The GLOCEPS Policy Brief
Research and Policy Analysis in Governance and Ethics Focus

Governing Elections in an AI-Enabled Environment in Eastern Africa

Stephen Nduvi, Denis Muniu, Ken Ngatia, Mwanaiddi Shafi & Sagero Levin



Photo Credit: Linked In

Executive Summary

The proliferation of Artificial Intelligence (AI) applications in information management is reshaping the electoral environment by accelerating the production, targeting, and dissemination of political information. This can increase the speed, scale, and sophistication of information manipulation, cyber-enabled disruption, and automated political communication, creating new demands on electoral institutions to identify and respond to emerging risks. The African Union Peace and Security Council has called for stronger institutional, operational, and technical capacities among Electoral Management Bodies (EMBs) in response to the growing threat posed by the unethical use of AI in elections. In Eastern Africa, the East African Community Artificial Intelligence Strategy for 2026 to 2031 and the EAC Artificial Intelligence Declaration provide a broader regional policy framework focused on responsible AI governance, infrastructure, skills, data, innovation, and African technological sovereignty.

This brief argues that the region should treat AI preparedness as an institutional capability integrated across the electoral cycle, not as a narrow technology or cybersecurity function. The analysis examines five interrelated issues: AI risk assessment, institutional and technical capacity, information integrity and digital trust, election security coordination, and regional resilience. It

recommends strengthening AI risk assessment in election planning, intensifying multi-agency simulations, developing an East African Community election-specific AI preparedness framework, strengthening coordinated threat intelligence and public communication, and improving assurance over AI-enabled electoral systems and data. This approach would complement existing regional AI and electoral governance initiatives while providing a more integrated framework for institutional preparedness.



Photo Credit: KICTANet

Context

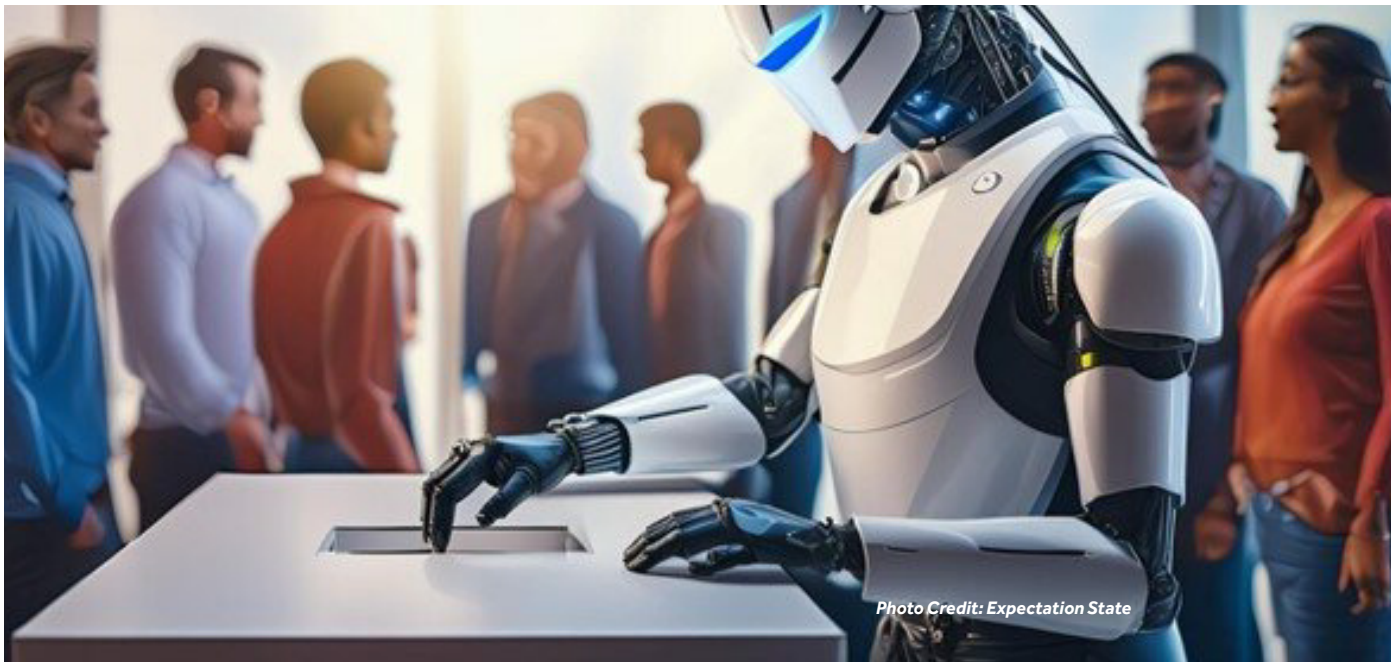
The rapid growth in the use of Artificial Intelligence (AI) applications is changing the operating environment in which elections are administered and contested. Generative systems can produce text, images, audio and video rapidly and at relatively low cost, while automated systems can accelerate the creation and distribution of political content. These capabilities can support legitimate electoral communication and administration, but they can also create vulnerabilities involving synthetic media, impersonation, automated misinformation, cyber-enabled disruption and manipulation of public information.

