloc, whether within West Africa or across the African continent, would possess greater leverage to demand stronger commitments from companies such as Meta and Google. He maintained that these corporations have a responsibility to protect African users in the languages through which they communicate, particularly because the companies derive substantial economic benefits from African markets. He also encouraged regulators to strengthen local fact-checking initiatives and support grassroots monitoring mechanisms capable of identifying and countering disinformation within communities in their languages.

Complementing this perspective, Edetaen Ojo emphasized the critical role of Media and Information Literacy in combating disinformation. He explained that empowering citizens with the ability to identify manipulative narratives and misinformation tactics would reduce public vulnerability regardless of language barriers. He further urged digital platforms to abandon the practice of moderating African content exclusively from distant global centres such as Silicon Valley or Dublin and instead collaborate with local experts who possess a deeper understanding of the cultural and linguistic realities of the region.

Key Takeaways and Recommendations

- Fundamental rights including freedom of expression, access to information, privacy, and media independence must underpin all regulatory actions.
- Emerging threats such as social media manipulation, AI-generated content, political interference, and electoral misinformation require proactive, systemic responses.
- Transparency, accountability, and oversight of platforms, including algorithmic assessments and content moderation, are essential for effective governance.
- Sensitive contexts, such as elections, conflicts, or public health crises, demand coordinated rapid-response mechanisms, early warning systems, and proportional safeguards.
- Media and Information Literacy is critical for long-term prevention, empowering citizens to identify misinformation and disinformation.
- Independent media, fact-checkers, civil society, researchers, and academic institutions are vital partners in maintaining a resilient information ecosystem.
- Regulatory independence, technical capacity, and robust reporting and oversight mechanisms are essential for state actors to act responsibly and transparently.
- Interventions must be evidence-driven, legally justified, proportionate, and minimally restrictive, avoiding measures like internet shutdowns or excessive penalties.

6.2 Presentation and Review of the Regulators' Guide

Michel Kenmoe (UNESCO)

This session highlighted the Guide for Regulators to Implement the Information Integrity Model Policy Framework in West Africa and the Sahel, a co-publication of UNESCO, ACRAN, and REFRAM. The Guide, which was developed in consultation with regional and international experts and validated in February 2026 in Pretoria at a meeting of regulators from the region, translates the Praia Policy Framework and the 2024 Abidjan Voluntary Protocol into practical, rights-based standards for regulators. It positions regulators as architects of information integrity rather than reactive content enforcers.

The Guide addresses systemic risks from disinformation, hate speech, technology-facilitated gender-based violence, and child online harms, emphasizing algorithmic accountability, safety-by-design, and local-language moderation. The Guide promotes sustained, coordinated regulatory action to enforce compliance and uphold human rights; Kenmoe drew on the FCCPC vs. Meta and WhatsApp case to illustrate how this might work in practice.

The Guide spans eleven thematic chapters, addressing the full regulatory lifecycle from data protection and multi-lingual redress mechanisms to platform accountability and outlines a proactive approach during elections, including risk assessments, coordination cells, simulations, and rapid-response channels. Non-negotiables, including the prohibition of internet shutdowns, ensure that fundamental rights are preserved even during crises.

To support practical implementation, the Guide provides a set of ready-to-use tools, such as model codes of practice, workflows for managing high-risk incidents, and inter-regulatory coordination frameworks. These tools guide regulators through self-assessment, mandate mapping, platform engagement, and regional coordination, establishing a proactive framework that protects information as a public good.

Michel Kenmoe emphasized a multi-stakeholder approach, involving regulators, civil society, fact-checkers, academia, and governments, while strengthening technical, legal, and institutional capacity to engage platforms effectively. The session also stressed systemic oversight of platform algorithms, advertising systems, and amplification structures, alongside promoting media and information literacy as a long-term solution to misinformation.

Coordination challenges, weak enforcement of existing legal instruments, electoral advertising risks, and the need for judicial technical awareness were noted as key barriers to effective governance.

The session concluded that sustainable information integrity requires ongoing collaboration among regulators, civil society, media institutions, platforms, researchers, and citizens. Success depends on coordinated implementation, institutional accountability, public education, and regional cooperation, recognizing that no single institution can address these challenges alone.

> *"Every rights-impacting decision applies the three-part test: 1) legality, 2) legitimate aim, 3) necessity*
>
> -- Michel Kenmoe, UNESCO

Discussion

Engagement with platforms: Concerns were also raised about the effectiveness of the guidelines when major digital platforms are foreign-owned and increasingly less accountable globally. Participants highlighted poor coordination among regulators and institutions. Participants also noted that digital platforms are businesses that may resist actions affecting profits or operational costs, while concerns were raised about political advertising, platform accountability, and coordinated disinformation campaigns. Kenmoe emphasised the importance of strong institutional coordination and clearer procedures for engaging digital platforms.

Legal framework concerns: Other questions focused on preventing governments from misusing cybercrime laws, internet shutdowns, and regulatory frameworks to suppress freedom of expression during elections, as well as whether regulators should focus more on individuals producing harmful content rather than concentrating mainly on platform regulation and litigation. Participants noted the weak implementation of existing laws, and the need for stronger enforcement and consequences for defaulters spreading misinformation. Kenmoe noted that countries are expected to adapt the Guide into their national frameworks.

Content creators: Participants raised questions about how the guide would engage content creators who are both contributors to the information ecosystem and targets of coordinated disinformation campaigns. Some participants stressed that focusing only on punishing individual content creators would not solve the systemic failures of platforms. Kenmoe explained that the guide promotes a strong multi-stakeholder approach involving content creators, fact-checkers, civil society groups, academia, regulators, and governments.

Media and information literacy was repeatedly identified as a critical pillar for building citizen resilience and reducing harmful online behaviour.

The session concluded with broad agreement that preserving information integrity requires collaboration across governments, regulators, civil society organisations, platforms, media, and citizens.

Key Takeaways

- The Guide functions as an evolving operational tool dependent on phased implementation, capacity building, and sustained multi-stakeholder collaboration.
- Pre-election coordination frameworks with clearly defined mandates and escalation pathways are essential.
- Shift from reactive content policing to systemic, rights-based, multi-stakeholder governance.
- Regulatory focus on major platforms, algorithms, advertising systems, and amplification structures.
- Integration of local-language moderation and safety-by-design mechanisms.
- Legal compliance: interventions must be lawful, necessary, proportionate, and human-rights compliant.
- Judicial institutions need technical capacity to adjudicate platform governance disputes.
- Elections are high-risk periods requiring rapid-response mechanisms, predefined thresholds, and stakeholder coordination.
- Internet shutdowns and platform blocking are unacceptable tools.
- Content creators are vulnerable actors and require protection alongside platform oversight.
- Media and Information Literacy is a critical long-term strategy to combat misinformation.
- Dedicated safeguards needed for women, youth, and minorities, addressing technology-facilitated gender-based violence.
- Institutional silos must be eliminated to strengthen collaboration across regulators, cybersecurity, data protection authorities, civil society, and academia.
- Regional coordination through ECOWAS and the African Union enhances negotiation power with global platforms.
- Transparency and accountability require privacy-compatible access to platform data for accredited stakeholders.

6.3 Mapping of institutional mandates within Nigeria's information integrity ecosystem

Daniel Ukpai (NDI)

Daniel Ukpai opened the session by underscoring the need for clarity regarding legal responsibility for information integrity in Nigeria, noting that effective governance cannot be achieved without first understanding institutional mandates. He explained that Nigeria does not have a centralized information integrity regulator; instead, responsibilities are distributed across multiple agencies. The session aimed to map these mandates, identify overlaps, and clarify coordination pathways to strengthen regulatory effectiveness while safeguarding public trust and human rights.

Ukpai emphasized that without a clear understanding of mandates, efforts risk duplication, institutional friction, and enforcement gaps, which can exacerbate misinformation, particularly during election periods. A well-defined mapping allows each institution to operate within its legal authority, while cross-cutting issues can be addressed collaboratively.

He presented the key regulatory bodies and their roles in the information ecosystem:

- the Nigerian Communications Commission (**NCC**) oversees telecom and internet infrastructure and enforces platform accountability;

- the National Broadcasting Commission (**NBC**) regulates broadcast content and election coverage;
- the National Information Technology Development Agency (**NITDA**) develops IT governance policies and mediates between platforms and national digital policy;
- the Nigeria Data Protection Commission (**NDPC**) protects personal data and ensures compliance on political microtargeting;
- the Independent National Electoral Commission (**INEC**) manages elections, voter education, and election-related misinformation
- the Office of the National Security Adviser (**ONSA**) provides cybersecurity coordination and cybercrime response
- Nigeria Police Force **(NPF)** Cybercrime Unit prevents, detects and investigates cybercrimes and online harms.
- the National Human Rights Commission (**NHRC**) ensures that regulatory actions respect freedom of expression, privacy, and non-discrimination;
- the Federal Competition & Consumer Protection Commission **(FCCPC)** addresses consumer protection, unfair practices, digital marketplace concerns;

- the Advertising Regulatory Council of Nigeria (**ARCON**) manages advertising standards and political and commercial advertising ethics;
- the Nigerian Press Council (**NPC**) upholds media standards and addresses complaints;
- **fact-checkers and CSOs** provide independent monitoring and public education; and
- **digital platforms** ensure operational transparency and follow escalation pathways.

Agencies' mandates overlap in at least three important areas:

i. **Platform governance**, which requires coordinated regulation of content standards, illustrated by scenarios such as viral AI-generated election manipulation videos spreading rapidly across media and telecom networks.
ii. **Data access versus privacy demands** balancing transparency with data protection obligations, particularly around automated political microtargeting.
iii. **Elections and crisis response** necessitate rapid verification, public notification, and protection of rights when misinformation arises during sensitive periods.

The presentation highlighted that Nigeria's information integrity challenge is less about the absence of laws and more about fragmented institutional mandates. The session concluded that the effectiveness of Nigeria's information integrity system depends on sustained coordination, strong inter-agency partnerships, and clear escalation pathways. Systemic, risk-based regulation, regulator independence, transparency, and adherence to human rights were emphasized as guiding principles.

"The ultimate desired outcome is a clearer roadmap for inter-agency cooperation where each agency knows its role and how it fits into the larger puzzle."

