ISSUE BRIEF

October, 2026

Generative AI-Driven Disinformation and Electoral Security in Nigeria: Emerging Threats and Policy Responses Ahead of the 2027 General Elections

By

Timothy Sunday Joshua Ph.D, Chukwuemeka Udeh & Onapajo Hakeem, PhD
Legislative Centre for Security Analysis (LeCeSA)
National Institute for Legislative and Democratic Studies (NILDS)

Executive summary

Nigeria's preparations for the 2027 general elections must account for the growing capacity of generative artificial intelligence (AI) to produce convincing but false political content. AI-generated videos, cloned voices, fabricated statements, manipulated images, and synthetic news reports can be used to impersonate political candidates, undermine public confidence in the Independent National Electoral Commission (INEC), inflame ethnic and religious tensions, and provoke electoral violence. The speed, scale, and apparent credibility of such content create a growing challenge for electoral security and democratic stability.

Although Nigeria's electoral legal framework contains provisions that may be relevant to certain forms of electoral misinformation, a critical concern is whether existing laws adequately address the distinctive characteristics of AI-enabled disinformation. In particular, the Electoral Act 2026 does not expressly establish a comprehensive framework for identifying and addressing AI-generated synthetic media, algorithmic amplification, coordinated disinformation campaigns, or the responsibilities of digital platforms in election-related information manipulation. Existing provisions may apply to particular conduct, depending on the circumstances, but their application to sophisticated AI-generated deception can raise questions of interpretation, evidence, attribution, and enforcement.

This issue brief examines the gap between Nigeria's existing electoral safeguards and the emerging threat of generative AI-driven disinformation. It argues that the challenge is not simply the absence of an AI-specific offence. It also involves weaknesses in institutional preparedness, digital forensic capacity, rapid-response mechanisms, platform accountability, public awareness, and coordination among electoral, security, regulatory, and law-enforcement institutions. Without timely intervention, these gaps could undermine the credibility of the 2027 elections and increase the risk of political instability.

The brief recommends a coordinated, rights-respecting response centred on targeted legal reform, stronger digital forensic capabilities, election-period incident reporting, cooperation with technology platforms, public education, and safeguards against the misuse of disinformation laws to suppress legitimate political criticism.

Introduction

Generative artificial intelligence (AI) is changing how political information is produced and distributed. AI tools can create convincing videos, cloned voices, fabricated statements, and manipulated images that appear authentic. While these technologies offer opportunities for political communication, they can

also be exploited to deceive voters, impersonate public officials, and distort electoral narratives.[1]

These developments present emerging electoral-security concerns for Nigeria ahead of the 2027 general elections. Political competition takes place within a complex environment shaped by partisan rivalry, ethnic and religious sensitivities, regional divisions, and persistent security challenges. AI-generated disinformation could exploit these vulnerabilities by spreading inflammatory narratives, fabricating evidence of electoral malpractice, or misleading citizens about voting procedures.[2]

The implications extend beyond whether voters believe a particular false claim. Synthetic media can create uncertainty about authentic evidence, undermine confidence in electoral institutions, and complicate efforts to verify information during politically sensitive periods. Research indicates that deceptive political deepfakes can increase uncertainty and distrust, even when audiences are not fully persuaded by the content.[3]

Nigeria's legal framework includes the Electoral Act 2026, the Cybercrimes (Prohibition, Prevention, etc.) Act 2015, as amended in 2024, and constitutional protections for freedom of expression. However, the application of these laws to AI-generated electoral deception depends on the precise conduct and applicable statutory provisions. Questions remain about legal clarity, digital evidence, platform accountability, institutional coordination, and the capacity to respond rapidly to emerging threats.

This issue brief examines these gaps and their implications for electoral security in 2027. It identifies areas for legislative intervention, with particular attention to the National Assembly's role in strengthening legal safeguards, institutional preparedness, and accountability while protecting legitimate political expression and democratic participation.

Instances of Generative AI Disinformation in Nigeria this Year

Though limited in number, their presence thereof constitutes a growing risk that cannot be taken for granted, especially as the general elections draw near. A few instances are;

January: Former Oyo First Lady Florence Ajimobi's office said a viral video of her making controversial comments about the 2027 Ekiti governorship election were AI-generated. A forensic review carried out by her office discovered manipulated lip movements and a cloned voice in the video.[4]

May: An AI voice resembling President Bola Tinubu was added to footage from Martins Otse's (popularly known as VeryDarkMan) Instagram video. The cloned voice made politically sensitive remarks about opposition parties, insecurity, public borrowing and the 2027 elections. The presidency condemned it and

[1] Chesney, R., & Citron, D. K. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. California Law Review, 107(6), 1753–1820. https://doi.org/10.15779/Z38RV0D15J

[2] Achi, C. (2026, October 11). AI deepfakes and the 2027 election: Nigeria needs intelligence, not just fact-checking. TheCable. https://www.thecable.ng/ai-deepfakes-and-the-2027-election-nigeria-needs-intelligence-not-just-fact-checking/

