KICTANet

The Power of Communities

Kenya General Elections Technology Observers mission

Pre-election Observations Report on Kenya's August 2022 Elections

6 August 2022

Kenya ICT Action Network
Email: info@kictanet.or.ke
https://www.kictanet.or.ke
Twitter: @KICTANet

Ver. 1.2

Introduction

The Kenya ICT Action Network (KICTANet) is a multistakeholder think tank that catalyses policy reforms in the ICT sector. It is guided by four pillars: policy advocacy, stakeholder engagement, capacity building, and research. KICTAnet's guiding philosophy encourages synergies for ICT policy-related activities and initiatives. As such, the network provides mechanisms and a framework for continuing cooperation and collaboration in ICT matters among industry, technical community, academia, media, development partners, and Government.

In our civic duty as active and engaged citizens, KICTANet has deployed 90 observers in 21 counties to observe the technology aspects of the elections. The KICTANet observer mission will assess the technology component covering aspects such as preparedness, the voting process, transmission, and post-election processes.

So far the KICTANet mission has: developed weekly articles on tech preparedness on elections; paid a courtesy call to IEBC commissioners; held a moderated discussion with the public on election preparedness and their expectations for the elections and shared it with IEBC; participated and presented on technology session during the 2022 National Election Conference; met with the European Union Election Observation mission; held public engagement with Meta Platforms inc, TikTok and Twitter on the emerging Concerns on social media use in the Upcoming 2022 Elections; conducted training of observers on the election process, and the technology components; and in partnership with AccessNow, and the #KeepItOn campaign, trained observers on internet measurements (OONI Probe) and use of VPNs and other tools in case of Internet Shutdowns (TunnelBear, Psiphon, Tor).

This pre-election report documents our findings on the state of elections technology preparedness and use with regard to the situation prior to the August 9 election, focusing on the progressive steps taken so far; highlighting the potential risks and challenges towards the election; and making some recommendations.

Key recommendations to IEBC and other stakeholders:

1. Provide a public API to IEBC results system, to enable observers and other stakeholders to access the database and carry out results analytics.
2. IEBC should also provide access to the results transmission portal by disclosing and publicising the URL for the portal to the public.
3. Grant observers access to back-room server operations on the processing of results forms.
4. Ensure that the use of manual registers is supported by the expected documentary evidence as per IEBC regulations (such as approvals from Presiding Officers, and completion of requisite forms).
5. IEBC should transmit and display both text results entered in the KIEMS and the scanned result forms transmitted for all the elective positions across all polling stations to enhance transparency, accountability and verifiability of the elections.

6. IEBC should publish publicly, the data protection impact assessment report and privacy policy.
7. Ensure all technologies and devices to be used in the elections are all tested prior to deployment to ensure sufficient performance.
8. Ensure comprehensive training of all election personnel well before the elections, especially on the aspects of the use of technology and devices.
9. Collaborate with electricity and telecommunications providers to ensure robust network and coverage during the elections, including ensuring that satellite backup is used in areas without 3G or 4G network coverage.
10. Incorporate cyber hygiene, digital security and privacy aspects in the curriculum used for the training of election officials.
11. Take measures to prevent vendor lock-in in the acquisition and maintenance of its technology infrastructure.
12. IEBC should respond in a timely manner to address any misinformation and disinformation targeting them.
13. IEBC should publish and publicise important information for voter education on its website and disseminate them widely including on its social media handles.
14. Social media companies should take measures to address rising hate speech, misinformation and disinformation on their platforms.

A. Progressive steps regarding election technology and technology use during the pre-election period

KIEMs Kit

- Use of KIEMS devices for capturing voter biometric details, voter identification and verification, and the transmission of results.
- Availability of enough kits for each polling station, and additional kits to provide redundancy during the elections.
- The system allows only voters registered in a particular polling station to vote only once.
- Devices enhance the efficiency of the identification of voters.
- Use of biometrics for registration stored to remove duplicity.
- KIEMS kit has both biometric and alphanumeric search capabilities and keeps records of its operations.
- IEBC has deployed 58,000 KIEMS devices across the country. There will be backup KIEMS Kits per Ward.

Internet and connectivity

- Mapping of polling stations to determine 3G network coverage. According to IEBC, the majority of the 46,229 polling stations have 3G or 4G mobile broadband coverage.
- Proposed use of satellite modems in polling stations that will help in the transmission of results in areas lacking 3G or 4G coverage.
- Internet coverage has increased in the country.

- Use of more than one telecommunication service provider for connectivity and ensure redundancy for connectivity.
- The government has given assurances that it will not interfere or shut down the internet.

Voter Registration and verification

- Mass voter registration using technology was largely successful, despite a low number of new voters registering.
- Voter register update was done, as shown in the KPMG audit.
- Use of biometric voter registration.
- Enough kits for the exercise.
- Confirmation of the distribution of voting devices.
- Provision of the voter registration status verification through the online portal (verify.iebc.or.ke) and SMS code (70000).