-- Daniel Ukpai, NDI

Nigeria's Information Integrity Ecosystem

3 KEY OVERLAP ZONES

1 PLATFORM GOVERNANCE RULES

Platform behaviour, content standards, takedowns, accountability.
Key Regulators: NITDA, NCC, NBC

2 DATA ACCESS VS PRIVACY

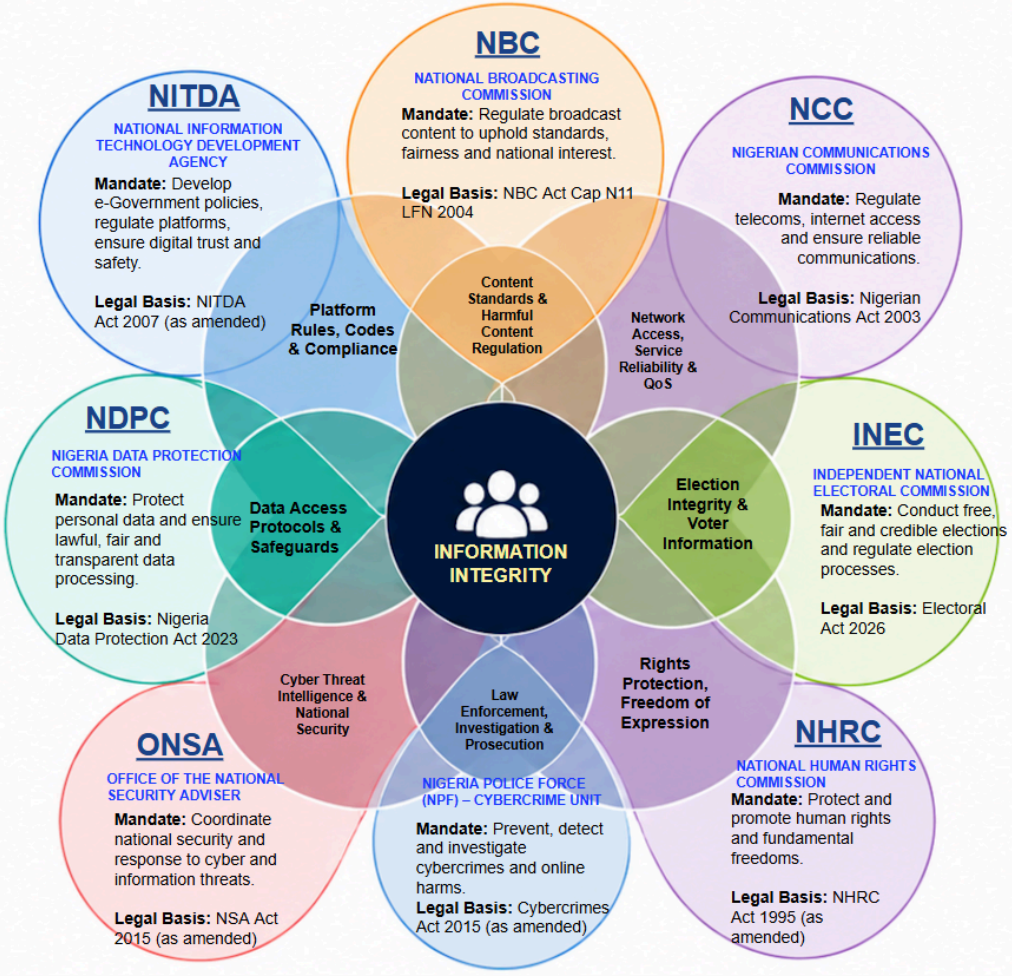
Regulatory access to data for transparency balanced with privacy and data protection obligations.
Key Regulators:NDPC, NITDA, INEC, Others

3 ELECTIONS & CRISIS RESPONSE

Coordinated actions during elections, emergencies and information crises.
Key Regulators: INEC, NCC, NITDA, NBC, ONSA, NHRC, NDPC, Police

OUR SHARED OPPORTUNITY

Each institution has a clear legal mandate. The strength of the system lies in how we connect our mandates through coordination, not in working in silos.



MANDATES INTERSECT

Platform Governance
How platforms operate, moderate content and comply with rules.

Data & Privacy
Access to data for regulatory purposes within privacy limits.

Elections & Crises
Coordinated response during elections and information crises.

Content Regulation
Ensuring accurate, fair and responsible content across media.

Cybersecurity
Protecting systems, infrastructure and citizens online.

Rights & Freedoms
Upholding human rights, freedom of expression and public trust.

THE LEGAL FOUNDATION

All regulators derive authority from Acts of the National Assembly and operating frameworks that empower them to protect the public interest within their domains.

Discussion

Regulatory mandate clarifications: Participants debated whether NBC's authority extends to digital/online platforms. The NDPC's role in enforcing data privacy, especially in cross-border or algorithm-driven cases, was clarified as being primarily through registration, audits, and compliance frameworks.

Coordination and overlap: Participants questioned overlaps between INEC, NBC, advertising agencies, and other regulators in handling election-related content and enforcement. There was a recurring concern about institutional duplication, particularly when multiple agencies act on the same information issue without coordination. While laws exist, enforcement responsibility is often unclear or fragmented across institutions.

When harmful narratives spread across multiple platforms, it was unclear who had primary responsibility. Ukpai explained that there is no single authority; instead, the response depends on content type, medium, and immediate risk. Coordination across agencies is therefore essential. Participants noted that election-related misinformation requires joint rapid-response teams involving INEC, NITDA, and NBC to ensure timely, consistent communication and safeguard public trust.

Security: A discussion emerged around cybercrime coordination and whether agencies such as cybersecurity units operate independently or under broader security institutions.

Advertising and electoral communication: Questions were raised about who holds authority over election-related advertising, misinformation, and micro-targeted political content. Clarification was sought on electoral communication vs electoral advertising and how both are defined within legal frameworks.

Platforms' responses to regulators are often inadequate. Ukpai emphasized the need for clear protocols and escalation pathways, highlighting that agencies like NITDA, NBC, and NCC must coordinate to avoid conflicting instructions.

Human rights protections: Comments from the NHRC stressed the need to protect human rights during content moderation and enforcement.

Key takeaways

- Information integrity in Nigeria is managed by a diverse group of agencies; understanding legal mandates is foundational to coordinating regulatory actions.
- Institutional overlaps exist, particularly in platform governance, data privacy, and election/crisis response, rendering coordination necessary in these areas.
- Networked, coordinated approaches are more effective than siloed action, especially when they involve partnerships with CSOs, media, fact-checkers, and the judiciary.
- Human rights and privacy rights must guide all interventions.
- Clear protocols and escalation pathways improve responsiveness during crises.
- To resolve mandate overlaps, a three-step approach can be used:
    - Mandate Analysis: Deep legal review of what each agency is empowered to do.
    - Overlap Identification: Pinpointing where responsibilities intersect.
    - Synergy Creation: Turning overlaps into collaborative strengths rather than points of conflict.

VII. Scenario Exercises

Moderators: Edetaen Ojo (Media Rights Agenda) & Michel Kenmoe (UNESCO)

This session transitioned the broader dialogue on information integrity from theoretical policy discussions into a practical simulation exercise designed to test institutional preparedness and

inter-agency coordination in a high-risk electoral scenario. Participants reviewed three hypothetical but realistic scenarios:

Plenary Scenario	Scenario A (Groups 1&2)	Scenario B (Groups 3&4)
Overlap of Functions where Multiple regulators have legal authority touching platform behaviour An AI-generated video starts trending across X, TikTok, Facebook, WhatsApp and major popular blogs. It claims that the Election Management Body has secretly tweaked results. Within 2 hours, it is on popular broadcast TV, it is on telecom networks (via sms) nationwide, and it is being amplified by influencers. Citizens are already reacting emotionally.	**Overlap of Functions in Elections and Crisis Response** 48 Hours to Election Day, an AI-generated video surfaces. It shows a candidate conceding defeat—but it is fake. It spreads across all platforms. Within hours, there is massive public outrage, threats and media amplification.	**Election-Period Information Disruption** Two weeks before national elections, false and misleading messages about voting locations, eligibility rules, and polling times begin circulating widely on a major social media platform. The messages are posted and reshared primarily in two local languages spoken in rural areas with historically low voter turnout. Fact-checking organizations observe that the content is being repeatedly amplified through recommendation features and community pages, while official corrections from the electoral commission are not reaching the same audiences. The platform acknowledges the issue but explains that its local language moderation capacity is limited and that escalation queues are already overloaded due to the election period.
Questions		
• Who should contact the platforms first? • Who determines if the content is harmful or just controversial? • Who ensures the response is not censorship? • Who has the authority to request action from platforms? • What if platforms ask: "Who exactly should we respond to?"	• Who verifies if video is fake? • Who informs the public first? • Who contacts platforms? • Who handles the potential criminal elements? • Who ensures that citizens' rights are protected? • How do we avoid different agencies responding at different times with different messages?	• How would you assess the nature and seriousness of this situation, and what factors would guide prioritisation? • Which forms of engagement with the platform are appropriate at this stage, and how would you frame expectations while safeguarding freedom of expression? • What coordination arrangements—with electoral bodies, fact-checkers, media, or other regulators— could improve response during this election and strengthen preparedness for the next one?

The simulations were designed as a "perfect storm" scenario to test how Nigerian institutions would respond when misinformation spreads simultaneously across digital platforms, broadcast media, and telecommunications networks during a politically sensitive period.

In plenary, participants representing different institutions and regulatory bodies provided perspectives based on their respective mandates and operational realities:

- A representative from the **NITDA** explained that agencies such as NITDA are often the first point of engagement with global digital platforms, particularly under directives from ONSA. However, it was observed that one of the major challenges regulators face is that global technology companies frequently prioritize their internal content policies over requests made by national governments and regulators.
- From the broadcast perspective, a representative of **NBC** explained that the Nigeria Broadcasting Code strictly prohibits the dissemination of false information by broadcasters, adding that stations which aired unverified AI-generated electoral content without proper fact-checking would be subject to "Class B" sanctions under the Code.
- A representative from the **Federal Ministry of Information** suggested that, in relation to traditional media, direct communication with editorial leadership and rapid clarification mechanisms may often be more effective than formal regulatory sanctions alone.

The facilitators challenged participants to define practical "thresholds for action" in situations where misinformation spreads primarily through social media platforms. It was observed that sanctioning a broadcast station alone would not sufficiently address the root problem if citizens were consuming information through platforms such as TikTok and Facebook.

Following the plenary simulation exercise, participants were divided into four breakout groups and tasked with responding to different governance scenarios related to platform regulation and electoral misinformation. Each pair of groups later reconvened to present their collective deliberations and recommendations.

Groups responding to **Scenario A** focused on determining which institutions should respond depending on the channel through which harmful content was disseminated. Participants agreed that NBC would oversee broadcast media, while agencies such as NITDA and NCC would address online platforms and SMS distribution networks. Where criminal elements were identified, matters would be escalated to the Federal Ministry of Justice, law enforcement agencies, and the Office of the Attorney General.

The groups also highlighted the role of the National Human Rights Commission (NHRC) in protecting citizen rights and ensuring accountability during enforcement processes. Participants stressed that while all institutions share responsibility for safeguarding citizens, accountability structures and reporting lines must remain clearly defined.

The groups emphasized the need for formalized cooperation frameworks among regulators, including operational codes of practice, escalation matrices, inter-agency coordination systems, and structured communication mechanisms capable of ensuring consistency during crises.

Groups responding to **Scenario B** examined the rapid spread of election-related misinformation and the institutional response required to contain its impact. Participants assessed the scenario from several perspectives, including platform governance failures, electoral timeframe, demographic vulnerabilities, and the risk of widespread public distrust and reduced voter turnout.

Participants proposed that engagement with platforms should involve direct coordination led by INEC alongside regulators. Suggested responses included requesting the takedown or quarantine of harmful content, attaching warning labels or community notes to misleading posts, and ensuring that verified electoral information from official INEC channels is widely disseminated.

The groups further emphasized the importance of collaboration with local media organisations, influencers, government agencies, fact-checkers, and civil society actors. Participants also recommended learning from regional and international experiences through partnerships with organizations such as ECOWAS and the African Union.

Additional recommendations included the development of structured election communication guidelines, misinformation observatories, training initiatives, and pre-planned communication strategies capable of responding quickly to harmful narratives. The breakout discussions concluded that no single institution can effectively manage election-related misinformation in isolation, and that success depends on coordinated, multi-stakeholder engagement supported by proactive planning.

