

Civic Counter-Intelligence: How Citizen-Owned AI Can Protect Democracy in West Africa

Jude McKelvin Oseh and Ayo O. Ogunlade

ABSTRACT

West Africa's democratic landscape is under unprecedented strain, not from the barrel of a gun alone, but from the barrel of an algorithm. Disinformation ecosystems, AI-powered propaganda networks, foreign-backed digital interference, and state-deployed surveillance infrastructures are quietly reshaping the conditions under which citizens exercise their civic rights—drawing on documentary evidence from Nigeria, Ghana, and Senegal and building on a growing body of scholarship on AI and democratic governance in Africa. This paper argues that the most durable response to these asymmetric threats is not merely regulatory or reactive; it is the construction of a new civic institution: citizen-owned artificial intelligence deployed as a form of Civic Counter-Intelligence (CCI). CCI is defined here as a proactive, community-governed, intelligence-grade capacity that enables ordinary citizens to detect, decode, and neutralise the manipulation of democratic life. Employing a conceptual framework analysis of four structural pillars - technical architecture, political governance, community resilience, and governance performance intelligence, the paper situates CCI within the empirical landscape of AI-enabled threats to democracy, the emerging discourse on African AI sovereignty, and evidence from citizen-led civic technology initiatives already underway across the subregion. The DUTY Civic Tech project (TriAfrica Empowerment Foundation and The Innovation Centre, Nigeria) is examined as an operational instantiation of the proposed framework. The paper concludes with eleven policy recommendations addressed to governments, regional bodies, civil society organisations, and international development partners.

Keywords: Counter-intelligence, civic, citizen, democracy, West Africa

Jude McKelvin Oseh, iamjudeoseh@gmail.com, and Ayo O. Ogunlade, Innovating African Politics and Governance Committee of the School of Politics, Policy and Governance, Public Leaders Network

The Nigerian Journal of Business and Social Sciences, Volume 13, 2026 (Special Issue)
A Journal of the Faculty of Social Sciences, University of Lagos, Akoka, Lagos, Nigeria
© 2026

1. Introduction

The intersection of artificial intelligence and democratic governance has emerged as One of the most consequential policy challenges of the 21st century. Globally, the rapid diffusion of generative AI tools has enabled the production of synthetic media, fabricated audio, video, and text at scale and at minimal cost, fundamentally altering the information environments within which democratic processes take place (Okolo, 2024). In West Africa, this challenge is compounded by structural vulnerabilities: low digital literacy in many communities, linguistic marginalisation in global content moderation systems, the dominance of mobile messaging platforms as primary political communication channels, and a long-standing deficit of verified public information about government performance (Sanusi, 2025; Zisengwe, 2024).

West Africa has simultaneously witnessed an explosion of civic technology initiatives oriented toward democratic accountability. Platforms such as BudgIT, Tracka.ng, UDEME, and the DUTY Civic Tech project represent a growing ecosystem of citizen-led tools designed to bridge the information gap between citizens and the state. However, as Duberry (2022) notes in his analysis of AI and civic technology, these tools are increasingly operating in an adversarial information environment for which they were not originally designed, one in which the data they produce and the citizens they serve are themselves targets of coordinated manipulation. West Africa's democratic landscape faces a new, asymmetric threat. As documented by Freedom House (2023) and the Centre for Democracy and Development (CDD West Africa, 2025), AI-powered disinformation, state-deployed surveillance technologies, and the structural under-representation of African societies in global AI training datasets collectively constitute a systemic threat to the integrity of democratic processes across the subregion. Between 2020 and 2024, internet shutdowns during electoral periods affected over 67 million people across Africa (Access Now, 2024). Africa generates only 2% of global AI training data, leaving the majority of AI systems operating in the subregion structurally miscalibrated for its linguistic, social, and political realities (GIZ, 2025).

Case evidence from Nigeria's 2023 presidential election, where AI-generated voice notes falsely attributed to electoral officials were circulated millions of times on the morning of polling day, and from Senegal's 2024 post-election period, where AI-synthesised video misrepresenting President Faye's statements circulated internationally, illustrates that the threat is not hypothetical. The more recent May 2026 case in Nigeria, in which an AI-generated audio recording was falsely attributed to President Bola Ahmed Tinubu in a video published by activist Martins Vincent Otse (VDM), resulting in a presidential investigation, further confirms that AI-enabled disinformation targeting the highest levels of executive authority has become a recurring feature of Nigeria's political information environment (BBC, 2026). A distinct but related dimension of the problem is governance opacity: the systematic failure of governments across the subregion to make public spending, project implementation, and electoral promises verifiable in real time. As argued by Couldry and Mejias (2019), in environments of information asymmetry, disinformation does not merely distort the truth; it fills vacuums that verified information should occupy. The absence of trusted baseline data on government performance therefore acts as a structural enabler of political disinformation.