The institutional significance lies in the reduction of the time available to identify and respond to electoral incidents. Conventional electoral risk management often relies on established procedures for political, logistical, security and operational threats. The use of AI introduces risks that can emerge, spread and interact across several of these categories simultaneously. A fabricated statement attributed to an electoral official, for example, can become an information integrity problem, a cybersecurity concern and a public order issue within a short period.

Eastern Africa's interconnected digital environment adds another layer of complexity. Electoral information increasingly crosses national borders through social media platforms, digital news networks and online communication systems. An incident generated in one jurisdiction can therefore be amplified in another and affect electoral processes beyond the country in which it originated. Differences in technical capability, regulatory frameworks and institutional preparedness consequently create potential points of vulnerability across the regional electoral ecosystem.

Regional policy developments provide an emerging foundation for addressing these challenges. The East African Community has adopted an Artificial Intelligence Declaration that emphasises regional cooperation on artificial intelligence including capabilities, infrastructure, skills, data and responsible governance while advancing African technological sovereignty. The Community subsequently validated its regional Artificial Intelligence Strategy for 2026 to 2031, providing a framework for inclusive and responsible development and deployment of artificial intelligence across Partner States.

The emerging regional framework is significant because it creates an opportunity to connect broader AI governance with the specific requirements of democratic institutions. The African Union Peace and Security Council has recognised this need by calling for stronger institutional, operational and technical capacities among electoral management bodies and greater attention to emerging challenges including deepfakes, digital political advertising and information integrity. The policy imperative for Eastern Africa is therefore to ensure that institutions are sufficiently prepared to govern AI use within increasingly complex electoral environments.


Photo Credit: Expectation State

Emerging Issues

Emerging vulnerabilities in the AI-Enabled Electoral Environment

Artificial Intelligence is transforming the electoral operating environment rather than simply introducing another category of cybersecurity risk. Its applications can influence political communication, voter education, public information, electoral technology, campaign messaging, results-related communication and the interpretation of electoral events. The same technology can generate institutional value while creating new vulnerabilities, with AI-enabled translation potentially improving accessibility while synthetic voice and image technologies can facilitate impersonation. The governance requirement is therefore to identify where AI changes established electoral processes and where conventional safeguards may no longer provide adequate protection.

A significant preparedness gap emerges when institutions assess AI through individual technologies rather than their effects across the electoral

cycle. Risks can arise at the intersection of political communication, cybersecurity, informa tion integrity, procurement, data governance, and public trust, making isolated assessments insufficient. An electoral institution may therefore have cybersecurity procedures and communication protocols while lacking a consolidated understanding of how these systems interact when AI-enabled threats occur simultaneously. This can leave responsibility unclear and limit the ability to anticipate risks before they affect electoral operations.

Preparedness consequently requires an electoral AI risk map covering the full electoral cycle. Such an assessment should identify where AI can affect voter information, institutional communication, technology procurement, cybersecurity, polling, results management and dispute resolution, while distinguishing risks that can be managed internally from those requiring inter-agency or regional cooperation. This would establish clearer risk ownership and provide a basis for incorporating AI scenarios into existing electoral planning rather than creating a parallel governance structure.


Photo Credit: Carles Abarca

Institutional Capability, Skills and Governance

Identifying AI-related risks does not automatically provide institutions with the capability to manage them. Effective preparedness requires personnel who can interpret technical assessments, authenticate digital evidence, evaluate AI systems and translate technical findings into operational decisions. The capability requirement extends beyond information and communications technology specialists to legal officers, procurement teams, communications officials, electoral administrators and senior decision-makers whose actions determine how risks are governed.