IT Security

- The introduction and adoption of VPNs for secure Results Transmission is progressive.
- The technical audit by KPMG was conducted which highlights the key challenges and measures implemented or proposed to be implemented by the IEBC.
- The forms have security features such as QR codes for each station.
- KIEMS kit captures logs for audit trail or polls diary.
- KIEMS kit requires password authentication and authorization by Presiding Officers at key stages of the election process.
- They have implemented digital backups with additional KIEMS kits for polling stations in case of failure.

Results transmission

- Testing of the result transmission portal.
- The proposed availability of an API to enable parties to view the results being received in the servers.
- Decision to not use the duplicate Form 34A.
- Implementation of Supreme Court decisions to improve the electoral process.
- Transmission of the result forms using the KIEMS kits.
- The 2nd trial test had a success rate of 97.59% where 566 out of 580 polling stations were able to successfully transmit results.
- Testing the technology equipment to be used during the elections is useful.

Data Protection

- IEBC has collected data of 22.1 million voters.
- IEBC has reported that it has conducted a data protection impact assessment.
- Data servers are now hosted locally at the IEBC data centres.
- IEBC has redacted the voter National ID & Passport numbers contained in the lists of registered voters published outside polling stations.

- IEBC has implemented internal controls to ensure the secure voter register as indicated in the KPMG Audit report response.

Identification of voters

- The electronic register is hosted on the KIEMS kit which aids in faster identification of voters.
- The complementary mechanism through the printed register is useful but also introduces new vulnerabilities.

Electricity and backup

- There is provision for backup power in the form of power banks for the KIEMs.
- Backup generators in case of a power outage.
- Some polling stations have electricity.

Staff capacity and training

- Training of election staff and personnel was done.
- Training of legal teams undertaken.

Voter education

- There was some voter education.
- Information and content for voters are shared on some social media pages.

Election offences

- ODPP opened a call centre to receive complaints and reports about electoral malpractices from the public.
- NCIC has been monitoring the environment for hate speech and flagged social media accounts propagating hate speech.

Inclusivity

- IEBC indicated that it has partnered with assistALL – a sign language interpreters' mobile application to disseminate voter information to the deaf community in Kenya.
- There will be staff ready to help PWDs to vote through an alphanumeric search.

Observation teams

- There are many stakeholder groups that have registered as observers.
- IEBC has accredited several stakeholder groups to observe the elections.

Social media

- Social media platforms such as Twitter, Meta and TikTok have implemented some measures to monitor and tackle misinformation and hate speech on their platforms during the elections period. These include supporting fact-checking, promoting educational content on misinformation and hate speech, dedicated links and information on the elections among others.

Stakeholder engagement

- There was engagement with stakeholders, especially closer to the elections.

B. Risks, challenges or issues of concern relating to election technology and technology use during the pre-election period

IT Security

- Increased cyber threats in the country as documented by the Communications Authority of Kenya, could potentially affect or target IEBC systems including the transmission of results or its data centres.
- The training curriculum published on the IEBC website does not include aspects on data protection and IT security e.g. on aspects such as password management and access control.
- There are potential vulnerabilities or weaknesses arising from manual methods of voter identification as compared to purely digital biometric voter identification. The audit trail around manual voter identification is not as strong as the ones provide by the biometric identification methods which automatically logs the times that non-biometric voters were identified and by who (which polling clerk/presiding officer)
- There are potential risks if the IEBC fails to publish logs from KIEMS Kits at polling stations. The logs could provide an audit trail (meta-data) about the events at the polling station in terms of what times the voters were voting, how many were identified biometrical vs manually, amongst others that shed light in case of electoral disputes.
- The release of the KPMG audit report released just a few days before the election has left little time to address all the key concerns highlighted in the report.
- The election result forms are not encrypted and digitally signed by the KIEMS device.
- Presiding & Returning Officers may forget passwords on election day etc.

Results Transmission

- Failure or delays with the results transmission system.
- Potential risks around IEBC choosing not to share the text results, but only sharing the images of the result forms. Despite the requirement for the results to be widely accessible on a public portal, IEBC will not provide summary result information to 'Wanjiku' as they did in the 2017 elections. Despite not being a strict legal requirement, it introduces opaqueness under the guise of information abundance. Specifically, the opaqueness means 'Wanjiku' is not able to verify the accuracy of the results by triangulating the information from a polling station based on the announced results at the polling station, the results form, the text results, scanned images of the result form, and final declared results by the IEBC.
- API access is yet to be provided to some stakeholders.
- The URL for the online public portal for display and transmission of election results has not yet been provided to the public, despite being tested during the simulation.