[3] Vaccari, C., & Chadwick, A. (2020). Deepfakes and disinformation: Exploring the impact of synthetic political video on deception, uncertainty, and trust in news. Social Media + Society, 6(1). https://doi.org/10.1177/2056305120903408

[4] Imoh, F. (2026, September 11). *Nigeria's 2027 elections face a new threat: AI-generated fakes, warns Toluwani Akinniyi.* Legit.ng. https://www.legit.ng/politics/1730303-nigerias-2027-elections-face-a-threat-ai-generated-deepfakes-warns-toluwani-akinniyi/

called for his arrest but it was later discovered that someone else had taken his Instagram video and attached the audio to it.[5]

August: An AI-generated footage was falsely used to depict terrorists' influx into Nigeria. AI-detection tools revealed that the footage was doctored to turn still photos into motion video and paint a false narrative.[6]

September: Viral newspaper images of Former Vice President Atiku Abubakar promising that "no Nigerian will pay house rent" was confirmed as AI-generated. Dubawa, a fact-checking group rated the image 97% AI-generated.[7] In the same month a video was circulated showing President Bola Tinubu confronting former Vice President Atiku Abubakar over past US records. The fabricated video was then confirmed to be AI-generated.[8]

These instances reflect the growing nature and diversity of AI-generated disinformation. This poses substantial security challenges through the malicious stirring of political, ethnic and religious tension in Nigeria.

Key Gaps in Nigeria's Existing Laws

1. **Legal and Regulatory gap**

The Electoral Act 2026 does not expressly establish a comprehensive framework for AI-generated synthetic political media or coordinated AI-enabled electoral disinformation. Although existing electoral and cybercrime laws may cover certain related conduct, their application depends on the specific offence and available evidence. Section 127 of the Electoral Act, for instance, concerns disorderly conduct at political meetings and should not be treated as a general prohibition of deepfakes. This creates a need to assess whether existing laws are adequate or require targeted clarification.[9]

2. Definitional and Evidentiary Gap

Nigeria requires clearer standards for distinguishing deliberate disinformation from misinformation, satire, political criticism, and legitimate AI-generated content. Establishing whether a recording is synthetic may require digital forensics, source verification, and evidence of intent and attribution. Without clear definitions and evidentiary procedures, enforcement may be inconsistent or expose innocent individuals to wrongful prosecution.

3. Institutional and Technological Capacity Gap

Investigating AI-enabled disinformation requires trained personnel, appropriate forensic tools, and reliable procedures for preserving digital evidence. Electoral authorities and security agencies must be able to identify synthetic content, investigate coordinated campaigns, and establish links between digital activity and unlawful conduct. Weak coordination or insufficient technical capacity could delay investigations and allow harmful narratives to spread unchecked.

---

[5] Babatunde, A. (2026, October 10). *AI and the rise of synthetic media: Is Nigeria ready for 2027?* Digital Tech, AI & Information Disorder Analysis Centre.

[6] Arome, D. (2026, September 7). *AI-generated footage falsely used to represent terrorists' influx into Nigeria.* Dubawa. https://dubawa.org/ai-generated-footage-falsely-used-to-represent-terrorists-influx-into-nigeria/

[7] Anorjin, P. (2026, September 7). *Newspaper images showing Atiku's promises on rents, AI-generated.* Dubawa. https://dubawa.org/newspaper-images-showing-atikus-promises-on-rents-ai-generated/

[8] Taddy, R. (2026, September 22). *False! Video of Tinubu confronting Atiku over past US records, AI-generated.* Dubawa. https://dubawa.org/false-video-of-tinubu-confronting-atiku-over-past-us-records-ai-generated/

[9] Federal Republic of Nigeria. (2024). Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act, 2024.

4. Digital- Platform Accountability Gap

Social media and messaging platforms can facilitate the rapid circulation of fabricated political content. However, uncertainty may remain over procedures for reporting synthetic impersonation, preserving evidence, and responding to deceptive electoral announcements. Clear and transparent platform protocols are necessary, but regulation must avoid arbitrary content removal or partisan censorship.

5. Early-Warning and Rapid-Response Gap

Delayed verification of fabricated election announcements, inflammatory recordings, or false allegations of electoral fraud could undermine public confidence and increase tensions. Fact-checking is important, but its effectiveness depends on timely verification and the reach of corrections. Nigeria needs coordinated reporting, verification, and public communication procedures capable of identifying credible threats before they escalate. For instance, the internet, especially social media was overloaded with AI generated election result, which almost set the country on fire as it was very difficult to differentiate between authentic and fake results, which were spread wide and fast.

6. Public Awareness and Digital-Literacy Gap
Voters may struggle to distinguish authentic recordings from convincing synthetic imitations, particularly when content circulates through trusted social networks. Public education should help citizens verify election-related claims through official sources, identify suspicious impersonation, and report harmful content. Such programmes should promote critical evaluation without treating ordinary political disagreement as disinformation.

Implications for Electoral Security ahead of the 2027 General Elections

1. Voter manipulation and suppression: Fabricated announcements about polling locations, voting dates, or election cancellations could mislead voters and discourage participation. False messages attributed to INEC may be particularly damaging when citizens cannot quickly verify them. Such incidents could compromise electoral participation and require rapid, authoritative communication.