Current responses to these threats have been predominantly reactive: fact-checking platforms adjudicate specific false claims after they have circulated; governments issue takedown requests; international organisations produce policy frameworks. What remains absent is a proactive, citizen-governed, AI-enabled counter-infrastructure that addresses the systemic

conditions enabling manipulation rather than its episodic manifestations. This paper aims to conceptualise and operationalise Civic Counter-Intelligence (CCI) as a framework for citizen-owned AI infrastructure to protect democratic processes in West Africa. Specifically, it seeks to:

1. Define CCI and distinguish it from existing reactive approaches such as fact-checking and content moderation;
2. Identify and analyse the four structural pillars of an effective CCI framework;
3. Examine the DUTY Civic Tech project as an empirical instantiation of the Governance Performance Intelligence pillar;
4. Address key counterarguments to the CCI approach; and
5. Propose evidence-grounded policy recommendations for governments, regional bodies, civil society, and international partners.

Scholarship on AI and democratic processes in Africa has accelerated significantly since 2023. Okolo (2024), in her analysis of African democracy in the era of generative disinformation, documents how AI-generated propaganda, including deepfakes, voice clones, and synthetic text, has been deployed across Nigerian, Burkinabe, and Gabonese political contexts to manipulate public opinion and precipitate institutional instability. Sanusi (2025), publishing through the Digital Tech, AI and Information Disorder Analysis Centre (DAIDAC), conducts a discursive analysis of AI disinformation across Nigerian (2023), Ghanaian (2024), and Liberian (2023) elections, finding that AI-generated content amplified ethnic and religious divisions while platform moderation consistently failed to detect manipulation in African language contexts. The structural dimensions of the problem are examined by Effoduh (2024), who argues in the Global Network on Extremism and Technology that the accessibility of AI tools to non-state actors has fundamentally altered the threat landscape for African elections. Research by Democracy in Africa (2025) documents that 60% of disinformation campaigns targeting Africa are foreign-sponsored, primarily from Russia, China, and Gulf states, with West Africa bearing a disproportionate share of such interference. These findings align with the broader literature on information disorder in African elections reviewed by Roberts and Karekwaivanane (2024), who demonstrate that digital disinformation in Africa is not incidental but structurally embedded in the political economy of contested governance.

On the civic technology response, Zisengwe (2024) provides the most rigorous empirical treatment in the African context, examining 52 civic technology initiatives across Nigeria and South Africa through a social accountability framework. The study finds that Nigerian civic tech is predominantly driven by the absence of governance, filling accountability gaps left by formal institutions. This finding echoes Duberry (2022), who identifies both the democratic potential and the institutional risks of AI-mediated citizen-government relations, noting that civic AI tools without robust governance structures can themselves become instruments of manipulation. The data sovereignty dimension is addressed by Couldry and Mejias (2019) in their foundational account of data colonialism and is extended to the African AI context by GIZ (2025) and the African Union's Continental AI Strategy (AU, 2024), both of which call for locally governed AI infrastructure that reflects African linguistic and political realities. The AU strategy's exclusive focus on state and commercial actors, however, leaves a significant gap in the literature on civil society-owned AI, the gap this paper seeks to fill.

The concept of counter-intelligence is deployed here from its security-studies origins. As defined in the US Army Field Manual and elaborated by Sims (cited in Greydynamics, 2025), counterintelligence encompasses 'operations designed to block, disrupt, or destroy the intelligence operations of an adversary.' Transposing this concept to civic life yields the CCI

framework developed in Section 3, which is a citizen-governed capacity to detect, decode, and neutralise threats to democratic decision-making environments. This transposition has precedent in the growing literature on information warfare and democratic resilience, including work by Tucker et al. (2018) on social media and political disinformation, and Gondwe (2025) on encrypted messaging platforms and electoral manipulation in sub-Saharan Africa. This paper employs a conceptual framework analysis methodology, supplemented by documentary evidence review and case study examination, drawing from three primary data sources:

