DOI: 10.20940/JAE/2023/v22i2a4

TECHNOLOGY, CYBER SECURITY AND THE 2023 ELECTIONS IN NIGERIA

Prospects, Challenges and Opportunities

Robinson Tombari Sibe and Christian Kaunert

Robinson Sibe is Visiting Research Fellow, University of South Wales, Lecturer in Computer Engineering, Rivers State University, Nigeria, Adjunct Lecturer in Cyber Security, National Open University of Nigeria and co-founder of Digital Footprints Nig.

Christian Kaunert is Professor of International Security, Dublin City University, Ireland Professor of Policing and Security, University of South Wales and editor of the Journal of Contemporary European Studies, and European Politics and Society

ABSTRACT

Nigeria's Electoral Act 2022 legitimises the use of technology in different aspects of the electoral process. The steady increase in technology adoption in the electoral process continued in 2023, after successful pilots in the Anambra, Ekiti, and Osun state elections. This article investigates how technology has been deployed to conduct elections in Nigeria, comparing it to other jurisdictions, notably Estonia. This study adopts a qualitative case study approach, synthesising expert views and reviews from the available literature, official documents, and press releases to produce emergent themes. The article considers the emerging legal, regulatory, and technical concerns from both a scholarly and industry perspective. The article also examines potential risks, such as reliability issues, cybersecurity concerns, gaps in technological capability, information governance and data protection concerns.

Keywords: e-voting; emerging threat landscape; electoral integrity; electoral management; cybersecurity; election technology; INEC

INTRODUCTION

Elections are an essential aspect of the democratic process. Over the years, a significant challenge facing elections has been the need to ensure the credibility of

the electoral process. Therefore, electoral bodies are saddled with the responsibility of ensuring free and fair elections. The last two decades have heralded an increase in the global adoption of technology in elections. This has been highly visible, particularly in Africa, with about half of all national elections conducted on the continent now employing the use of technology in critical aspects of the electoral process, such as biometric registration, voter verification, and electronic transmission of results (Cheeseman et al. 2018).

Nigeria has a long history of elections fraught with rigging, and for years there have been demands for reforms to ensure credible elections. These demands led to the introduction of technology in the electoral process to improve the quality and integrity of the electoral process (Agbu 2016). INEC, Nigeria's Independent National Electoral Commission, has has been commended for the introduction of technology in elections, resulting in improved quality of elections in Nigeria. For instance, Enwere and Ladan-Baki (2015) argued that using Smartcard addressed the challenge of rigging and multiple voting. Agbu (2016) posited that the use of technology in the 2015 elections made it difficult to manipulate electoral figures, citing the transparency of technology as an essential feature in credible elections.

Despite the positive contributions of technology to the quality and integrity of the electoral process, it has not been without attendant debates and controversies. For instance, at the beginning of the 20th century, Allen (1906) argued that the mechanical voting machines used in Rochester, New York, in 1902 undermined the provisions of the electoral law. In Kenya's 2013 general elections the electoral body deployed technology which led to widespread failure, with many technical challenges (Ali 2015). Alebiosu (2015) documented some of the challenges experienced using biometric technology in Nigeria's 2015 elections, including reliability issues, equipment failure, and user challenges. Sibe (2015) argued that the 41% failure rate of the biometric process reported by INEC in the pilot test of the Smartcard reader technology in 2015 (Adebayo 2015) was too significant to ignore, yet INEC went ahead with the same technology in a national election.

Over and above these challenges, the emerging electoral threat landscape has thrown up a new kind of risk, which is becoming a major concern. The increased digitalisation of core electoral processes accentuated cybersecurity threat. For instance, just before the 2015 Nigerian presidential elections, the INEC website was attacked and defaced by a hacktivist group identified as the Nigerian Cyber Army (Abimboye 2015). In the 2022 gubernatorial elections in both Osun and Ekiti states, the INEC chairman also reported several cyberattacks on the INEC Result Viewing Portal (IReV). These attacks were of international dimensions, some of which originated from Asia (Ufuoma 2022). In the recently concluded February 2023 presidential election, Nigeria's Minister of Communication and Digital Economy announced that the country

had experienced a total of 12 988 978 cyberattacks days before and during the election (Michael 2023). These attacks originated both within Nigeria and externally. Therefore, the manipulation of election results by cybercriminals and foreign elements is technologically possible, and a major concern.