"No single institution can preserve information integrity in isolation."

-- Breakout Session Contribution

Discussion

Platform cooperation: Regulators aim to compel global technology companies such as Meta, X, and TikTok to cooperate with national directives during electoral crises. Participants acknowledged that although regulators maintain communication channels with digital platforms, the companies often rely primarily on their own internal policies when deciding whether content constitutes harmful misinformation or protected opinion. Several comments highlighted the broader structural challenges surrounding platform governance. Participants observed that digital platforms are highly influential actors whose algorithms and amplification systems often intensify misinformation during politically sensitive periods.

Regulatory jurisdiction: Discussion over which regulatory institutions should take the lead in responding to harmful AI-generated content during elections revealed overlapping mandates among agencies. Participants noted that while NITDA and NCC are responsible for social media platforms

and telecommunications channels, NBC regulates broadcast stations that rebroadcast harmful content.

Institutional coordination: Contributors repeatedly emphasized the importance of institutional synergy and inter-agency cooperation, noting that fragmented responses weaken crisis management efforts. CSOs and fact-checking networks were identified as critical partners because they are often faster at identifying and debunking viral misinformation than formal regulatory institutions.

AI detection capacity: Participants agreed that there is an urgent need to strengthen internal technical capacity within regulatory institutions to accurately and independently identify synthetic and AI-generated media and manipulated content instead of relying solely on external fact-checkers. This will empower them to more expeditiously escalate complaints to platforms.

Strategies to address misinformation: Participants also emphasized that electoral misinformation cannot be addressed solely through punitive approaches such as content takedowns. Instead, labelling content as AI-generated, issuing rapid public clarifications, and amplifying verified information were identified as more effective strategies in situations where harmful content has already gone viral.

Rights-based approaches: The discussions further highlighted the importance of balancing electoral integrity with freedom of expression and human rights protections. Participants agreed that interventions must remain proportionate, transparent, and legally justified.

Key Takeaways

- Preserving information integrity requires a proactive and coordinated approach, including early warning systems, standard operating procedures, and election preparedness measures.
- Pre-election engagement with digital platforms is essential and should include establishing clear communication channels, escalation procedures, and agreed moderation priorities.
- Harmful AI-generated content is a growing challenge, requiring stronger technical capacity within regulatory agencies to independently detect and assess manipulated content.
- Civil society, fact-checkers, researchers, and media practitioners are vital partners for rapid detection and response to viral misinformation.
- Content takedowns alone are insufficient; systemic strategies such as public rebuttals, warning labels, community notes, and AI-content disclosures are more effective.

VIII. Identification of coordination modalities among relevant institutions

Gabreal Odunsi (Techsocietal) & Edetaen Ojo (Media Rights Agenda)

The session examined current coordination practices among regulators in Nigeria's information integrity ecosystem, focusing on what is working and what could be improved. Gabriel Odunsi of Techsocietal emphasized that while institutional mandates are clearly defined on paper, effectiveness depends on how regulators collaborate in practice, especially when dealing with overlapping issues like election misinformation, platform governance, and cybersecurity incidents.

The discussion focused on improving coordination among institutions responsible for information integrity, misinformation, platform accountability, and election-related digital risks. Odunsi highlighted the need for clear institutional responsibilities in responding to digital harms, including disinformation campaigns, political advertising transparency, child safety, closed channels of virality, synthetic media, and deepfakes. Media and communication regulators, electoral commissions, cybersecurity agencies, data protection authorities, and child protection bodies were identified as key actors depending on the issue involved.

Alongside these areas where institutional leadership might be clear, the discussion underscored that effective platform governance requires moving beyond isolated agency actions toward a National Coordination Council (NCC) model, which can leverage institutions' relative strengths and help identify and address enforcement gaps. Regulators noted that while agencies currently generally perform well within their mandates, issues that cut across agency mandates often lack clear leadership, resulting in delays, duplication, or gaps.

Participants[1] highlighted areas where coordination is working well, including:

- NBC:
    - The development and issuance of the Code of Practice for Interactive Computer Service Platforms/ Internet Intermediaries alongside NITDA and NCC.
    - Dissemination of political broadcasting guidelines and emerging AI-generated content guidelines to broadcast stations ahead of elections.
    - Training of about 500 NBC staff between December 2025 and January 2026 to improve understanding of the NBC Code and aid in correct implementation.
    - Sensitisation workshops for broadcasters, security agencies, INEC, and politicians on what constitutes a political broadcast ahead of off-cycle elections.
    - Engagement with NCC and platforms for coordination, including efforts to ensure platforms with presence in Nigeria register with the commission, which is already being implemented.
- NITDA:
    - The development of the National Data Strategy and National AI Strategy to guide data governance and address AI-generated misinformation.
    - Collaboration with NBC on the Code of Practice for Interactive Computer Service Platforms/Internet Intermediaries. This includes mandatory registration of major platforms in Nigeria and yearly reporting obligations on takedowns and harmful content.
    - The set-up of an election monitoring room that tracks cyberspace and reports harmful content to security stakeholders, such as the Office of the National Security Adviser, for dissemination to relevant stakeholders.
- INEC:
    - Voter education and public communication initiatives aimed at countering misinformation and ensuring citizens receive accurate and timely electoral information.
    - Collaboration with security, intelligence, and relevant stakeholders to respond to

[1] Because of time limitations, only two agencies had sufficient time to provide detailed responses.

emerging electoral information threats, including coordinated disinformation campaigns.
    - Rapid response and information management efforts to support transparency around voter registration, polling procedures, and election result processes.
- NPF:
    - Enforcement of cyber-related offences, particularly cases involving cyberstalking, identity fraud, and coordinated malicious online activity within defined legal frameworks.
    - Collaboration with regulatory and intelligence agencies to support escalation and investigation of digital threats affecting public safety and electoral integrity.
    - Response to election-related cyber threats where activities are clearly actionable and supported by sufficient technical and investigative evidence.

They also described areas of challenge, including:

- NBC:
    - Limited coordination at the system level with other regulators and platforms, especially where action depends on other institutions like NITDA or where platform compliance is slow and content damage may already have spread before takedown.
    - NBC does not have the legal authority to sanction broadcasters since sanctions are seen as censorship.
- NITDA:
    - No effective collaboration among agencies.
    - Ineffective enforcement of extant national information integrity frameworks.
- NDPC: fast-moving online issues present challenges
- INEC: delays occur when communication is fragmented
- NPF: overlaps create delay

Participants highlighted suggestions for improvement in coordination, including the need to:

- pre-assign lead agencies for specific scenarios (e.g., NBC for broadcast media, NITDA for platforms, NDPC for data);
- establish joint rapid-response teams;
- standardize communication protocols with platforms;
- conduct regular training and simulations for elections and crises; and
- use practical implementation tools, such as the **Model Inter-Regulatory Bodies Coordination Framework (Tool 9 of the Guide),** to ensure coordination becomes operational rather than abstract.

Odunsi introduced the “RACI” coordination model (which identifies which stakeholders are Responsible, Accountable, Consulted, and Informed) as a framework for clarifying institutional roles in digital governance and platform regulation. Tool 9 of the guide presents an example of how this tool can be established; the issue categories listed in the coordination framework are not exhaustive and can be adapted and expanded by countries based on their institutional realities.

The presentation repeatedly emphasised that consultation and coordination mechanisms should already exist before crises emerge. Participants noted that existing structures, including arrangements developed by NITDA, could serve as foundations for broader coordination mechanisms.

"Rapid-response teams should be standard, not optional, during elections or misinformation crises."

"Coordination is not about hierarchy; it is about acting quickly and clearly when issues overlap."

-- Session Participants

Discussion

NBC staff training: A participant asked what training NBC conducted for staff. Ms. Erhunmwunsee responded that 500 NBC staff were trained between December 2025 and January 2026 to improve their understanding of the NBC code and aid implementation.

Legal framework: NBC shared that proposed amendments to the NBC Act are before the National Assembly. Approximately 60 submissions were received during broadcasting code review consultations. Participants asked whether Nigeria's data protection and legal frameworks should compel platforms to comply with local laws. NITDA responded that, in practice, platforms still prioritise their internal global policies over local requests.

Sanctions: Participants questioned whether NBC's sanctioning system respects independent adjudication and fair hearing mechanisms. Civil society representatives argued that ministerial influence over sanctions undermines regulatory independence.

Content takedowns: Participants asked whether NITDA engages with journalists and fact-checkers beyond content takedowns. NITDA acknowledged that takedowns are not sufficient and emphasised the need for awareness campaigns, sensitisation, and media literacy. One person commented that some government takedown requests globally are attempts to censor speech, hence platforms must also try to protect freedom of expression. NITDA reported that platforms have removed millions of harmful contents and accounts under the code of practice.

Transparency concerns were raised over the lack of public visibility into government takedown requests and platform decision-making. Participants noted the importance of access to information frameworks in combating misinformation and disinformation. Stakeholders questioned the adequacy and transparency of platform reports, arguing that raw figures alone are insufficient for research or accountability. Participants urged NITDA to publish more detailed and research-friendly transparency reports. One participant noted that a forthcoming National Cybersecurity Outlook publication from NITDA is expected to contain more detailed transparency data.

Key Takeaways

- Agencies perform effectively within their individual mandates, but cross-cutting issues reveal coordination gaps.
- Pre-defined lead institutions for each major likely scenario could reduce delays and duplication.
- Joint rapid-response teams can improve efficiency and public trust.

- Standardized escalation and communication protocols are critical for multi-agency collaboration.

IX. Keynote Speech: The information environment of the upcoming elections by

Dr. Lawrence Bayode, Director ICT (INEC)

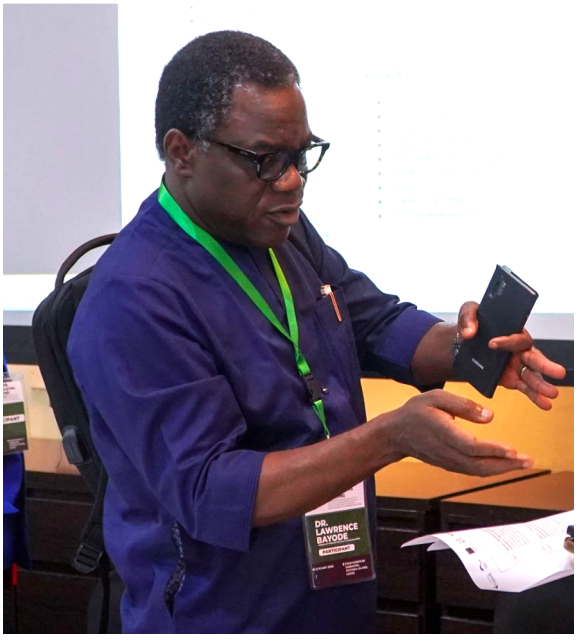
In his keynote, Dr. Lawrence Bayode emphasized that in contemporary electoral processes, elections are contested not just at polling units but also in digital spaces and through narratives, algorithms, viral content, and, increasingly, AI.

He highlighted the evolving nature of disinformation, noting that it is now often coordinated, targeted, and technologically engineered, with threats such as deepfakes, impersonation, manipulated results, and synthetic political messaging. Bayode posed a fundamental question to the assembly: Are existing institutions evolving quickly enough to respond to these emerging threats?