- i. Peer-reviewed academic literature and grey literature on AI, disinformation, and democratic governance in Africa, reviewed systematically across publications from 2019 to 2026;
- ii. Documented case evidence from specific AI-enabled disinformation incidents in Nigeria (2023, 2026), Ghana (2024), and Senegal (2024), drawn from verified journalistic sources (Punch, BBC, Africa Check) and academic analyses (Sanusi, 2025; Okolo, 2024); and
- iii. Institutional documentation from the DUTY Civic Tech project (TriAfrica Empowerment Foundation and The Innovation Centre), including the project's published theory of change, impact architecture, and the founding statement of the Coalition for Participatory Governance (CPG, 2026).

2. Conceptual Framework: Civic Counter-Intelligence (CCI)

Counter-intelligence, in its conventional security-studies formulation, refers to 'information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against' threats to an organisation's intelligence and decision-making environments (Sims, cited in Greydynamics, 2025). The U.S. Army Field Manual defines it as activities 'to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons. This paper transposes this concept from the military-national security domain to civic democratic life, a move with precedent in the public intelligence and democratic theory literature (Tucker et al., 2018).

Civic Counter-Intelligence, as defined in this paper, designates the organised, citizen-governed capacity to:

- Detect AI-generated disinformation, coordinated inauthentic behaviour, and algorithmic manipulation of civic discourse;
- Decode the political interests and technical architectures behind information operations targeting democratic processes;
- Narrate findings back to communities in culturally legible and actionable forms;
- Build resilient information environments that are harder to manipulate; and
- Monitor and expose governance opacity, creating the verified baselines without which disinformation cannot be effectively challenged.

CCI is distinguished from existing approaches along three axes. Unlike fact-checking organisations such as Dubawa Nigeria or Africa Check, CCI operates by proactively mapping information operations architectures before and during deployment, rather than adjudicating specific claims after they have circulated. Unlike state-led content moderation, CCI is citizen-governed; it constitutes surveillance of Power by citizens, not surveillance of citizens by the state. Moreover, unlike imported AI tools that operate in African contexts with foreign training data and foreign governance structures, CCI is locally owned technology adapted by the communities it serves.

The CCI framework is divided into four key pillars: Technical architecture, Political architecture, Community architecture, and Governance Performance Intelligence. The goal is to enable accurate and inclusive stakeholder participation to deliver broad-based, high-impact performance.

i. Technical Architecture: Open-Source, Locally Trained AI Systems

A credible CCI capacity requires a sovereign technical foundation. As the African Union's Continental AI Strategy and the 2025 Kigali Summit commitments recognise, the concentration of AI infrastructure outside African jurisdictions constitutes both a data sovereignty risk and an accountability gap. The first CCI pillar extends this principle to civil society, arguing that sovereign civic AI infrastructure - not merely state or commercial infrastructure is essential for democratic resilience (Couldry & Mejias, 2019).

Key design requirements include:

- Multilingual deepfake and synthetic media detection models trained on West African language corpora (Yoruba, Hausa, Twi, Wolof, Igbo, Fula). As documented by Sanusi (2025) and Democracy in Africa (2025), current moderation tools fail systematically in African language contexts, leaving communities in these languages disproportionately exposed to AI-generated manipulation;
- Open data cooperatives governed by civil society organisations, universities, and community groups, sharing verified datasets on disinformation incidents and electoral manipulation for continuous model improvement, modelled on practices emerging from Code for Africa's continental civic tech network (Code for Africa, 2025);
- Federated AI architectures that allow local organisations to train and update models without centralising sensitive political data outside citizens' jurisdictional control; and
- Lightweight deployment architectures suited to low-bandwidth environments and feature phone ecosystems, addressing the infrastructure realities documented across much of the subregion (Access Now, 2024).

ii. Political Architecture: Democratic Governance of Civic AI

Technology without governance is Power without accountability. This pillar addresses how citizen-owned AI must itself be constituted as a democratic institution.

- Community Oversight Boards composed of civil society actors, journalists, legal aid organisations, traditional community leaders, and elected citizen representatives with authority over model deployment, data use policies, and findings dissemination.
- Adversarial stress-testing protocols that regularly audit CCI AI systems for bias, capture, and misuse.
- Transparency-by-design: all CCI AI systems should operate with publicly disclosed methodologies, open-access findings, and human-in-the-loop verification before outputs are made public.
- Legal protection frameworks for civic technologists, modelled on whistleblower and press freedom protections.