Institutional vulnerability increases when technical expertise is separated from decision-making authority. Technical teams may identify an emerging threat without clear procedures for escalating it, while senior officials may have to make time-sensitive decisions without sufficient technical understanding. Dependence on external technology providers can further widen this gap, where institutions have limited capacity to assess system architecture, data practices, security arrangements and the implications of automated outputs. The issue is therefore not simply whether institutions possess AI expertise but whether that

expertise is embedded within effective governance and accountability arrangements.

Institutional preparedness requires sector-specific AI competencies and governance arrangements within existing electoral institutions. These should include capacity to assess AI-related procurement, scrutinise third party systems, interpret technical evidence, maintain human oversight and establish accountability when automated or AI-enabled systems are used in consequential electoral functions. The arrangements will connect techical expertise with institutional authority, legal safeguards and operational decision-making so that identified risks can generate timely and accountable action.



Photo Credit:Carnegie Endowment for International Peace

Information Integrity and Digital Trust

The rapid growth in the use of AI systems is altering the information integrity environment by reducing the technical barriers to producing and distributing convincing synthetic content. Fabricated statements, manipulated recordings, synthetic images and altered videos can be presented as authentic electoral information and circulated through established communication networks. The institutional risk becomes particularly significant when such content impersonates electoral officials, political actors or trusted public institutions because the perceived credibility of the source can influence public reaction before the material is verified.

The preparedness requirement is increasingly defined by the speed and credibility of institutional verification. Where citizens encounter competing versions of an electoral event, delayed authentication can allow uncertainty to develop before an official response is issued. Even when manipulated content is subsequently disproved, the initial information can continue circulating through digital networks. This creates a response problem in which institutions must not only establish factual accuracy but also communicate that determination quickly enough to prevent uncertainty from becoming a wider information integrity challenge.

Information integrity should therefore be treated as a shared institutional function rather than solely as a communications responsibility. Electoral agencies in the region require reliable official

channels, rapid authentication procedures and mechanisms for responding when institutional accounts or electoral information are compromised. The wider information ecosystem is also important because electoral institutions cannot independently monitor every digital platform or information network. Effective preparedness consequently requires functional relationships between electoral agencies, cybersecurity institutions, communications regulators, media organisations and relevant technology actors.

Language capability forms an additional dimension of this preparedness requirement. Eastern Africa's multilingual information environment means that AI systems and verification mechanisms that perform poorly in local languages may create vulnerabilities in the production, interpretation and authentication of electoral information. Strengthening the digitization of local languages in AI applications can increase the capabilities of citizens who are frontline actors to support information integrity while improving the accessibility and credibility of official electoral communication.



Photo Credit: Facebook

Integrated Election Security and Rapid Response

AI-enabled electoral threats increasingly operate across institutional boundaries, making it difficult to separate information manipulation, cybersecurity and election security into independent risk categories. A compromised electoral account can be used to disseminate synthetic content, while a cyber intrusion can coincide with a coordinated information manipulation campaign. Public reactions to such incidents can subsequently generate administrative, political or security pressures, allowing a technical incident to develop into a broader electoral governance challenge.

The preparedness implication is that institutional fragmentation can become a source of vulnerability. An electoral management body may identify suspicious electoral content while a cybersecurity institution detects malicious network activity and a communications authority detects coordinated digital dissemination. If these institutions lack established procedures for combining information, escalating incidents and coordinating public communication, each may respond within its own mandate without generating a common operational picture. The result can be slower

decision-making at precisely the point when speed is necessary to contain uncertainty.

The institutional requirement is therefore stronger coordination across existing mandates rather than the creation of parallel structures. Electoral, cybersecurity, communications and data protection institutions require clearly defined interfaces for threat-intelligence sharing, technical assistance, escalation and public communication. Preparedness should also be demonstrated through multi-agency exercises that reproduce interconnected scenarios rather than testing individual risks separately. Such exercises can establish whether institutional procedures work under pressure and identify gaps between policy, technical capability and operational decision making.



Photo Credit: Facebook

Inclusive and Regional Electoral Resilience

Electoral risks are increasingly being shaped by AI use, becoming unevenly distributed across populations and more difficult to contain within national boundaries. Citizens with limited access to reliable digital information or language-appropriate verification mechanisms may face greater difficulty distinguishing credible electoral information from manipulated content. Digital information can also move across borders through platforms and communication networks, allowing an incident generated in one jurisdiction to influence electoral information environments elsewhere.