2. Incitement and electoral violence: Synthetic recordings falsely attributed to political, ethnic, or religious leaders could inflame existing tensions and provoke retaliation. Where such content circulates during an already volatile period, delayed verification may complicate security responses. These are plausible risks rather than inevitable outcomes of AI use (Chesney & Citron, 2019).

3. Erosion of institutional trust: Fabricated election results, manipulated recordings of electoral officials, and false allegations of secret political arrangements could undermine confidence in INEC and other institutions. Repeated exposure to deceptive content may also encourage citizens to dismiss authentic evidence as fabricated, complicating electoral dispute resolution (Vaccari & Chadwick, 2020).

4. Coordinated Political Destabilisation: Organised actors could combine synthetic media, impersonation, automated accounts, and targeted messaging to amplify false narratives or discredit political opponents. Such campaigns could exploit existing grievances and overwhelm institutional responses. Effective monitoring should focus on evidence of coordination and credible threats, not political affiliation or viewpoint.

5. Politicisation of Enforcement: Broad or ambiguous disinformation laws could be used to suppress opposition figures, journalists, activists, and legitimate criticism. Such enforcement could weaken public trust and undermine democratic participation. Any response must comply with constitutional protections for freedom of expression and provide safeguards against arbitrary or partisan restrictions (Federal Republic of Nigeria, 1999).

Areas of Legislative Intervention

1. Review of the Electoral Act and Related Legislation

The Senate Committees on Electoral matters may review the Electoral Act 2022 and relevant cybercrime legislation to determine whether they adequately address AI-enabled electoral deception. The review should clarify applicable offences, jurisdiction, evidentiary requirements, and the relationship between existing laws. Any new offence should be narrowly defined to address demonstrably harmful conduct without criminalising ordinary political debate.

2. Clear Definitions and Evidentiary Standards

The Senate Committee on National Security may consider amending the Electoral Act to be able to distinguish deliberate, materially deceptive synthetic media from satire, political opinion, legitimate campaign content, and good-faith reporting. It should also establish appropriate standards for digital evidence, intent, attribution, and prosecution. These safeguards would improve legal certainty and reduce the risk of arbitrary enforcement.

3. Institutional Coordination and Rapid Response

The Senate Committees on Electoral Matters and National Security may consider a clear framework defining how INEC, security agencies, and relevant regulators report, verify, and respond to credible AI-enabled electoral threats. The framework should establish reporting channels, referral procedures, and responsibilities for public communication while respecting institutional mandates. It should also provide for appropriate legislative oversight of implementation.

4. Digital Forensic and Investigative Capacity

The Senate Committees on ICT and Cybercrime may intensify their oversight ensure that relevant agencies have appropriate funding, technical equipment, and training to detect synthetic media and investigate coordinated disinformation campaigns. Support should extend to evidence preservation, prosecution, and judicial understanding of digital forensic evidence. New offences will have limited value without the capacity to investigate them reliably.

5. Public Education and Electoral Information Integrity

The Senate Committee on Communications may support sustained public education on AI-generated disinformation through appropriate legislation, budgetary allocations, and oversight. INEC, educational institutions, civil society organisations, and media partners should provide practical guidance on verifying official announcements and identifying suspicious political recordings. These programmes should promote informed participation rather than impose government control over political narratives.

7. Oversight and Protection of Constitutional Rights

The Senate Committee on Justice may consider a legislative framework which includes safeguards against selective enforcement, unlawful surveillance, and the suppression of legitimate political expression. The Nigeria security agencies should provide appropriate reports on incidents, investigations, enforcement decisions, and complaints, subject to privacy and security requirements. Independent review and effective remedies should be available where individuals or organisations are wrongly targeted. These protections are essential to ensuring that electoral security measures remain consistent with Section 39 of the Constitution.

Conclusion

Generative AI-driven disinformation presents a growing challenge to Nigeria's electoral security ahead of the 2027 general elections. Its potential consequences include voter manipulation, heightened communal tensions, reduced confidence in electoral institutions, and the spread of coordinated political deception.

Nigeria's response should address the gaps in legal clarity, digital evidence, institutional coordination, platform accountability, and public awareness. The National Assembly has a central role in reviewing existing legislation, providing resources for institutional preparedness, and ensuring that any new powers are proportionate and subject to oversight.

The priority is to establish a clear, coordinated, and rights-respecting framework that enables Nigeria to detect and respond to AI-enabled electoral threats without undermining democratic freedoms. Early legislative action, supported by INEC, security agencies, technology platforms, and civil society, would strengthen the country's preparedness for the 2027 elections.

CONTACT
Legislative Centre for Security Analysis (LeCeSA)
National Institute for Legislative and Democratic Studies (NILDS)
National Assembly
Plot 307, Cadastral Zone, Umaru Musa Yar' Adua Expressway
Airport Road, Abuja, Nigeria
E-mail: info@nils.gov.ng
Website: http://nils.gov.ng

NILDS Liaison Office
Suite 214 Senate Wing
National Assembly Complex
Mobile: +234 806 694 5075