The political pillar also addresses the electoral context directly. The paper proposes differentiated CCI "access tiers" real-time threat intelligence for Electoral Management Bodies (EMBs); verified public narratives for citizens; and forensic datasets for journalists and researchers with appropriate governance gates separating each tier.

3. Community Architecture: Grassroots AI Literacy and Distributed Resilience

Technical and political structures are insufficient without a population capable of engaging with them. This pillar draws on the community-centred tradition in West African civic technology, including platforms like UDEME, Gavel, BudgIT, and Tracka.ng, CivicHive's fellowship programme, and disinformation-tracking coalitions to argue for distributed democratic resilience as the CCI foundation.

Required community-level investments include:

- Community-embedded AI literacy programmes that go beyond generic digital skills to teach communities how to identify synthetic media, understand algorithmic curation, and interrogate information provenance delivered in local languages, through trusted community intermediaries;
- WhatsApp and Telegram-native CCI tools, given that these are the dominant political communication platforms in the subregion. Platforms like CitiBot, deployed during Nigeria's 2024 Edo State gubernatorial election, demonstrate the viability of AI-assisted civic Education through messaging applications;
- Youth-led innovation ecosystems: investing in campus AI clubs, civic hackathons, and community innovation labs cultivating citizens who relate to AI as authors and governors, not merely as users; and
- Indigenous knowledge integration: CCI systems must incorporate community-specific markers of authenticity, local trust networks, and culturally situated norms of evidence. The most reliable sensors of governance failure are often the people most directly harmed by it; making their experiences machine-readable is both a technical challenge and a democratic Justice imperative.

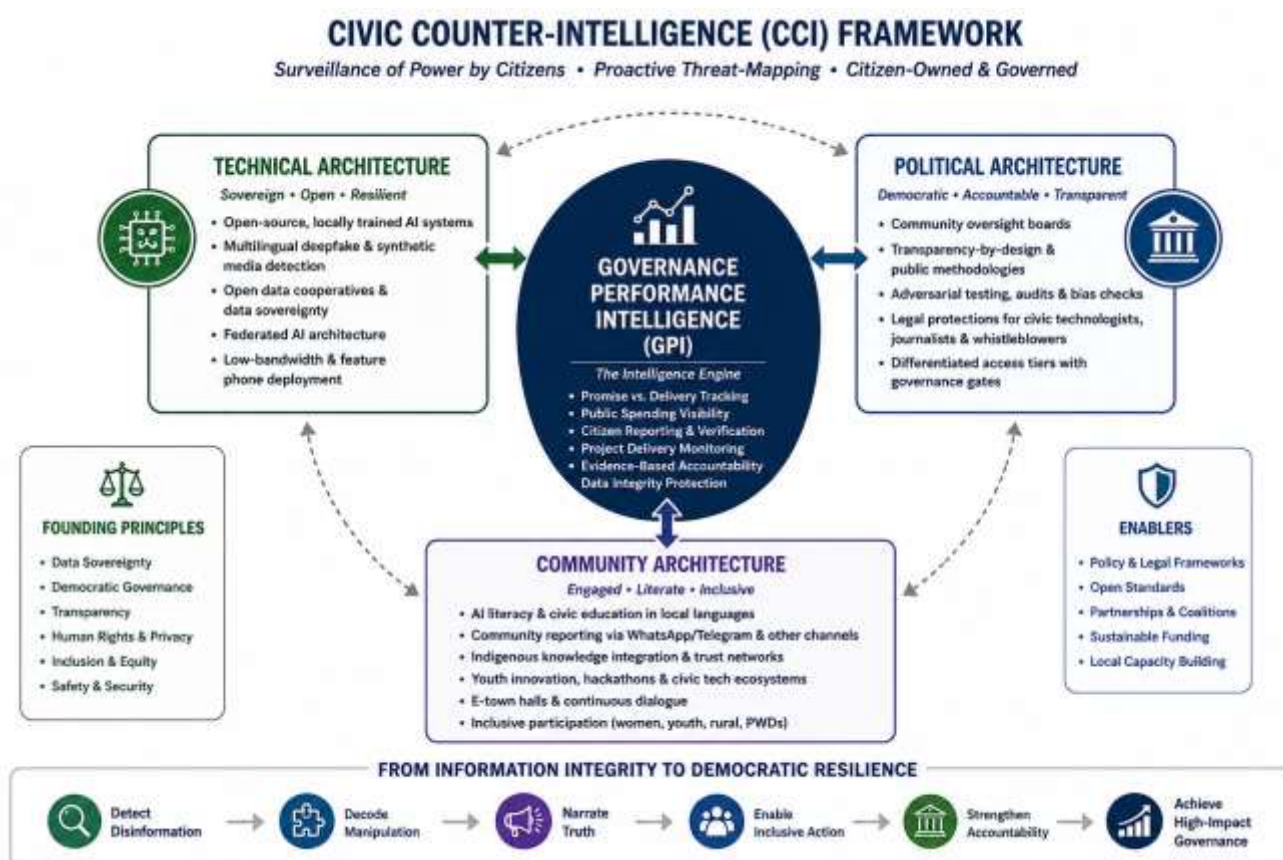
4. Governance Performance Intelligence: Proactive State Accountability as Counter-Intelligence