Nigeria hosts one of Africa's largest digital populations, and the stakes are both national and regional. The credibility of Nigeria's elections impacts broader democratic stability. For INEC, the challenge is not only administrative but also custodial, including protecting electoral truth and ensuring citizens have access to accurate information.

Dr. Bayode outlined three strategic pillars guiding INEC's approach toward the 2027 General Elections:

i. *Proactive Information Integrity Management*: Moving from reactive responses to real-time monitoring and early warning systems powered by data and emerging technologies.
ii. *Structured Engagement with Digital Platforms*: Establishing clear escalation channels with social media platforms to address harmful content swiftly and responsibly.
iii. *Public Trust Through Transparency*: Strengthening public communication, voter education, and transparent results management, enabling citizens to verify information directly from official sources.



He stressed that no single institution can safeguard information integrity alone. Effective response lies at the intersection of telecommunications, media regulation, data protection, cybersecurity, and law enforcement. Coordination is therefore essential, not optional. In alignment with the Praia Policy Framework, Dr. Bayode committed INEC to support a coordinated national framework for election information integrity, including:

- Real-time information sharing among institutions.
- Joint response protocols for misinformation and harmful digital content.
- Harmonized engagement with digital platforms and stakeholders.
- Coordinated public communication during critical election periods.

He concluded by emphasizing that the credibility of elections now depends on what citizens see and believe online. The ultimate message was a call to action: institutions must move from awareness to practical, coordinated action, ensuring that truth prevails, public trust is preserved, and democracy is safeguarded.

> *"Today, elections are no longer contested only at the polling units; they are contested in the digital space, in narratives, in algorithms, in viral content, and increasingly in Artificial Intelligence."*
>
> -- Dr. Lawrence Bayode, Director ICT (INEC)

Discussion

Trust-building: A participant raised concerns about the existing deficit of trust in INEC as an institution. Dr. Bayode acknowledged that public confidence has been seriously eroded. He emphasized that restoring trust requires INEC to continue performing its mandate fairly, delivering credible elections consistently, and demonstrating integrity in all its operation to rebuild confidence over time.

Critical electoral periods: A participant asked what constitutes a "critical period" for elections and where Nigeria currently stands. Dr. Bayode explained that the critical period begins as soon as the election timetable is released by INEC. This is the official start of intensive monitoring, coordinated communication, and response activities related to information integrity.

Inter-agency collaboration: In response to a question about practical collaborations for monitoring electoral information, Dr. Bayode detailed that INEC is actively collaborating with the National Cybersecurity Coordination Centre (NCCC) under ONSA, as well as other stakeholders involved in information management. These partnerships enable real-time monitoring and coordinated responses to disinformation threats.

Practical implementation of data-driven approaches: A participant asked about this pillar of INEC's data-driven strategy, including existing partners and gaps. Dr. Lawrence Bayode explained that INEC's proactive approach relies on collaborations with key agencies such as NCC and ONSA, and remains open to further partnerships. He stressed that access to accurate data is essential for real-time monitoring, early warning, and effective intervention against misinformation and harmful content.

Key takeaways

- *Trust Restoration*: Consistent fair execution of INEC's mandate is essential to rebuild public confidence.
- *Critical Periods:* High-alert monitoring and intervention start immediately after the election timetable is released.
- *Data-Driven Strategy*: Access to accurate data and collaborations with relevant stakeholders underpin proactive interventions.
- *Inter-Agency Coordination*: Real-time collaboration among regulatory and cybersecurity bodies is central to electoral information integrity.
- *Transparency and Accountability*: Sustained transparency in communication and operations is crucial for public trust and effective electoral oversight.

X. Discussion of preparedness measures for elections and crisis contexts

Moderator: Francis Madugu (NDI)

Each regulatory body presented its plans related to digital platform governance around the election period.

10.1 Independent National Electoral Commission (INEC)

Dr. Bayode delivered a technical presentation outlining INEC's strategic roadmap for the 2027 General Elections. He described INEC as the primary authority for electoral information credibility in Nigeria. Elections are increasingly contested in digital spaces, and false information, misinformation, AI-generated content, impersonation, and fake election narratives can undermine voter confidence and destabilise electoral processes.

The Commission identified several strategic priorities for 2027, including:

- Combating misinformation and disinformation
- Monitoring deepfakes and AI-generated content
- Establishing structured engagement with digital platforms
- Strengthening voter education and public communication
- Enhancing public trust through transparency and accountability

INEC outlined operational plans for the 2027 elections, including:

- Deployment of a real-time Election Information Monitoring System
- Creation of an Election Information Response Framework
- Structured engagement protocols with digital platforms
- Expanded public information campaigns
- Improved result verification systems
- Development of an AI-driven Election Information Integrity Platform

INEC intends to improve transparency around election technology and communication systems ahead of the 2027 elections. Challenges occurred during the 2023 general elections, particularly misunderstandings about the functionality of the IReV system; clearer communication should have been provided regarding the role and limitations of election technologies. INEC emphasised that going forward it intends to improve public understanding through more direct and proactive communication.

Inter-agency coordination was highlighted as essential for election information integrity. Specifically, INEC plans to look to:

- NCC for telecom and data support
- NBC and ARCON for content regulation
- NDPC for voter data protection and privacy
- NITDA for digital governance
- Security agencies and ONSA for enforcement and response

- Civil society and media organizations for public awareness and fact-checking

INEC proposed the establishment of a National Election Information Integrity Coordination Mechanism to facilitate:

- Real-time information sharing
- Joint response protocols
- Harmonized engagement with digital platforms
- Unified public communication during elections

The presentation concluded by stressing that no single institution can safeguard electoral integrity alone and that collaboration is critical.

Discussion

Access to electoral information: A participant asked what INEC is doing to allow access to electoral information without impediment. Information, including the voters' register, is on the website. Extra information, like Certified True Copies of the register, will cost the applicant a printing fee. Proactive information is available on the agency's official channels.

10.2 National Broadcasting Commission (NBC)

Stella Erhunmwunsee from NBC opened by highlighting the growth of broadcast and online platforms in Nigeria, including over 800 terrestrial radio and television stations, 7 cable operators, and 25 IP-based platforms. While this expansion has enhanced democratic participation, it has also introduced risks such as misinformation, disinformation, fake news, and hate speech, which can threaten national cohesion and the integrity of elections.

NBC's key priorities are as follows:

i. *Real-Time Monitoring*:
Deploying tools to monitor broadcast and online platforms, detect harmful content, and track compliance with regulatory standards.
ii. *Strengthening Broadcaster Compliance*: Enforcing INEC guidelines and NBC regulations through training, sensitization, and oversight.
iii. *Coordinated Platform Governance*: Collaborating with digital platforms and other regulatory agencies to ensure unified responses to harmful content.

Erhunmwunsee highlighted that traditional regulations are limited, as the NBC Act does not yet explicitly cover online platforms. To address this, NBC is pursuing amendments to the NBC Act and the Broadcasting Code to provide clear authority for regulating online content and aligning with the Information Integrity Model Framework.

She emphasized co-regulation as NBC's preferred model, collaborating with NITDA, NCCC (under ONSA), and other agencies. NBC is also deploying modern IP-based monitoring equipment and an NBC monitoring dashboard to provide real-time oversight across terrestrial, cable, and online platforms. Erhunmwunsee discussed initiatives aimed at transparency and local content promotion, including:

- The upcoming FreeTV platform with over 100 free-to-air channels and local content requirements.
- Six regional production studios in Lagos, Abuja, Port Harcourt, Enugu, Kano, and Benin, aimed at creating employment opportunities and producing authentic Nigerian content.

For institutional capacity building, NBC collaborates with civil society organizations and academic institutions, including CEMESO and IPC, and seeks technical and funding support from international partners like UNESCO and GIZ. Proposed initiatives include:

- Joint Election Regulatory Task Force with INEC, NCC, and NITDA.
- Shared rapid response communication protocol to counter viral disinformation and hate speech.
- Collaboration with ICPC and EFCC for monitoring political advertising and campaign finance compliance.

Erhunmwunsee concluded by emphasizing that the evolving digital landscape demands adaptive regulation, capable of addressing AI-driven misinformation and platform manipulation while preserving democratic freedoms. The session's overarching theme was collaboration as the key to effective information integrity management.

Discussion

Voter registers cost: Why did INEC request ₦1.5 billion for access to Certified True Copy (CTC) of voter registers? (In October 2025, V.C. Ottaokpukpu & Associates requested these documents under the Freedom of Information Act.) INEC explained that the amount represented the cost of printing, duplicating, and certifying millions of pages of voter register and polling-unit documents requested as CTCs.

Transparency and public trust: What is INEC doing to improve transparency and public trust? More electoral information will be proactively published through official channels and emphasised lessons learned from previous elections.

INEC servers: Does INEC have a server, and if so, where is it located? Is it publicly or privately owned? INEC has a disaster recovery server, a server running on AWS, and an on-premise server at its Headquarters.

10.3 National Information Technology Development Agency (NITDA)

Dr. Ayodele Bakare's presentation focused on cybersecurity, information integrity, platform governance, and inter-agency collaboration ahead of the 2027 elections. He explained that NITDA's mandate covers both IT regulation and digital development, including digital literacy, deployment of IT centres, and cybersecurity support for government institutions.

He identified cyberattacks as one of the major risks to the election process, particularly because INEC will rely on digital systems that could become targets. To address this, NITDA plans to work with INEC to assess its systems, conduct vulnerability checks, and carry out penetration testing before the elections.

The presentation also highlighted misinformation, disinformation, AI-generated content, fake accounts, bots, and platform abuse as major threats. Dr. Bakare noted that AI could significantly

increase the scale and sophistication of false information during elections.

To respond to these risks, NITDA has established an Election Monitoring Situation Room, which has been used for three election cycles, to monitor harmful election-related content in real time, gather threat intelligence, detect incidents, and share information securely with relevant institutions, such as INEC, ONSA, NBC, and other stakeholders. The monitoring room uses AI-driven Open-Source Intelligence Tools to monitor cyberspace for harmful election-related content. The system includes live threat dashboards, incident detection systems, escalation protocols, and trusted intelligence-sharing platforms. The agency reported achievements from previous election cycles, including addressing over 500 misinformation incidents, removing fake accounts, and maintaining 48-hour communication channels with social media platforms.

He also explained that NITDA has communication channels with major social media platforms through the Code of Practice for Interactive Computer Service Platforms and Internet Intermediaries. This allows the agency to request takedowns and escalate harmful content where necessary.

Dr. Ayodele Bakare concluded by stressing that NITDA cannot handle these challenges alone. He called for strong collaboration among government agencies, platforms, civil society, academia, industry, and international partners to protect Nigeria's digital democracy ahead of the 2027 elections.

Discussion

Monitoring encrypted communications: Does NITDA have the authority or technology to monitor encrypted communications? It does not intercept private encrypted communications but monitors public online spaces using OSINT tools and keyword-based searches.

Platform regulation difficulties: Are social media platforms difficult to regulate because of their business interests and economic influence? NITDA acknowledged challenges in obtaining cooperation from platforms, noting that platform decisions are ultimately subject to their internal policies.