These conditions create two interconnected preparedness requirements. At the citizen level, resilience depends partly on the availability of accessible and trusted sources through which electoral information can be verified. At the institutional level, resilience depends on the capacity of national institutions to exchange information and coordinate when risks originate, spread or generate consequences across jurisdictions. Uneven technical and institutional capabilities among Eastern African states can consequently create vulnerabilities that cannot be addressed through national preparedness alone.

Regional cooperation should complement rather than substitute national electoral responsibility. The East African Community can provide a platform for structured information exchange,

peer learning, common risk assessment, technical capacity development and joint preparedness exercises focused on emerging electoral technologies. Such cooperation would not require a regional electoral authority but would create practical mechanisms through which national institutions can learn from one another and respond to risks with cross-border dimensions.

The regional dimension also has implications for technological and linguistic agency. Eastern Africa's capacity to govern AI-enabled electoral environments will depend partly on whether institutions can assess technologies against local languages, data environments and electoral requirements rather than relying entirely on externally developed systems and standards. Building regional knowledge, technical expertise and local language capabilities can therefore strengthen resilience while improving the ability of institutions to make informed decisions about technologies used within democratic processes.



Photo Credit: techweez

Conclusion

Eastern Africa's preparedness for AI-enabled environment for elections should ultimately be understood as a test of institutional adaptability rather than technological control. The issue is not whether emerging technologies can disrupt electoral processes, but whether institutions can continuously adjust their systems, responsibilities and decision making as technological risks evolve. This shifts preparedness from the existence of strategies, regulations and technical systems towards the capacity to deploy them effectively under pressure, particularly when information integrity, cybersecurity and public confidence are affected simultaneously.

For Eastern Africa, the implications extend beyond national electoral boundaries because digital platforms, information flows, technological dependencies and emerging AI capabilities operate across jurisdictions. Strengthening practical regional exchange can therefore complement national responsibility while improving collective capacity to anticipate, assess and respond to emerging risks. The coming electoral cycles provide an important opportunity to connect technological awareness with institutional learning, operational responsiveness and strategic agency. The enduring objective should be an electoral

governance system capable of adapting to technological change while preserving public trust, accountability and democratic continuity.



Photo Credit: The Africa Report

Recommendations

1. **The Regional Electoral Management Bodies should:**
   a) Strengthen AI risk mapping and scenario-based preparedness within existing electoral planning to identify how AI can affect the full electoral cycle and clarify institutional risk ownership.
   b) Intensify AI-related skills development for electoral, legal, procurement, communications and senior management personnel, ensuring technical expertise is connected to operational decision-making.
   c) Strengthen institutional procedures for identifying, authenticating and responding to synthetic electoral content and compromised official communication channels.
   d) Conduct regular multi-agency preparedness exercises covering interconnected AI, cybersecurity and information integrity scenarios.
2. **The East African Community Secretariat should:**
   a) Develop a regional election-specific AI preparedness framework with a common risk taxonomy and practical coordination mechanisms.
   b) Intensify regional information sharing, peer learning and joint preparedness exercises among national electoral and relevant oversight institutions.
   c) Strengthen regional technical capabilities and local-language capabilities to improve the governance, verification and accessibility of AI-enabled electoral information.

3. **National Cybersecurity and Communications Authorities should:**
   a) Strengthen formal threat intelligence sharing and operational coordination with electoral management bodies.
   b) Establish clear procedures for incident escalation, technical assistance and coordinated public communication during AI-enabled electoral incidents.
   c) Leverage rapid authentication and verification mechanisms for suspected synthetic electoral content and compromised institutional accounts.
4. **National Data Protection Authorities in each country should:**
   a) Strengthen oversight of AI systems processing voter, biometric and other electoral data.
   b) Intensify assessment of third-party AI providers, data security arrangements and cross-border data transfers.
   c) Strengthen accountability, human oversight and data protection safeguards for AI-enabled electoral systems.



THE GLOBAL CENTRE FOR POLICY AND STRATEGY
(GLOCEPS)
Research | Knowledge | Influence
Runda Drive 100, Nairobi, Kenya
P. O. Box 27023 - 00100, Nairobi.
Telephone: 0112401331
Email: info@gloceps.org