Disinformation about government performance is most effective in environments where citizens lack access to verified baseline data on what government has actually done. This fourth pillar argues that civic counter-intelligence must include proactive, AI-assisted monitoring of government promises, public expenditure, and project implementation, creating a verified evidentiary baseline that makes disinformation harder to plant and easier to refute. This is not a peripheral add-on to the CCI framework; it is its evidentiary foundation. The three disinformation pillars (detect, decode, narrate) depend on a trusted information baseline. Without that baseline, CCI operates reactively, correcting specific false claims rather than maintaining the information integrity of the democratic environment as a whole.

- AI-assisted promise-vs-delivery tracking across electoral cycles, creating a public record difficult to manipulate retrospectively
- Crowd-sourced, field-verified citizen reporting on abandoned projects, corruption, and poor service delivery, integrated with open public financial data
- Structured feedback channels between citizens and public officials, generating a documented record of governance engagement that constitutes civic intelligence
- Protection of platform data integrity against coordinated disinformation attacks targeting the accountability data itself, requiring integration with disinformation detection layers.

This pillar shifts CCI from reactive disinformation correction to a proactive accountability architecture, making the democratic information environment harder to distort, rather than merely correcting distortions after the fact. As Sanusi (2025) observes in his analysis of West African election disinformation, mitigation 'requires multi-stakeholder collaboration,

robust digital public infrastructure, and policies targeting AI-generated content', precisely what Governance Performance Intelligence, when integrated with the other three pillars, provides, as seen in the diagram below:



In May 2026, TriAfrica Empowerment Foundation convened nine civil society and civic technology organisations into the Coalition for Participatory Governance (CPG), explicitly oriented toward strengthening accountability ahead of Nigeria's 2027 general election. The coalition, powered by BudgIT and Lagos Island Connect, with members including EiE Nigeria, SERAP, the Center for Fiscal Transparency, and the Nigeria Diaspora Coalition for Change, represents precisely the institutional architecture we advocate: a multi-organisational, civic-governed network linking accountability data, legal capacity, fiscal transparency, and citizen mobilisation into a coherent democratic oversight system.

DUTY operates as a node within this coalition: not a standalone tool but a data and engagement infrastructure that feeds into a broader civic intelligence network. This is the correct design model for civic AI in high-stakes democratic environments, distributed nodes, shared methodologies, collective governance, and coordinated response.

From Tools to Institution

The CPG coalition demonstrates the maturation of Nigerian civic technology from individual platform-building to the establishment of institutional networks as a critical developmental threshold. CCI capacity is not built by any single tool or organisation; it emerges from the coordinated operation of multiple civic actors who share data standards, governance principles, and operational trust. TriAfrica Empowerment Foundation's

convening role in the CPG positions it as a potential anchor institution for the broader West African CCI Consortium, as this paper recommends.

Addressing the Counterargument

"Opposition movements or foreign actors could capture Citizen AI"

This is a legitimate risk that is addressed through the governance architecture in Pillar 2. Transparent, multi-stakeholder oversight with adversarial auditing reduces, though cannot eliminate, the risk of capture. The comparison case is not a perfect civic AI; it is the status quo, in which AI-enabled disinformation operates without any citizen-governed counterweight. The CPG coalition's multi-stakeholder composition is itself a structural safeguard against single-actor capture.