Content takedowns: Participants raised concerns about how quickly harmful content can be removed once identified, especially where disinformation may trigger offline violence. Dr. Bakare of NITDA acknowledged that platform responsiveness remains a major challenge. He explained that although NITDA has escalation channels under the Code of Practice, international platforms may still take hours or even longer to respond because of internal review systems, time-zone differences, and company policies. Where takedown is delayed, NITDA relies on public awareness, fact-checking, and collaboration with security agencies where the content threatens public order.

10.4 National Human Rights Commission (NHRC)

Paulinus Nwoko's presentation emphasised rights protection, voter awareness, election monitoring, and incident reporting. He explained that the Commission has long been involved in monitoring and observing elections, and that its experience from the 2023 elections has helped it strengthen its systems for real-time feedback and response.

A major development is the NHRC's toll-free call centre, 6472, which also functions as a situation room for receiving reports on election-related incidents. The Commission has also sustained its Mobilization of Voters for Election (MOVE) initiative, to educate citizens across the 36 states and the FCT on their right to vote and the importance of participating in elections.

The presentation also highlighted NHRC's focus on security conduct during elections. The Commission is preparing programmes to educate security personnel that their role is limited to protecting voters and maintaining order, rather than interfering in the electoral process. It will also engage political parties and aspirants through town hall meetings to promote peaceful campaigns, discourage hate speech, and encourage responsible political behaviour.

Nwoko further noted that the Commission has developed a hate speech database and an automated complaint-handling platform, report.nhrc.gov.ng, with Android and iOS applications. This platform allows citizens and partner organizations to report election-related issues, gender-based violence, and other human rights violations in real time.

Discussion:

Safeguards: Participants stressed that information integrity work must not become a tool for censorship or abuse.

10.5 Advertising Regulatory Council of Nigeria (ARCON)

Chukwudi Ezeaba explained that ARCON is responsible for ensuring that advertisements comply with Nigerian law, the ethics of the advertising profession, and acceptable community standards. In the context of elections, this role becomes especially important because political parties, candidates, and supporters use advertising to promote political ideas, personalities, and campaign messages.

He noted that ARCON has established offices across all 36 states and the FCT to strengthen monitoring and enforcement. During election periods, the Council sets up special monitoring and reporting systems for political advertisements, with emphasis on vetting and approval before materials are released. This is intended to prevent inflammatory, misleading, abusive, or poorly sourced political messages from entering the public space.

The presentation also highlighted ARCON's concern about the shift of political advertising from traditional media to social media. Chukwudi explained that while traditional media content can be more easily controlled, social media creates new challenges because anyone with a phone can create and distribute political content. For this reason, ARCON works with relevant stakeholders to monitor, report, and respond to harmful or non-compliant political advertising.

He further stressed that political advertisements must be issue-based, clearly sponsored, verifiable, and free from abusive language; ethnic or religious exploitation; distorted claims; and misrepresentation. ARCON is also working with agencies such as NBC, NCC, NCCC, EFCC, and the Police to strengthen enforcement and ensure fairness for all political parties and candidates.

Discussion

Freedom of expression vs. advertising limitations: ARCON was asked how political advertisement vetting can be balanced with freedom of expression. Chukwudi explained that ARCON's role is not to silence criticism or opposition voices, but to ensure that political advertisements are factual, issue-based, and free from hate speech, incitement, abusive language, or unverified claims. He clarified that ethical standards should apply equally to all political parties, including the ruling party.

10.6 Federal Ministry of Justice

Barr. Garuba Sunday explained the Ministry's role in relation to elections, electoral offences, prosecution, and access to public information.

Although the Ministry may not be directly involved in the conduct of elections, its role becomes important where electoral malpractice, prosecution, or post-election legal issues arise. Cases can come to the Ministry through investigations carried out by agencies such as INEC, the Police, EFCC, DSS, and other agencies. The Ministry's responsibility is to monitor developments and intervene where necessary, especially where prosecution is required.

He emphasized the current Attorney-General's cautious approach to public communication and policy action, stating that the Ministry prefers to complete its work carefully before making public pronouncements. He noted that for the forthcoming elections, the Ministry will continue to monitor activities in the background and support lawful intervention where needed.

Barr. Sunday explained that the Freedom of Information Act gives citizens the right to request information from public institutions and also requires institutions to proactively disclose certain categories of information. He referenced INEC's proactive disclosure of some public records and clarified that controversies may arise when people request certified true copies of information that is already publicly available. In such cases, institutions may charge for certification costs, especially where large volumes of documents are involved. He further stated that the Ministry of Justice intervenes when public institutions impose excessive charges that obstruct access to information. Where charges are unreasonable, the Ministry advises such institutions to reduce barriers and respect citizens' right of access to public records.

10.7 Nigerian Police Force National Cybercrime Centre (NPF-NCCC)

Mr Egbunike Nnamdi Emmanuel stressed that the Police are a law enforcement agency, not a regulator of speech or political truth. Therefore, the Police do not intervene simply because a statement is controversial, offensive, or politically disputed. Their involvement begins only when content or conduct meets the threshold of a crime.

He explained that during elections, the Cybercrime Centre focuses on criminal investigation, public safety response, cyber threat attribution, evidence gathering, and support to relevant agencies. The Centre runs cyber election desks that monitor the digital space, produce regular reports, and escalate issues to the Inspector General of Police where necessary. When incidents are detected, the Police assess the evidence, determine whether a criminal threshold has been met, and either investigate directly or refer the matter to the appropriate regulator or agency.

Nnamdi Emmanuel also emphasized that legal thresholds have changed, especially after the 2024 amendment on cyberstalking. He noted that complaints such as online insults or offensive comments may not automatically amount to a crime. In such cases, the Police may decline criminal action and instead advise complainants to seek other civil or regulatory remedies.

He explained that platforms assess takedown requests against both Nigerian law and their internal policies. He warned that this process can be slow, especially with companies that operate under different legal cultures and strong free speech standards.

He concluded by stating that Police intervention must be necessary, proportionate, and based on actionable intelligence. The Police will support election information integrity where criminal conduct, cyber compromise, public safety threats, or evidence-based investigations require law enforcement action.

Discussion:

Expansion opportunity: A participant suggested that existing cybersecurity coordination structures under NCCC could potentially be expanded to include other regulators.

Limits on law enforcement: The Police representative clarified that the Police cannot arrest people simply because a post is false or offensive. Intervention must be based on a clear criminal threshold,

such as incitement, cyberstalking, or a direct threat to public safety. This point was important because it showed the tension between the need for quick action and the need to protect citizens from arbitrary arrests. The Police emphasized that legality, evidence, and due process must guide any enforcement action.

10.8 Yiaga Africa

Cynthia Mbamalu explained that the CSO Yiaga Africa's key activities include systematic election observation, civic and voter education, electoral process and results integrity verification, and countering information manipulation, including foreign information manipulation and interference.

'Watching the Vote' is Yiaga Africa's election observation methodology. A pre-election observation component places supervisors across local government areas to monitor developments and feed information into a centralized database in Abuja. This helps Yiaga verify claims circulating on social media, confirm incidents from local sources, and detect early warning signs that could affect the election environment.

The Process and Result Verification for Transparency, PRVT, is a methodology that Yiaga uses on election day to assess the voting process and verify whether announced results reflect votes cast. Because the method relies on statistics and technology, Yiaga provides estimates rather than exact figures, but the approach enables it to speak credibly on the integrity of election results after INEC announces them.

Cynthia further highlighted Yiaga's Election Results Analysis Dashboard, ERAD, which draws from INEC's IReV portal to analyze and visualize election results in real time. She noted that ERAD depends on the functionality of IReV, meaning that if IReV is unavailable, Yiaga would rely more on PRVT.

Yiaga also counters foreign interference and electoral disinformation through a developing framework that includes real-time social media monitoring; citizen media literacy campaigns with broadcasters; an incident database and reporting; digital campaigns; and coordination with information integrity partners and relevant institutions.

In closing, Mbamalu identified three key needs:

i. a responsive partnership with INEC for timely data and information,
ii. stronger coordination among CSOs working on information integrity, and
iii. collaboration with relevant state institutions.

10.9 Digital Africa Research and Safety Lab (DigiAfricaLab)

Rosemary Ajayi focused on DigiAfricaLab's role in identifying, preventing, and mitigating digital threats to elections and civic participation. This work is especially relevant during high-risk civic periods, where digital threats can influence public trust, voter behaviour, and the wider electoral environment.

The presentation emphasized that digital threats do not begin on election day; rather, they are often built gradually through coordinated amplification, engagement manipulation, impersonation, malicious parody, platform governance gaps, and the laundering of false or misleading information through trusted channels. This makes early monitoring and preparedness

essential well before campaign periods or voting day.

For the 2027 elections, DigiAfricaLab's priorities include election information monitoring and early warning; continuous engagement with platforms, regulators, and civil society; development of election information integrity standards and guidance; institutional preparedness; and building on previous election monitoring and advocacy work.

Ajayi highlighted four areas requiring stronger coordination before 2027:

i. *information sharing:* Ajayi noted that one of the challenges civil society organisations currently face is having to engage multiple regulators individually when reporting or discussing digital threats. She stressed the need for a coordinated regulatory structure that would allow organisations monitoring election-related risks to share information through a central entity rather than having to "knock on the door of every regulator."
ii. *election communication:* Drawing on DigiAfricaLab's experience monitoring elections since 2011, Ajayi emphasised the importance of continuous election information monitoring and early warning efforts. She noted that the organisation plans to produce regular digital risk bulletins and share findings with relevant stakeholders to support informed responses to emerging election-related information threats.
iii. *platform escalation pathways:* Ajayi highlighted DigiAfricaLab's long-standing engagement with social media platforms and noted that the organisation has developed relationships and lessons from those engagements that could benefit Nigerian regulators and civil society. She stressed the importance of strengthening engagement with platforms and creating clearer pathways for raising concerns about harmful content and other digital threats.
iv. *crisis coordination:* Ajayi called for stronger collaboration among civil society organisations, regulators, and government institutions in responding to digital threats. Drawing on the example of the Nigerian Fact-Checking Coalition, she pointed to the value of organisations working together, pooling resources, and coordinating efforts rather than operating independently. She argued that a coordinated approach would enable stakeholders to respond more effectively to emerging election-related risks.

The central message of the presentation was that preparedness, coordination, and public trust must begin early because election-related digital risks develop long before the immediate election period.

10.10 International Press Centre (IPC)

Lanre Arogundade's presentation focused on the IPC's role in strengthening media responsibility and protecting the integrity of the electoral process. IPC's work is grounded in the belief that the media plays a central role in shaping public understanding of elections and can either help safeguard democracy or contribute to the spread of harmful information.

He noted that IPC has been involved in election monitoring since 1999, and its approach for 2027 is built around three main pillars:

i. *media monitoring:* IPC is tracking more than 20 print and online newspapers, as well as broadcast stations across the country, with attention to hate speech, misinformation, disinformation, and coverage of underrepresented groups such as women, young people, and persons with disabilities.
ii. *capacity building:* Journalists need the capacity to verify information before publishing, especially as AI makes fake content easier to produce. Lanre warned that if journalists are unable to fact-check properly, the media could become a channel for spreading disinformation.
iii. *stakeholder engagement*: IPC engages with NBC, the Nigerian Press Council, and other stakeholders to promote compliance with the Nigerian Media Code of Election Coverage.

The overall message was that responsible media practice, fact-checking, and institutional collaboration are essential to protecting electoral integrity.