KIEMS Kit

- The Auditor-General's report for 2019-20 revealed that 392 laptops, 1,315 hard disks, 116 fingerprint scanners, 408 webcams, 1,062 USB hubs, 104 chargers and 8,041 flash disks were missing.
- Software malfunctions on the devices after the upgrade of the devices that could introduce bugs and vulnerabilities into the system.
- Biometric kits could be faulty and fail to work properly on election day, and not identify some voters.
- It is worth noting that the entire KIEMS was not subjected to a full dry-run with all the devices in operation. The first simulation exercise showed a success rate of 41% as only 1,200 out of the 2,900 polling stations successfully transmitted data. Only some 580 devices were tested during the second simulation exercise, which had a 97.59% success rate, which despite being high, does not mean the same shall be replicated during the elections.
- Software supplied by Smartmatic used in the KIEMS kits has been reported to have failed while in use in Uganda, Venezuela and the Philippines polls.
- The late procurement of KIEMS kits affected preparation for the elections.

Electronic Register

- The KPMG audit report has revealed glaring gaps in the management of the voter register. The defects and gaps in the register as identified in the audit report will affect the ability of voters to participate in the elections. The assurance that the issues from the Audit Report have been addressed is not verifiable.
- IEBC internal administrative processes have not made it easy for voters to correct or update wrong information about them in the register. For example, despite having an electronic register, voters are forced to travel back to their original place of registration to confirm and update their details.
- The re-introduction of manual register without sufficient safeguards for abuse, could introduce vulnerabilities in the voter identification process.
- Where a KIEMS kit is delivered to the wrong area, it may not be useful due to geo-location.

Voter education

- The voter education programmes especially on their online platforms started late, almost two weeks to the election.
- The programmes did not take advantage of the wide reach of the various social media platforms to target social media users, including the young population and new voters with relevant content.
- There is still limited information dedicated to voters' education on the IEBC website and its social media handles such as on Instagram, Twitter and Facebook for example.
- The IEBC has not utilised paid advertisements on social media platforms to proactively increase access to and availability of information that targets voters.

Data protection

- Data protection impact assessment has not been made public.
- IEBC has not published a data protection policy or notice.
- The increase of the use of spam messages sent to the mobile number of voters irregularly obtained by political candidates. Thus, many political candidates are spamming voters with very targeted, unsolicited campaign messages that indicate abuse of voter data.
- The KPMG audit report identified several gaps in regard to the management of the personal data of voters, some of which IEBC indicated it will not be able to address before the election.

Internet and Connectivity

- 1,272 polling stations out of 46,229 have no 3G or 4G mobile broadband coverage coverage
- Communication network failures or disruptions e.g. the fibre cut or poor network signals during the simulation could still present problems during the election.
- Poor internet access especially in remote areas could result in delays in the transmission of results.
- The reliability of satellite modems was not established during the simulation exercise.
- The possibility of an internet shutdown or disruptions during the election period could affect the flow and access to information, including the transmission of results.

Staff capacity and training

- Inadequate staff training on the KIEMS with limited time and opportunity to learn and familiarise themselves and gain experience with the operations of the device and the system. This could affect their capacity to effectively use the devices on election day.
- The recruitment and training of election staff started late.
- The unfamiliarity of the technology used.
- Ensuring effective technical support across all polling and tallying centres.

Electricity and power backup

- Lack of electricity supply in all polling stations.
- Power outages in the polling station could affect charging of KIEMS and power banks, as not all polling centres have backup generators.
- The KIEMS device battery life cannot sustain operations for an entire day.

IEBC Website

- The IEBC website (www.iebc.or.ke) continues to experience regular and intermittent downtime meaning users cannot access information from it, as and when required.
- The website and social media channels (Instagram, Facebook and Twitter) had limited information on the elections and were not regularly updated with up-to-date and comprehensive information on the upcoming elections targeting new and previous voters, until a few days before the election.
- Some of the information was not presented in accessible formats or languages to ensure greater inclusivity and access by ordinary citizens, including persons with disabilities, marginalised and minority groups.

Social media

- There has been use of social media platforms to spread hate speech, misinformation and disinformation including on the IEBC and the upcoming elections. The key perpetrators include politicians and other organised politically affiliated groups.
- There is little if any evidence that state security agencies have been successful in curbing misinformation and hate-speech flows on social media networks.
- Social media companies have not invested and taken sufficient steps to detect, reduce and prevent hate speech, misinformation and disinformation on their platforms.

Suppliers

- There have been several controversies surrounding the elections software provider Smartmatic, which have not been sufficiently addressed.
- IEBC has not effectively addressed concerns around vendor lock-in, especially with previous vendors (Idemia) affecting the ability of the new vendor (Smartmatic) to transfer and integrate all information from the electronic database which was developed by Idemia.

Observers

- The online portal for observer accreditation was slow and sometimes non-functional and offline.
- There have been delays in printing and accessing observer accreditation badges.
- The observers have not gained access to observe the back-end server operations of the IEBC for results transmission.
- These factors have affected the ability of observers to access key location and information prior to the election.

Ends/