In 2022, INEC announced the use of the Bimodal Voter Accreditation System (BVAS) as the technology to be used in the 2023 presidential election. BVAS uses fingerprint verification and facial recognition technology (INEC 2022a). The BVAS system has been deployed in at least three mid-season elections as a pilot test, and despite some concerns, initial feedback was promising (Munya 2022; Agiri & Morka 2022). The Commission announced the deployment of over 200 000 BVAS units for the 2023 general election (*The Guardian* 2022). The Electoral Act 2022 has also added a layer of legitimacy for INEC to use any technology they deem appropriate, which gave the Commission impetus to stay with the BVAS. Amidst this optimism, there were concerns, particularly about technical challenges and the emerging threat landscape.

This article examines how technology has been deployed in Nigeria and other jurisdictions to conduct elections. The paper investigates some of the challenges in technological deployments in previous elections in Nigeria and other jurisdictions, captured by Alebiosu (2015), Cheeseman et al. (2018), and Munya (2022). The article considers the emerging legal, regulatory, and technical concerns from both a scholarly and industry perspective. The article also examines some potential risks in the emerging threat landscape, such as cybersecurity concerns, low adoption rate, gaps in technological capability, information governance, and data protection.

RESEARCH METHODOLOGY

This article investigates the emerging challenges of technological deployments in elections, structured as a qualitative case study. When investigating a relatively unknown phenomenon, a qualitative study is usually appropriate if there are sufficient resources for review (Hancock & Algozzine 2017). It is an exploratory approach, which allows for a phenomenon to be studied within its context. A qualitative study allows for data from multiple sources to synthesise wide perspectives and allows for an in-depth investigation.

The paper reviewed over 250 sources, including papers from peer reviewed journals, official press releases, reports, election observer reports, newspaper articles, and official websites. Various papers reviewed highlighted Estonia as a pioneer in electronic voting (the first to adopt i-voting in a national election in 2007) and one of the most advanced countries in terms of technological deployment in election and in e-government generally (Heiberg et al. 2011, September). Estonians have used the electronic voting system in four national elections, three European

Parliamentary elections, and four nationwide local elections between 2005 and 2019 (Ehin et al. 2022). Also, the country's voting system has been robustly studied and analysed, examining themes such as efficiency, transparency, security, and auditability (Nurse et al. 2017; Heiberg et al. 2011, September).

A major step in qualitative case studies is the determination of a case, and this study adopted Estonia as the case, and compared the findings on technology deployment in elections in Estonia with those from Nigeria. The choice of Estonia was predicated on their leading role in electronic voting, as corroborated by several scholarly and industry sources presented in this study. Estonia was the first country to conduct electronic voting on a national scale. Their voting system has been robustly interrogated and has recorded consistent gains for over 15 years. Eleven themes emerged from the literature review and were hand coded. These emergent themes from literature showing key features of technological deployment in election are presented in the next session.

TECHNOLOGY DEPLOYMENTS IN ELECTIONS

Emergent Themes from Literature

Although there are several voting technologies available, there are common features in different implementations. The key themes that emerged from the available literature are summarised and presented below, and will be used to evaluate the case study implementations of Estonia's iVoting system and Nigeria's electoral technological deployments.

- *Correctness*
  A voting machine should correctly count votes. All technologies deployed in an election should be correct and accurate. Several of the papers reviewed corroborated this position. For instance, Cortier and Wiedling (2017) noted the need for election technology to be correct and accurate. If stakeholders have no trust in the accuracy and correctness of the election technology deployed, they will challenge the outcome, particularly if this is unfavourable.