"West Africa lacks the technical infrastructure for this"

The infrastructure gap is real but narrowing. Federated, lightweight architectures can operate at the community level without server-grade infrastructure. The \$60 billion Africa AI Fund (2025 Kigali Summit) and the African Union's Continental AI Strategy create a policy opening for channelling resources into civil society AI capacity, if civic actors advocate for their inclusion.

"This is a duplicate of existing fact-checking organisations"

Civic Counter-Intelligence is not a replacement for fact-checking; it is a complementary upstream function. Fact-checkers operate reactively, adjudicating specific claims after they have circulated. CCI operates proactively, maintaining a verified information baseline that enables effective fact-checking and mapping information-operation architectures before and during deployment. Partnerships between DUTY-style accountability platforms and fact-checkers such as Dubawa Nigeria, BudgIT, Tracker.ng, and others are not redundancies; they are the integration model this paper recommends to complete the full CCI architecture.

Policy Recommendations

From the foregoing, the following policy recommendations include establishing national Civic AI Funds, ring-fenced from political executive control, to support citizen-governed AI tools for democratic resilience. Mandate the disclosure of AI-generated political content in electoral periods, with penalties for non-compliance, consistent with emerging international standard-setting on synthetic media labelling. Integrate CCI outputs, under strict protocols jointly developed with civil society, into EMB threat-assessment processes ahead of elections. Develop a West African Civic AI Compact that establishes minimum standards for community-governed AI in democratic contexts, data-sharing protocols among national CCI networks, and cross-border mechanisms for responding to disinformation incidents. Anchor the AU's Continental AI Strategy explicitly in civil society by requiring that a minimum percentage of the \$60 billion Africa AI Fund (Kigali Summit, 2025) reach registered civic technology organisations. Build a West African Civic Counter-Intelligence Consortium, modelled on the Coalition for Participatory Governance, to pool capacity, share methodologies, and collectively govern shared CCI infrastructure. Prioritise African-language AI model development as a core component of civic AI sovereignty, addressing the moderation failure documented across Nigerian, Ghanaian, and other West African election contexts. Embed governance-first principles from the outset of civic AI product design, not as an afterthought. Develop civic AI platforms as integrated, multi-layer accountability systems, combining promise-tracking, public spending visibility, field-level citizen reporting, and multi-stakeholder platforms APIs integrations. Fund these as core CCI infrastructure, not merely as transparency tools, and

support their integration with disinformation-detection capabilities. Establish formal partnerships between governance accountability platforms and fact-checking organisations to protect the integrity of verified governance data against coordinated disinformation attacks. Fund civic AI infrastructure on sustained, multi-year grant cycles, rather than short-cycle literacy campaigns, consistent with the evidence that systemic democratic resilience requires institutional capacity, not episodic awareness interventions. Respect civic AI sovereignty in all technical assistance: tools, data, and governance structures must vest in local organisations, consistent with the data sovereignty principles articulated in the AU Continental AI Strategy (AU, 2024).

Conclusion

Our proposition is simple but consequential: democracy in West Africa cannot be protected by the state alone, cannot wait on foreign platforms to improve their moderation, and cannot be secured by awareness campaigns that outpace the infrastructure they seek to protect. It requires citizens to become themselves intelligence actors, equipped with AI tools they own and govern, embedded in communities they understand, and oriented toward the democratic futures they are building. Civic Counter-Intelligence, as a framework, names this aspiration and provides it with a practical architecture across four pillars: sovereign technical infrastructure, democratic governance of civic AI, grassroots distributed resilience, and proactive governance performance intelligence. It is not a silver bullet. It is a civic institution, One that must be built, contested, refined, and sustained in the same Spirit of participatory democratic practice that the information operations it confronts are designed to destroy. The DUTY Civic Tech project and the Coalition for Participatory Governance are evidence that this institution-building is not waiting for the right conditions; it is already underway. Nigeria's civic technology community is demonstrating, practically and at scale, that citizen-owned AI for democratic resilience is not a theoretical possibility but an organisational reality. The task now is to scale the model, deepen its CCI integration, and connect it to the continental architecture. West Africa's democracy will not be saved by algorithms alone. However, it may yet be defended by citizens who have learned to wield them.