Discussion of overall session:

Participants observed that multiple regulators appear to be duplicating efforts in platform engagement and monitoring. Several recommended a coordinated engagement mechanism with clearly designated lead agencies depending on the issue. They noted that political interference and institutional hierarchy may however undermine long-term coordination efforts among agencies.

XI. Identifying and addressing challenges to effective regulation

Gabreal Odunsi (TechSocietal)

Participants reflected on the structural, legal, and operational challenges that currently limit the effectiveness of regulatory oversight in Nigeria's information ecosystem and identified realistic approaches to addressing them. This session was structured around four groups, each assigned a specific theme for which they identified key challenges, priority reforms, and immediate actions that could realistically be implemented.

Group 1: Overlapping Mandates

Group 1 examined whether regulatory functions overlap among Nigerian institutions working on information integrity. The group concluded that, at the level of statutory mandates, there are no direct overlaps, but overlaps clearly emerge during implementation. This is especially visible in the moderation and management of harmful content on digital platforms, where institutions such as NITDA, NBC, NCCC and the Police may all have a role.

The group observed that platforms do not necessarily exploit confusion among agencies; they know the relevant government contact points for issues such as takedown requests and cyber-related concerns. However, the group acknowledged that some areas remain unclear, especially online content regulation, where the boundaries between digital platform governance, broadcast regulation, cybersecurity, and harmful content response are not always clearly defined.

Reform suggestions: The group recommended strengthening and expanding the existing **Code of Practice for Interactive Computer Service Platforms and Internet Intermediaries**, which was co-developed by NITDA, NCC, and NBC. They proposed bringing in other relevant actors, such as NCCC, NDPC, civil society, industry actors, and other stakeholders to improve coordination and reduce duplication.

Group 2: Access to Platform Data and Transparency

Group 2 focused on the difficulty of obtaining useful data and transparency from digital platforms. The group identified legal, technical, procedural and financial barriers that limit access to platform data, particularly for African actors. They noted that platforms often refuse to disclose data based on their internal policies, even where such data would support research, intervention, or protection of vulnerable groups.

The group also raised concerns about opaque platform procedures, noting that users and organizations often face unclear complaint or appeal systems. Technical limitations were also highlighted, especially the absence of physical offices for major platforms in Nigeria, which makes follow-up difficult. The group further noted that even when platforms provide data, restrictions such

as non-disclosure agreements may prevent researchers or CSOs from using it meaningfully in reports or public accountability work.

Reform suggestions: The group recommended a stronger framework for access to platform information, clearer transparency obligations, and coordinated engagement between regulators, civil society, and platforms. They stressed that individual agencies acting alone can easily be delayed or redirected, but a joint multi-stakeholder engagement would carry more weight.

Group 3: Capacity and Operational Constraints

Group 3 examined the resource and operational challenges affecting regulators and supporting institutions. The group identified inadequate funding, limited technical expertise, insufficient human resources, and Nigeria's linguistic diversity as major barriers to effective information integrity work. They also noted that overlapping mandates can complicate enforcement because different regulators may be addressing similar issues through different procedures and timelines.

The group identified AI-generated misinformation, deepfakes, and the rapid spread of false information on social media as risks that are growing faster than institutional capacity. They warned that the 2027 election environment is likely to be more complex than previous elections because AI tools are now more accessible and easier to use.

Reform suggestions: The group recommended stronger collaboration among regulators, clearer coordination of overlapping functions, stronger takedown powers, and prosecutorial powers or a prosecutorial mechanism for election-related offences. Immediate actions proposed included training for regulators, civil society, supporting institutions, and the public, as well as strengthening the communication units of regulators so they can become more proactive rather than reactive.

Group 4: Crisis and Election-Specific Gaps

Group 4 addressed whether institutions can respond quickly enough to fast-moving disinformation during elections and crises. The group's answer was no. They identified fragmentation of mandates, weak inter-agency coordination, uncertainty over who communicates with the public, political reluctance to act, skill gaps, and slow platform response as major bottlenecks.

The group warned that if these gaps are not addressed before the next election, the consequences could be serious. These include deeper trust deficits, democratic fatigue, voter apathy, social unrest, insecurity, and the exclusion of vulnerable groups. Gendered disinformation was specifically highlighted as a risk that can discourage women's political participation and reinforce harmful social expectations.

Reform suggestions: The group recommended proactive election communication from INEC before, during, and after elections; inclusive media and information literacy; clearer mandates for regulators; reduction of inter-agency bottlenecks; and direct engagement between regulators and digital platforms on election-period disinformation. They also proposed that platforms should amplify credible information from regulators during high-risk periods.

Key Takeaways

- Nigeria's information ecosystem needs better coordination, clearer authority, stronger capacity, faster access to platform data, and rights-respecting crisis response systems.
- The 2027 elections will require early preparation, joint action, public communication, and structured engagement with platforms to

reduce confusion, delay, and institutional fragmentation.

XII. Development of a short-term roadmap aligned with institutional mandates

Moderators: Daniel Ukpai (NDI) & Alfred Bulakali (Article 19)

Working groups identified a set of practical actions that regulatory institutions can undertake in the short term to strengthen coordination and regulatory effectiveness. Groups 1 and 2 were made up largely of regulators, while Groups 3 and 4 were primarily civil society. The following outputs are largely presented as submitted by groups, with copy edits for clarity and deduplication.

Groups 1 & 3: Elections period

Context-Specific Oversight (Page 39-40 of the Guide)
Ensuring platforms have adequate moderation and crisis-response protocols in place.

Challenges anticipated

- Cyber-attacks on electoral information system
- Disinformation targeting female candidates
- Coordinated harassment
- Impersonation
- Foreign efforts to manipulate election narrative
- Incitement of violence
- Opposition information suppression
- Platform blocking as regulatory tool
- Local language moderation
- Delayed response rate to real-time harms
- Absence of human moderators /over-reliance on AI
- Use of an evasion tactic to bypass moderation
- Lack of investment by platforms in understanding patterns, tactics, and context of information manipulation tactics

Proposed practical actions

- Joint election monitoring situation room
- Standard operating procedures for responses
- Encourage platforms to implement evidence-based preservation policies
- Early platform investment and engagement
- Real-time monitoring and observation of patterns prior to the elections
- Engagement of local moderators and reactivation of the trusted partners network
- Use of AI for local language interpretation

Lead Organization

- ONSA

Other institutions to involve

- NITDA, NBC, Police, NDPC, INEC, ARCON, and other relevant agencies

Algorithmic risks, Response Systems and Proactive Information (Pages 40-41)

Challenges anticipated

- Proliferation of AI-generated content and information manipulation
- Delay in agency response to issues
- False positives or false negatives as an algorithmic risk
- lack of Algorithm transparency
- Prioritisation of paid accounts increases information disorder

Proposed practical actions

- Proactive response from platforms and regulators
- Intensify engagement with platforms to understand and manage algorithm balance
- Media literacy and sensitisation

Lead Organization

- ONSA

Other institutions to involve

- NITDA and other relevant agencies.

Coordination, Partnerships, Learning (Page 41-42)
Collaborating with electoral authorities, civil society, fact-checkers, and judicial and other stakeholders

Challenges anticipated

- Lack of synergy between CSOs, regulators, and platforms
- Silo mentality among stakeholders
- Mutual suspicion among stakeholders
- Lack of a coordination framework among stakeholders
- Ownership of ideas
- Rivalry over funding or jurisdiction
- Gaps in knowledge, technical skills, procedural understanding
- Absence of a single coordinating body or agency for civil society to engage with

Proposed practical action

- Creation of a coordination framework
- Mechanism to improve inter-agency and stakeholder cooperation
- Creation of a monitoring and evaluation framework

Lead Organization

- INEC

Other institutions to involve

- NITDA, NBC, Police, NDPC, INEC, ARCON, and other relevant agencies.

The groups identified the following answers across all three components.

What internal resources will be mobilized?

- Coordination on sources of funding
- Human resource technical capabilities
- Capacity to engage platforms
- Leverage existing initiatives and tools
- Financial resources

How can civil society be involved?

- Monitoring, accountability, and report sharing
- Advocacy
- Public enlightenment
- Engage platforms to uphold regulatory suggestions
- Counter incitement narrative

Groups 2 & 4: General focus

Monitoring: Establishing mechanisms to track systemic risks enabling disinformation, hate speech, and other threats to thrive.

Challenges anticipated

- Virality and the speed of how disinformation spreads across different digital media platforms.
- Lack of synergy among regulators
- High volume of data to sieve through
- Difficulty in tracing the source of disinformation
- Lack of technical skills/capacity in monitoring cases of cybercrime/disinformation
- No funding for monitoring tools and software
- Skill gap and expertise

Proposed practical action

- Create a real time monitoring/rapid response team
- Coordination and active political will on the side of government to ensure effectiveness and efficiency
- Capacity building on the usage of emerging technologies, e.g, AI dashboard
- Strategic budgeting
- Identify funding partners
- Capacity building and step-down training, followed by M&E for impact and effectiveness

Lead Organization

- NITDA

Other institutions to involve

- NBC
- NCC
- Federal Ministry of Communications Innovation and Digital Economy (FMCIDE)
- Federal Ministry of Information and National Orientation (FMINO)
- NDPC
- INEC

What internal resources will be mobilized?

- Human resources (ICT Teams, Data Analysts)
- AI Platforms
- Goodwill

How can civil society be involved?

- Advocacy
- Tracking/reporting
- Fact-checking disinformation
- Training
- M&E

Risk Assessment: Supervising platforms' algorithmic risk assessments and preventing the misuse of personal data for microtargeting.

Challenges anticipated

- Lack of transparency from platforms from owners
- Privacy laws
- Transfer of data across borders
- Low resource languages

Proposed practical action

- Review enabling legislation
- Regional/Sub-regional coordination through the AU and ECOWAS
- Enforcement of data protection laws
- Advocate for the training of AI models to moderate content in local languages

Lead Organization

- NDPC or NITDA

Other institutions to involve

- NCC
- ONSA
- FMOJ
- FCCPC
- INEC

What internal resources will be mobilized?

- Technical expertise
- Law enactment/review
- Legal framework (can exert this for punitive measures, investigation)

How can civil society be involved?

- Advocacy
- Tracking implementation and reporting on progress for accountability
- Factchecking disinformation
- Awareness on digital rights and governance

Public Reporting: Publishing regular reports on decisions, complaint statistics, and observed trends in the information ecosystem.

Challenges anticipated

- Lack of consistent reporting formats
- Lack of cooperation from the platforms in giving data on decisions and actions taken
- Potential misinterpretation of data
- Lack of capacity and manpower to gather, harvest, and analyse huge datasets from multiple platforms and across multiple agencies
- Lack of coordination among regulators

Proposed practical action

- Have standardized reporting template
- Increasing technical capacity of staff
- Developing AI tools to fast-track analysis
- Use revenue generated from digital tax and international funding
- Set up a inter- regulatory consultative committee for the election period and subsequent election cycles similar to what the security agencies have

Lead Organization

- NITDA

Other institutions to involve

- Media Organizations
- NBC
- INEC
- NOA
- FMINO

What internal resources will be mobilized?

- Information Desks, research departments, and public relations offices across regulators

How can civil society be involved?

- Alternative source of information to include in the report
- Advocacy
- Tracking implementation and reporting on progress for accountability
- Factchecking disinformation
- Awareness on digital rights and governance
- M&E

Enforcement: Ensuring platforms comply with harmonized standards through transparent institutional practices.