- *Legal and Regulatory Framework*
  Deployment of technology in the electoral process must derive legitimacy from an underlying legal framework that recognises and supports its operations. This is because elections are rooted in constitution and law, therefore any technology used should not be in violation of the enabling laws and legislations. Several papers and articles reviewed supports this position. For instance, Shchebetun et al. (2020) and Sibe (2015) reinforced the need to ensure that technological deployments are within the legal framework.

- *Mirrors Traditional Voting*
  An electronic voting system should be designed to have the same objectives and criteria (such as security and anonymity) as the traditional system (Martens 2011). Therefore, whatever technology is to be deployed should reflect and automate the procedural flow and objectives of the manual system.

- *Voter Anonymity*
  An important feature of a voter system is voter anonymity. This is important so that voters can freely elect their choice without any fear or coercion. A voting system should protect the identity of the voter. Several authors, such as Ayed (2017) recommended the need for a voting system to protect the anonymity of the voter.

- *Cybersecurity and Privacy*
  One of the major emerging risks of an electronic voting system is that of cybersecurity attacks. Private and even nation-state attacks have increased over the years, targeting both corporate and critical national infrastructure. Also, since voting is a people-centric process involving the capture and storage of Personally Identifiable Information (PII) of millions of citizens (during registration), there is an emerging risk of data breach. For these reasons and because of the sensitivity of elections, an electronic voting system is a natural target for cyberattacks. Several scholars such as Yavuz et al. (2018, March) emphasised the need to install necessary controls to ensure that cybersecurity risks and privacy concerns are mitigated in a voting system.

- *Transparency*
  Elections are a multi-stakeholder activity involving several parties and citizens. Therefore, the automation of an electoral process must be seen to be transparent. Several sources reviewed, such as Cheeseman et al. (2018) noted that the voting system must be transparent for voters to have confidence in the system.

- *Trust*
  For citizens to accept the outcome of elections, they must trust in the voting system. Several scholars outlined this as a major requirement of a voting system. For instance, Garnett and James (2020) submitted that election technology should be designed and deployed in a manner that engenders citizen trust.

- *Audit and Verification*
  Competing interests in elections could challenge the process, particularly

when the outcome is unfavourable to them. An important feature should be the ability to audit the process end-to-end, and to verify votes cast in order to build trust and confidence in the election technology deployed. Several scholars such as Chaum (2009) submitted that voting systems should be auditable and votes should be verifiable.

- *Reliability*
  Any failure of a voting system or election technology could prove catastrophic. Therefore, it is important that any election technology deployed should go through robust reliability tests to ensure the effectiveness and efficiency of the system. This theme emerged from reviews of Yavuz et al. (2018, March) who submitted the need for a robust reliability test for any election technology.

- *Stakeholder Engagement*
  Elections are a multistakeholder process. Therefore, any technology deployed must have the buy-in and acceptance of the stakeholders. Several scholars, such as Adeshina and Ojo (2020) submitted that for an election technology to be accepted, there must be a robust stakeholder engagement. Such robust stakeholder engagement will present the technology to stakeholders and introduce key features such as transparency, reliability, efficiency, and security.

- *Pilot Tests*
  Pilot tests are usually best practice in large-scale technology deployments. This allows for the testing of such technology in a controlled environment where the variables can be better managed. Election deployments are large-scale technology deployments; therefore, it is a good practice to test any election technology in smaller elections or in mock elections to check for the reliability of the system, end-to-end. Several scholars, such as Adeshina and Ojo (2020), Sibe (2015), and Alebiosu (2016), all submitted that electoral technology should be robustly tested in a controlled environment. Pilot testing allows for reliability verification with minimal impact.