References

- Access Now. (2024). Internet shutdown tracker: Africa report 2020–2024. Access Now.
- African Union (AU). (2024). Continental AI strategy. AU Commission.
- BBC. (2026, May). Nigeria: AI voice note attributed to President Tinubu under investigation by the presidency. BBC News.
- Brinkerhoff, D. W., & Wetterberg, A. (2015). Gauging the effects of social accountability on services, governance, and citizen empowerment. *Public Administration Review*, 75(2), 220–232.
- CDD West Africa. (2025). Artificial intelligence and democratic stability in West Africa: A game changer or a passing disruption? Centre for Democracy and Development.
- CivicHive. (2025). West Africa civic tech landscape report. CivicHive West Africa.
- CivicHive. (2026). Call for papers: Civic technology, democratic resilience, and artificial intelligence in West Africa: West Africa Civic Tech Network / Nigerian Journal of Business and Social Sciences.
- Code for Africa. (2025). Africa's civic tech moment. Medium / Code for Africa DataLab.
- Couldry, N., & Mejias, U. A. (2019). The costs of connection: How data is colonizing human life and appropriating it for capitalism. Stanford University Press.
- Democracy in Africa. (2025). AI-generated propaganda threatens African democracy. Democracy in Africa.

- Duberry, J. (2022). AI and civic tech: Engaging citizens in decision-making processes but not without risks. In *Artificial intelligence and democracy: Risks and promises of AI-mediated citizen–government relations* (pp. 195–216). Edward Elgar.
- Effoduh, J. O. (2024, March 8). The role and potential of artificial intelligence in extremist-fuelled election misinformation in Africa. *Global Network on Extremism and Technology (GNET)*.
- Freedom House. (2023). *Freedom on the net 2023: The repressive Power of artificial intelligence*. Freedom House.
- GIZ. (2025). *Africa-relevant open datasets: Catalysing open AI innovations*. Deutsche Gesellschaft für Internationale Zusammenarbeit.
- Gondwe, G. (2025). AI-driven disinformation and political influence on WhatsApp in South Africa's 2024 elections. *The International Journal of Press/Politics*. <https://doi.org/10.1177/19401612251395434>
- Greydynamics. (2025, November). *A guide to counterintelligence*. Greydynamics Strategic Intelligence.
- Jabareen, Y. (2009). Building a conceptual framework: Philosophy, definitions, and procedure. *International Journal of Qualitative Methods*, 8(4), 49–62.
- Okolo, C. T. (2024). *African democracy in the era of generative disinformation: Challenges and countermeasures against AI-generated propaganda*. ResearchGate / Preprint.
- Penplusbytes / DAIDAC. (2025). *AI and disinformation: A discursive analysis of West African elections*. The CJID.
- Roberts, T., & Karekwaivanane, G. (Eds.). (2024). *Digital disinformation in Africa: Hashtag politics, Power and propaganda*. Zed Books.
- Sanusi, S. A. (2025, October 29). *AI and disinformation: A discursive analysis of West African elections*. Digital Tech, AI & Information Disorder Analysis Centre (DAIDAC). <https://daidac.thecjid.org>
- Smart Africa / Africa AI Council. (2025). *Africa AI strategy: Pooling continental resources*. Smart Africa Secretariat.
- The Cable. (2026, May). *TriAfrica Empowerment Foundation launches Coalition for Participatory Governance ahead of 2027 elections*. The Cable.
- The Cable. (2026, May). *TriAfrica Foundation coalition for participatory governance founding statement*. TheCable.
- Timcke, S., Orembo, A., & Hlomani, H. (2023). AI and 'information disorders' during democratic processes—*African Journal of Information and Communication (AJIC)*, 36.
- TriAfrica Empowerment Foundation & The Innovation Centre. (2026). *DUTY Civic Tech project: Theory of change and impact architecture*. Unpublished institutional document.
- Tucker, J. A., Guess, A., Barberá, P., Vaccari, C., Siegel, A., Sanovich, S., Stukal, D., & Nyhan, B. (2018). *Social media, political polarization, and political disinformation: A review of the scientific literature*. SSRN Electronic Journal.
- US Army. (n.d.). *FM34-60: Counterintelligence — Chapter 3: Operations and techniques*. Federation of American Scientists.
- Zisengwe, M. (2024). *Intersections between civic technology (civic tech) and governance in Nigeria and South Africa*. *African Journal of Information and Communication (AJIC)*. <https://doi.org/10.23962/10539/38956>