Challenges anticipated

- Jurisdictional limitations
- Resistance from platforms
- Limited enforcement capacity
- Lack of enforcement of the existing sanctions and punitive measures

Proposed practical action

- strengthen interagency cooperation
- Impose fines
- Investigate and conduct public hearing for why regulators are not enforcing sanctions

Lead Organization

- Federal Ministry of Justice or NITDA

Other institutions to involve

- NDPC
- NBC
- ARCON
- NHRC

What internal resources will be mobilized?

- policy experts
- compliance units
- investigative teams
- Justice system and the enabling laws of the regulatory institutions to enforce their mandates

How can civil society be involved?

- Monitor and document human rights violations
- Advocate for transparency and accountability

Key Takeaways

- Across the four groups, participants agreed that regulatory effectiveness depends on early preparation, stronger coordination, better technical capacity, and clearer engagement with platforms.
- The most repeated recommendations were the creation of joint monitoring or rapid response structures, improved local-language moderation, better use of AI and data tools, stronger public reporting, and more consistent enforcement.
- The groups emphasized that civil society should not be treated as external observers only. CSOs, fact-checkers, media groups, and digital rights actors can support monitoring, reporting, accountability, advocacy, public education, and human rights protection throughout the election cycle.

XIII. Next Steps for Regional Collaboration

*Moderator: **Hannah Ajakaiye (FactsMatterNG)***

This session explored regional and global approaches to improving regulatory oversight, platform governance, and information integrity, with particular attention to election periods. Panellists emphasized cross-border collaboration, multi-stakeholder engagement, and practical measures to disrupt the economy of disinformation while respecting human rights.

Michel Kenmoe (UNESCO) highlighted the importance of regional observatories, knowledge sharing, and coordinated policy frameworks. He emphasized that ECOWAS and UNESCO are supporting structures to monitor misinformation, harmonize regulations, and facilitate cross-border cooperation. The Praia Policy Framework was cited as a key reference, providing principles for platform governance and collaborative intervention in West Africa. Kenmoe stressed that standardized practices, guided by human rights, transparency, and accountability, are crucial to ensure platforms respond predictably to regulatory requests, reduce duplication, and improve compliance.

Francis Ezekiel (ECOWAS Commission) detailed the institutional and legislative context, explaining that ECOWAS is working to harmonize policies, enable cross-border data flows, and build a regional observatory for information integrity. He noted that ECOWAS's efforts aim to strengthen collective negotiations with digital platforms, facilitate peer learning among member states, and integrate lessons from other regions such as the EU.

Stella Erhunmwunsee (NBC, ACRAN) focused on the practical implementation of platform engagement and monitoring, highlighting voluntary protocols adopted in Accra and Abidjan. She argued that regulatory bodies must develop expertise to analyse platform data, identify the economic incentives behind disinformation, and propose interventions that alter platform behaviour, rather than focusing only on individual takedowns. Erhunmwunsee emphasized the need for collaboration with civil society and academia to build in-house and regional expertise and to standardize requests and procedures for platforms.

Alfred Bulakali (Article 19) emphasized the human rights dimension, warning against regulatory approaches that suppress freedom of expression. He advocated for multi-stakeholder solutions to ensure that interventions target disinformation without curtailing access to diverse information. He argued that regulating platforms should ultimately protect citizens' rights and prevent abuse, balancing accountability with freedom of speech.

> *"Regulators need to leverage civil society and academic expertise to build strong evidence"*
>
> -- Participant from NBC

Discussion

Regional standardization: A participant asked if this was feasible given differences in interpretations of content violations across countries. Erhunmwunsee explained that standardization is principle-based, anchored in human rights, transparency, and accountability and designed to allow innovation while aligning enforcement practices across ECOWAS member states.

"Made in Africa" platforms: Panellists agreed that home-grown digital platforms could help incentivize compliance and reduce dependency on foreign companies.

The session concluded with panellists reinforcing cross-border coordination, capacity building, journalist training, standardisation of processes, and civil society engagement as critical elements for improving platform governance and countering disinformation ahead of elections.

Key takeaways

- Regional coordination, knowledge sharing, and harmonised frameworks are essential for effective platform governance.
- Standardising requests and procedures to platforms improves predictability and compliance.
- Multi-stakeholder approaches in line with the Praia Framework would ensure that interventions protect freedom of expression and human rights.
- Regulatory effectiveness depends on expertise, strong evidence, and collaboration with civil society and academia.
- Interventions should disrupt the economic incentives behind disinformation, not just remove individual posts.
- Home-grown digital platforms could reduce dependence on global platforms and strengthen regional compliance.
- Capacity building for journalists and regulators enhances monitoring, reporting, and proactive engagement during elections.

XIV. Closing remarks

Lilian Seffer (GIZ) & Francis Madugu (NDI)

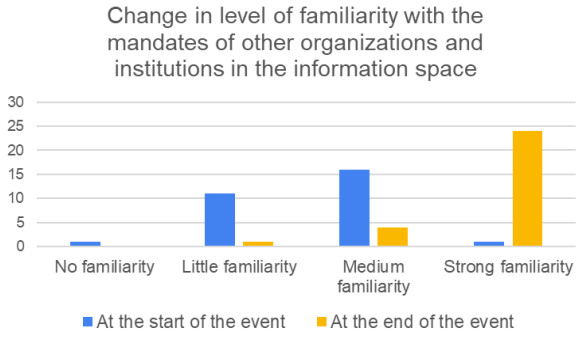
The closing session, delivered by Lilian Seffer (GIZ) and Francis Madugu (NDI), reflected on the successes and lessons of the two-day meeting. Lilian Seffer emphasized appreciation for all contributors, noting the long-term work and dedication of technical teams, regional partners, and civil society actors who enabled the meeting. She highlighted that the event created a space for open dialogue, reflection, and practical planning for the upcoming Nigerian elections, reinforcing the importance of using the developed frameworks in actionable ways. Lilian also reiterated GIZ's commitment to supporting ongoing collaboration between regulators, civil society, and international partners to strengthen information integrity and democratic processes.

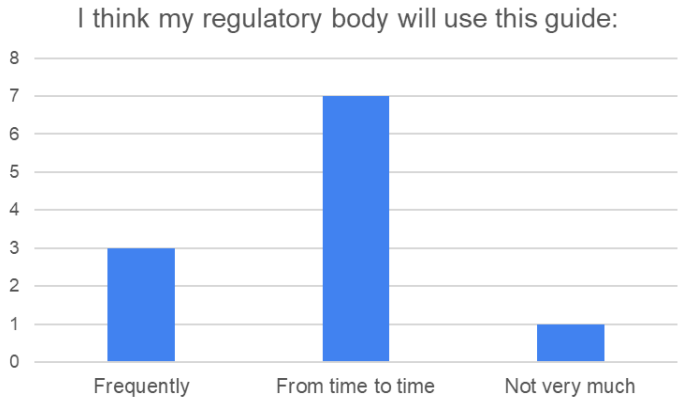
Francis Madugu complemented these remarks by focusing on the importance of celebrating collective achievements, recognizing both Nigerian and international participants, and acknowledging the technical and institutional support that made the event possible. He highlighted the policy framework as a key outcome, emphasizing the dual focus on human and technical elements, hardware and software thinking as critical to effective implementation. Francis Madugu also encouraged participants to use the opportunity to expand networks; actively engage with regulators and civil society partners; and maintain momentum beyond the meeting.

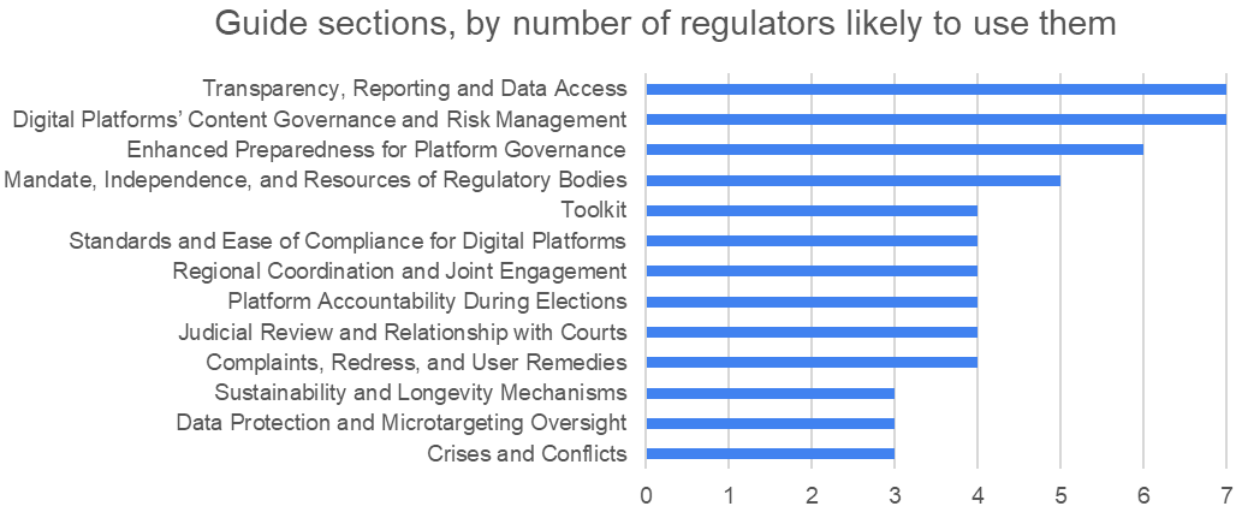
Overall, the closing remarks reinforced collaboration, reflection, appreciation, and proactive engagement as central themes to ensure that the outcomes of the meeting translate into sustained action in Nigeria's election information ecosystem.