CASE STUDE – ESTONIA

Estonia was the first country to carry out nationwide internet voting during the March 2007 national parliamentary election (Heiberg et al. 2011, September). In the last 15 years, Estonians have used the electronic voting system in four national elections, three European Parliamentary elections, and four nationwide local elections (Ehin et al. 2022). It is noteworthy that the concept of e-voting for Estonia is different from what may be obtained elsewhere. While others used the

term to describe the process of deploying technology in the voting stations, the focus of the Estonian e-voting process was to allow for remote voting through the internet (Maaten 2004). This informed why it is also generally referred to as i-voting (internet voting). To vote electronically in Estonian elections, the voter needs a secure computer with an internet connection, an ID-card with a reader, or a mobile ID (Estonian National Electoral Committee (NEC) 2022). Public acceptance in Estonia for the electronic voting system got off to a slow start, but this would improve later. When it started in 2005, only about 1.9% of votes were cast using the internet voting system. As of the 2015 parliamentary elections, this had increased to 30.5% of the votes cast. By 2019, this had risen to 43.8% (ibid.). This growth shows a sustained level of adoption and user acceptance.

Legal and Legislative Framework

Before e-voting was fully operational in Estonia, the necessary legal and legislative framework was put in place (Maaten 2004). This legislation relied on previous acts for effective implementation. For instance, the Identity Documents Act of 1999 evolved to provide digital identity cards with complex functionality for digital identification through mobile-ID. The Digital Signatures Act 2000 legitimised legally binding digital signatures. Also, the Population Register Act and Personal Data Protection Act are essential legislations in the overarching legal framework on which the Estonian e-voting law depended (Ehin et al. 2022).

Like every voting system, there have been legal contestations regarding legitimacy and validity. Over the years, Estonia's courts have made pronouncements on the legality of the Estonian e-voting stem. For instance, in judgments 2011, 2013, and 2017, the Supreme Court of Estonia ruled that the Estonian elections followed legal provisions, and no major incident undermined the process. Therefore, Estonians continue to use the i-voting system for nationwide voting, and the increasing number of voters using i-voting indicates the rising level of adoption and user acceptability.

The Estonian Electronic Voting System

Estonia's e-voting system has important features that ensure both the verification of voters and voter anonymity. To ensure voter anonymity, the e-voter application encrypts the citizen's vote with a public key and signs the result digitally. The system utilises two envelopes: an inner envelope containing encrypted votes and an outer envelope from which the voters' list is compiled. The inner envelope with the encrypted votes (ensuring that the voter cannot be identified) is forwarded for actual vote counting using the system's private key. Tsahkna (2013, p. 62) noted

that to ensure the privacy of voters, the system provides that at no time 'should any party of the system have both the digitally signed e-vote and the private key of the system'.

The system ensures that the encrypted votes with personally identifiable information are separated before the declaration of the result on the evening of election day. That is, the inner envelope must be separated from the outer envelope; otherwise, the system will not open the votes. To ensure that people do not take advantage of both traditional and e-voting channels so as to vote twice, the system is designed to ensure that only one vote is counted. A list of all internet voters is printed and sent to polling stations two days before the election. This is checked at the polling stations to eliminate the possibility of people voting both ways. Where this is the case, the internet vote of that citizen is cancelled with a note on the e-voting system (Martens 2011).

Privacy and Cybersecurity Concerns

Despite its high praise, the Estonian e-voting system has not been without criticism. Concerns about breaches have led to greater scrutiny through observations, code reviews, and adversarial testing of the voting system components (Nurse et al. 2017). Some criticise the security of the system, arguing that this should depend on the technical measures implemented rather than on the hope that officials will act professionally. After Estonia's 2011 elections, Heiberg et al. (2011, September) published findings identifying new vulnerabilities in Estonia's electoral system, called 'Student attack'. A student had written malware that compromised Estonia's electoral system. The Estonian NEC made some improvements, adding modules to verify votes. Despite this improvement, Springall et al. (2014, November) submitted that the system had both procedural and architectural weaknesses, leaving a potential vulnerability for hackers to alter the outcome of an election. The issues identified include procedural controls, lax operational security, insufficient transparency, and vulnerabilities in the published application code. Springall et al. (2014, November) argued that the Estonian internet voting system does not have end-to-end (E2E) verifiability. Instead, its simplistic model means trust is conferred on the integrity of voters' computers, server components, and election staff. To prove the integrity of the voting system, the Estonian electoral body relied more on procedural controls than technical means. Yavuz (2018) also observed that the centralised structure of the Estonian electronic voting system creates a single point of failure and is vulnerable to malicious software and hackers. Also, there is a potential challenge of scalability. Estonia is a relatively small country and replicating the Estonian electronic voting model might prove daunting for large nations. Nurse et al. (2017) noted that the various concerns raised suggest

