



# Beyond the Card Reader:

## Elections Rigging as an Emerging National Security Threat in Nigeria

ISSN 0794-4152

AfriHeritage Policy Brief No. 12 /October, 2017

### Executive Summary

This paper offers an evaluation of the existing technological strategies introduced into the Nigerian electoral process to address the problem of electoral malpractices and fraud affecting the quality of elections. The paper answers the following questions: (i) Are technological devices really fit for the purpose for which they were introduced? (ii) In what ways have the technological devices improved the quality of elections in Nigeria? (iii) Is Nigeria technically ready and able to manage effectively electronic devices that have the potential of being used to unleash massive electoral fraud that could completely undermine peaceful coexistence within its fragile and sensitive electoral context? Following the findings of a larger study, which identify many challenges surrounding the use of electronic devices in the electoral processes of other countries, the paper provides a set of policy recommendations on how to ensure the effective mobilisation of high technology devices towards improving the credibility of elections in Nigeria.

### The Issue: Electoral Fraud and the Introduction of Technological Model

Since the democratic transition in 1999, Nigeria's elections have been associated consistently with assorted stories of fraud and related malpractices. Basically, election results commonly failed to reflect the popular wishes of the people. Increasingly, this has contributed to a general lack of confidence by the public in electoral processes and the institutions governing them. In many instances, the controversies generated in the post-election period have often led to incidents of large-scale violence, which have consumed many lives and property over the years. Thus, the problem of electoral fraud and stolen

election franchises have produced three major problems for both the society and the state:

- The political officeholders who emerge from the process struggle with a certain legitimacy burden;
- Because officeholders often assume office without credible support, many often feel unconcerned about building bridges within their constituencies; and
- A negative impact results on governance from the dissonance due to the combination of lack of legitimacy, arrogance about needing support to remain in office, and (sometimes) the need to spend significant amount of financial resources and time in a legal fight to remain in office.

Thus, in a bid to address the nagging problems, the Independent National Electoral Commission (INEC) under the administration of Attahiru Jega initiated bold efforts to reform the system. In line with emerging trends around the world, INEC sought to stop electoral fraud by deepening modernizing efforts (previously initiated but poorly pursued by Maurice Iwu's administration) through the introduction or strengthening of new technologies in the electoral process. The idea was to prevent electoral fraud, reduce electoral disputes, encourage voter participation and, ultimately, improve public confidence in the electoral process. It deployed the Automated Fingerprint System (AFIS), the Permanent Voter Cards (PVC), and Smart Card Reader (SCR) technologies.

### The Successes, Problems and Challenges of Electronic Devices

The 2015 general elections provided a useful platform for the assessment of the technological devices introduced by INEC. The study revealed that

Nigerians generally concluded that the quality of the elections improved following positive ratings by different groups of election observers; so, they readily accepted the results. Many experts and practitioners believed that the PVCs and SCRs helped to reduce the incidents of election rigging as systematically perpetrated previously by politicians. In addition, it was observed that the strategies made accreditation less cumbersome and more transparent, and provided backup information that could assist in electoral adjudication, should they occur.

Also, it cannot be disputed that the digital procedures (as with other countries that digitalized voting systems) provide mechanisms to save costs and facilitate faster electoral processes than the manual ballot card processes. However, despite the usefulness of the technological devices, there were strong evidences that the 2015 Nigerian elections were not entirely free of rigging and other forms of manipulations. This was encouraged by the technical and logistical problems encountered by INEC, which necessitated recourse to manual accreditation in some polling units.

The digitization exercise, notwithstanding, there were many cases of manipulations and fraud due to several factors including:

- Poor attitude and inadequate training on handling the SCRs;
- Poor technical readiness and inadequate on-field experiences on the use of the SCRs by elections staff;
- Inadequate security for the SCRs against subterfuge or sabotage by some election officials;
- Illegal abuses of PVCs by election officials and proxies; and
- Data mismatch that compromised the biometric data and the true identity of voters.

In essence, the 2015 electoral outcomes showed the vulnerability of electronic devices to criminal manipulation. So, contrary to the conclusions of Nigerian officials and citizens, the elections actually demonstrated the need for wariness in embracing electronic devices fully. Electoral processes can be manipulated or rigged electronically before, during, and after elections. This is because they have many demonstrable strike points of vulnerability with respect to: machine or software tampering; chain voting and impersonation; rigged tabulation; and outright fraud through electronic misrepresentation of vote counts. Indeed, some experts argue that most challenges associated with the Optical-Scan Paper Ballot (OSPs) SCRs and the Direct Recording Electronic (DREs) SCRs can be moderated or prevented altogether through various means such as introducing a cryptographic verification mechanism.

However, there is overwhelming agreement by security experts that all electronic voting devices can be easily rigged not only through external hacking but also through hacking by insiders such as government officials, hardware makers, and software producers. Due to such concerns, several countries are beginning to re-assess their use of electronic devices with a view to either discard them altogether or strengthen the management and integrity of the system. For instance, Ireland, Netherlands and the United States have either banned, suspended, or allow only limited use of electronic voting devices.

Nigeria embraced the technological model because it provides the country's electoral system with a measure of credibility and transparency. However, should those positives trivialize its vulnerability to massive fraud? Should technologically poor or socially divided countries with highly contested political systems such as Kenya, Nigeria, South Sudan or South Africa embrace such systems without due regard to the prospect that massive election rigging may not only undermine electoral credibility but also could lead to devastating pre-election or post-election violence? The commotions surrounding the manipulations of the 2016 and 2017 elections in the US and Kenya, respectively, are instructive.

If America, Russia or other such powers can target and manipulate the electoral processes of rival technological powers, a comparatively weak country such as Nigeria must be especially wary and vigilant. Nigeria's electoral processes are not safe from manipulation by its own officials or those of foreign governments, producers of electronic devices, or makers of electronic software.

Clearly, the presumption of technological inevitability regarding electoral devices is premature now -- even if it is adjudged to anticipate the future of democratic elections. But before that can happen, care must be taken to ensure that electronic devices do not destroy the development and the deepening of the values that underpin democracy by undermining electoral processes.

## Policy Recommendations

- The electoral processes and the associated equipment should be formally regarded as national security matters. As such, appropriate laws should be put in place to govern the use and handling of electoral devices.
- The use of smart card readers and other technological devices should be revisited formally with a view to identify and vet all crucial issues around their deployment and implications for the electoral system, democracy and the national security of Nigeria.
- The adoption and introduction of technological devices for Nigerian elections should entail (at minimum) the development of a strong pool of formally certified skilled experts in all areas pertaining to such devices including equipment design and assessment, and software development and monitoring.
- All experts involved in the use and monitoring of the devices must undergo certification and periodic recertification processes including appropriate tests, assessments, and clearances to handle, evaluate, and work with such equipment and software.
- Procedural enhancement for election practitioners is critical for ensuring orderly processes and national security. Stringent rules on qualification and disqualification should be put in place to govern all candidates and legal practitioners.
- To ensure transparency in the system, it is crucial that all information related to elections -- from the pre-election to the post-election periods -- should be regularly updated on the website of INEC and made available for easy accessibility to the public. Most importantly, the accredited voters and their polling units and results of elections at each polling unit should be officially available in media platforms of INEC as they are counted.
- Efforts should be made to ensure additional layers of protection of election processes by enabling the involvement of civil society organizations in monitoring electoral processes and reporting fraudulent actions.
- The stakeholders involved in the electoral process such as INEC, political parties, the media, and civil society organizations should be enabled to educate the public properly about the voting processes and the use of enabling technologies.