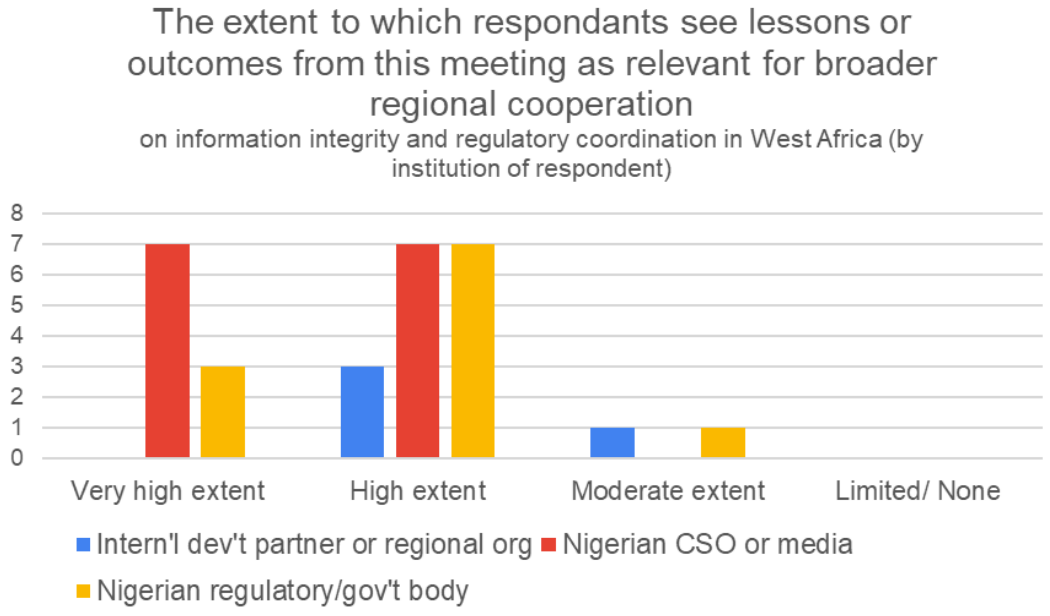
XV. Evaluation

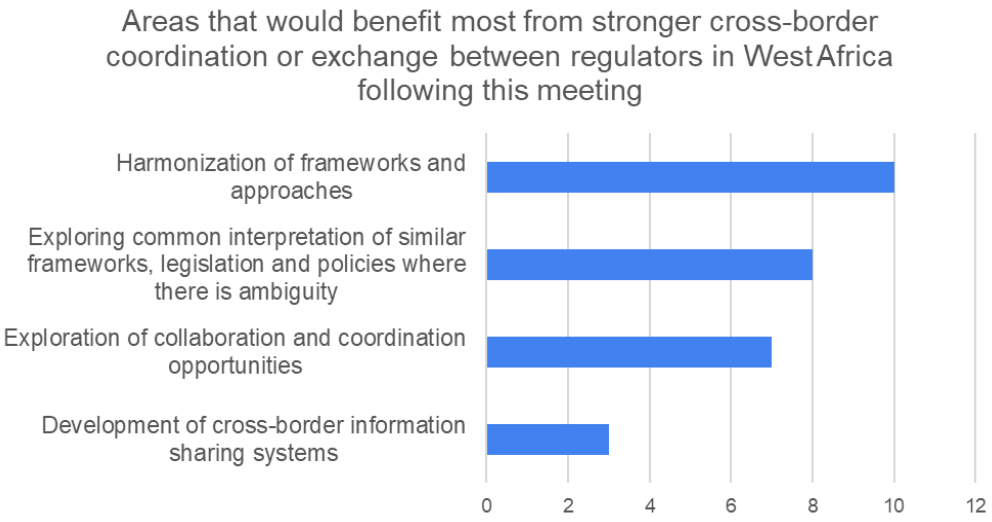
Participants completed an online evaluation questionnaire at the end of the event. The following graphs summarize pertinent results.




I think my regulatory body will use this guide:
8
7
6
5
4
3
2
1
0
Frequently
From time to time
Not very much

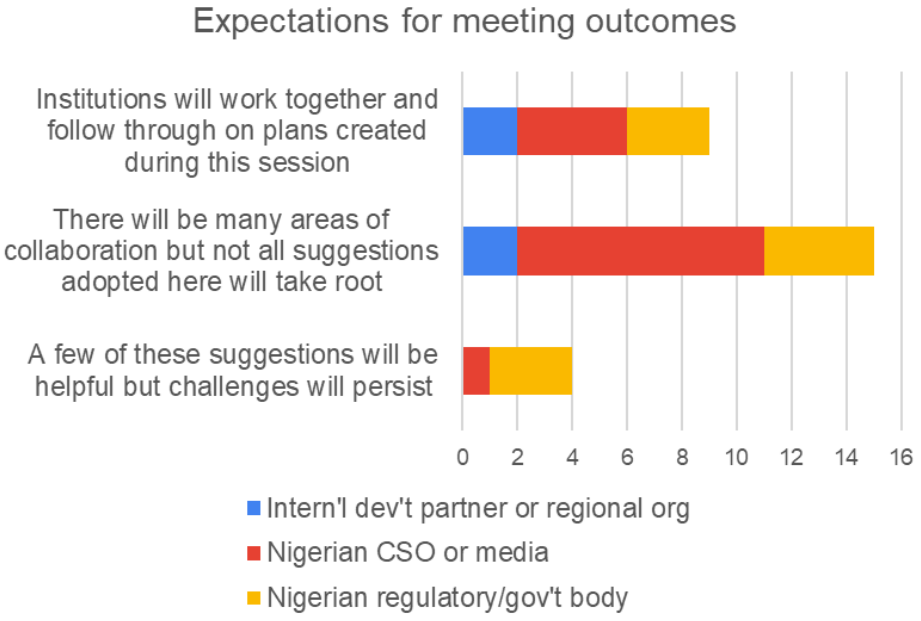

Guide sections, by number of regulators likely to use them
Transparency, Reporting and Data Access
Digital Platforms' Content Governance and Risk Management
Enhanced Preparedness for Platform Governance
Mandate, Independence, and Resources of Regulatory Bodies
Toolkit
Standards and Ease of Compliance for Digital Platforms
Regional Coordination and Joint Engagement
Platform Accountability During Elections
Judicial Review and Relationship with Courts
Complaints, Redress, and User Remedies
Sustainability and Longevity Mechanisms
Data Protection and Microtargeting Oversight
Crises and Conflicts
0
1
2
3
4
5
6
7


The extent to which respondants see lessons or outcomes from this meeting as relevant for broader regional cooperation
on information integrity and regulatory coordination in West Africa (by institution of respondent)
8
7
6
5
4
3
2
1
0
Very high extent
High extent
Moderate extent
Limited/ None
Intern'l dev't partner or regional org
Nigerian CSO or media
Nigerian regulatory/gov't body



Participants were also asked for **examples of regional cooperation** opportunities, priority areas, or mechanisms/platforms that could support coordination within West Africa and the Sahel. Responses included:

- Coordinated engagement with digital platforms and stakeholders
- ECOWAS frameworks and/or protocols
- Stringent attention of platforms to TFGBV across the region. While the EU tightened policies recently in response to Grok scandals, Nigeria and Africa did not respond, even though African women and children are disproportionately affected by TFGBV.
- ACFTA
- An observatory comprising regulators and civil society
- Pooling technical expertise and resources together for the benefit of member states
- Cross border elections monitoring
- knowledge and resources sharing with other Ecowas countries
- Harmonized framework for the region
- regulators' networks (ACRAN and REFRAM)
- CSO/media networks and crossborders plans



Participants were asked what specific **step(s) towards collaboration or changes in their operations** discussed during this meeting they expect their institution will adopt. Responses included:

- Information sharing and regular meetings/ creation of coordination framework for better collaboration
- Capacity development in the area of required technical skills to equip staff with the relevant knowledge.
- Capitalising on human capital and technical skills to achieve goals
- Ensure compliance of relevant institutions
- Familiarization with the Practical Guide and technical review
- Focus on local language adoption for media literacy and other advocacy drives.
- Monitoring and oversight over platforms
- Partnering with fact checking organizations
- Reform laws and regulatory frameworks to meet current realities and use public interest litigation to define the legal mandate of some of the regulatory institutions

Participants were asked what step(s) towards collaboration or changes in their operations they expect to be the **hardest to implement** but are worth the effort? **What support** will they need to implement? Responses included:

- Establishing a joint task group of all organizations that are relevant for platform monitoring and complaints' handling. Selecting a lead agency may be difficult.
- Building sustainable information-sharing and referral systems between civil society, government institutions, and community actors. While trust gaps, bureaucracy, and differing mandates may slow implementation, coordinated response systems are essential for timely accountability and citizen protection. Sustaining long-term collaboration and implementing operational changes across different stakeholders and institutions may be difficult, however.
- Having a broader monitoring and reporting system with other regulatory agencies
- Connection with stakeholders
- Funding
- Engagement with platforms – a formal contact person for the country beyond a regional spokesman
- Training
- Collaboration between CSOs and regulators to flag mis and disinformation.
- Revising existing legal frameworks and statutes will be difficult
- We need a clear plan/strategy leveraging on Praia and post Praia policy framework to guide our advocacy and support

Participants were asked if there was any **specific external support** that they anticipated needing in the short or medium term to use the guide effectively or implement newly suggested actions. Responses included:

- Aggressive advocacy and sensitisation
- Connection with stakeholders
- Funding/ Provision of digital equipment to enhance adequate monitoring and compliance enforcement
- Engagement with relevant stakeholders
- Experiences from other countries and regions
- Domestication of the guide and policy
- Training and capacity building

Participants were asked for their suggestions to make this event **even more effective in future** if it was replicated. Responses included:

- Adoption of a clear plan of action during the event; dedicate 4-6 hours at least to this.
- Develop clear post-event accountability structures such as shared action points, timelines, focal persons, or follow-up working groups to ensure conversations translate into implementation.
- Allocate more time to participants and more interactive means of contributions by participants. Let regulators speak more on the challenges and let CSOs provide solutions to some of the issues raised. A third day could be helpful.
- Bring together the same categories of regulators and ensure the top leadership of regulatory agencies attend. Include more representatives of media professional bodies. Bring in Law makers and judiciary.
- Include even more interactive sessions, practical case studies, and networking opportunities.
- Create follow-up platforms or resources after the event to sustain collaboration and knowledge sharing among participants.
- Share the training resources in advance so there's sufficient time to engage with them.

XVI. Conclusion

The sessions concluded with a shared understanding that information integrity cannot be protected by one institution acting alone. Participants agreed that collaboration, coordination, trust-building, and shared responsibility are necessary to respond effectively to disinformation, harmful online narratives, and digital threats to democracy.

The discussions reinforced the importance of moving beyond isolated reactions toward more proactive, coordinated, and evidence-based responses. Participants stressed that protecting information integrity is not only about regulating content, but also about protecting freedom of expression, public trust, electoral credibility, and democratic participation across the region.

Speakers emphasized that the region is operating within a borderless information environment where the actions of platforms and the spread of harmful content affect multiple countries at the same time. As a result, regulators, governments, civil society organizations, media practitioners, and regional institutions must continue working together across the region to strengthen democratic information ecosystems and protect human rights.

Annex I: List of Acronyms and Abbreviations

ACRAN	African Communications Regulatory Authorities Network
ARCON	Advertising Regulatory Council of Nigeria
AI	Artificial Intelligence
ARCON	Advertising Regulatory Council of Nigeria
BMZ	German Federal Ministry for Economic Cooperation and Development
CEMESO	Centre for Media and Society
CJID	Centre for Journalism Innovation and Development
CSO	Civil Society Organization
ECOWAS	Economic Community of West African States
FCCPC	Federal Competition and Consumer Protection Commission
FMINO	Federal Ministry of Information and National Orientation
FMOJ	Federal Ministry of Justice
GIZ	Deutsche Gesellschaft für Internationale Zusammenarbeit (German Agency for International Cooperation)
ICT	Information and communications technologies
IFES	International Foundation for Electoral Systems
INEC	Independent National Electoral Commission
IPC	International Press Centre
IReV	INEC Result Viewing System
MIL	Media and Information Literacy
MILID	Media and Information Literacy and Intercultural Dialogue Foundation
MRA	Media Rights Agenda
NBC	National Broadcasting Commission
NDI	National Democratic Institute
NDPC	Nigeria Data Protection Commission
NCC	Nigerian Communications Commission
NHRC	National Human Rights Commission
NITDA	National Information Technology Development Agency
NPF-NCCC	National Police Force National Cybercrime Centre
ONSA	Office of the National Security Adviser
OSPRE	Office for Strategic Preparedness and Resilience
SERAP	Socio - Economic Rights And Accountability Project
TFGBV	Technology-Facilitated Gender-Based Violence
UNESCO	United Nations Educational, Scientific, and Cultural Organization