vulnerabilities that malicious insiders and sophisticated external attackers may capitalise on to compromise the voting system.

The ability to audit an election process is crucial to its acceptability. Estonia's internet voting system does not have a full public server-side function. However, Ehin et al. (2022) and Nurse et al. (2017) noted that Estonia employed designated auditors to verify the process's integrity, much like traditional elections. Also, the system's mixer and decryption server components use cryptographic proofs that can be relied on for independent verification. In addition, to boost transparency and trust in the system the authorities released the source code running the i-voting platform, except that of the official voting application, which is not released as a defense mechanism (Ehin et al. 2022).

TECHNOLOGY IN NIGERIAN ELECTIONS

The Fourth Republic (1999 to Date)

Nigeria has a long history of poorly organised elections, with allegations of rigging and many documented accounts of election malpractice (Enwere & Ladan-Baki 2015). Studies have suggested that this widespread malpractice continued due to the manual methods used in the process (Jibia & Zake 2020), culminating in calls for the total reform of the electoral system in Nigeria. A direct outcome was the decision to deploy technology to ensure the quality and integrity of the electoral process (Jega & Hillier 2012). This study summarises technological deployments in Nigeria's elections with the timeline indicated in Figure 1. The paper will focus on the newest technological addition.

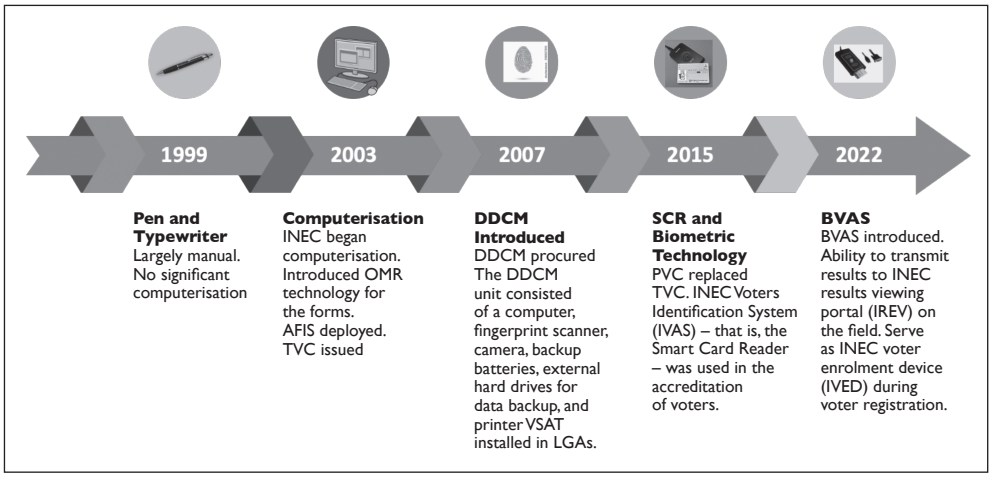


Figure 1: **Timeline of technological deployments in Nigeria**

Bimodal Voter Accreditation System (BVAS)

The smart card reader introduced in the 2015 elections did record remarkable successes. However, as this article has shown, there were also many shortcomings. In addressing this, INEC introduced the BVAS. It is an all-in-one multifunctional integrated device serving different functions in the electoral process (Munya 2022). It verifies the authenticity of the Personal Voter Card (PVC) and fingerprints and has facial recognition technology, which it uses during the accreditation process. Another important feature is the ability to transmit unit results to the INEC Results Viewing portal (IReV) on the field. It is also used as the INEC voter enrolment device (IVED) during voter registration (Agiri & Morka 2022). The two-factor (finger print and/or facial recognition) verification option of the BVAS is expected to eliminate the use of incident forms.

The introduction of BVAS has not been without its challenges. For instance, Odalonu and Ogu (2022) noted that there were 'severe challenges' with the new BVAS in the Anambra Governorship elections. The Transition Monitoring Group (TMG) also observed the presence of the BVAS challenges and urged INEC to fix them before the 2023 elections (Ileyemi 2021).

TECHNOLOGICAL CHALLENGES AND PROSPECTS IN THE 2023 ELECTIONS

INEC (2022) recently adopted new technologies for elections – BVAS, the INEC Voter Enrolment Device (IVED), and INEC Results Viewing Portal (IReV). These innovations look quite promising in improving the quality of elections in Nigeria. However, like any innovation, there are emerging risks and challenges. This section assesses these risks and makes recommendations and identifies the following themes and sub-themes from peer-reviewed journals, reports, expert analysis from newspapers.

Legal Framework

Elections are governed by legislation. The Nigerian Constitution 1999 (as amended) gives INEC the mandate to conduct elections. The Electoral Act 2022 prescribes how elections are to be conducted in Nigeria. E-government (and by extension, emerging technologies in the electoral process) must derive legitimacy from an underlying legal framework that recognises and supports its operations (Sibe 2015). Therefore, for technology to be deployed in a public-centric process like elections, it is important to have a robust legal framework that establishes its legitimacy. One of the challenges faced with introducing the smart card reader

in 2015 was that the applicable law appeared not to recognise its operations. The many post-election litigations around this issue corroborate this fact. This trend necessitated the passage of the Electoral Act 2022, which is a commendable step. The following themes are discussed under legal challenges:

Electoral Act 2022

The Electoral Act 2022 is the primary legislation regulating the conduct of elections in Nigeria. The previous Electoral Act 2011 did not seem to consider the involvement of hi-tech, and left loopholes that could be exploited legally and technically. The Electoral Act 2022 addressed some of the concerns raised in 2015 and legitimised technological innovations deployed by INEC for smooth elections in line with global best practice and industry trends (Sibe 2022).

This section examines some key sections where the Electoral Act 2022 refers to technological involvement. Section 41(1) gave the Commission the mandate to provide suitable boxes, electronic voting machines, or other voting devices for conducting elections. Section 47(2) requires the presiding officer to use a smart card reader or any other technological device prescribed by the Commission to verify, confirm, authenticate, and accredit voters. Section 50(2) states that subject to Section 63, voting at an election and the transmission of results shall be in accordance with the procedure defined by INEC. Section 62(2) gives the Commission the power to maintain a centralised electronic register of voters for collation.

From these sections of the Electoral Act 2022, the following sub-themes emerged as technological possibilities:

1. Electronic voting machine
2. Smart card reader or any other technological device
3. Result transmission
4. Centralised electronic register
5. Collation.

Apart from the first and last sub-themes (electronic voting machine and collation, which were done manually), the remaining three sub-themes were used by INEC in the 2023 national elections. INEC used the BVAS for voter verification as well as electronic transmission of votes. Notably, the Electoral Act 2022 did not make it mandatory for INEC to use any of these but merely gave them the power to decide which technology they deem fit. In their guidelines for the 2023 elections, INEC repeatedly insisted that the BVAS will be strictly adhered to for the accreditation of voters and electronic transmission of votes directly from the polling units

(INEC 2022b). Also, while INEC clarified that collation will be done manually, the Commission announced that results will be published centrally on the INEC Results Viewing Portal (IReV) (Anichukwueze 2022; *Premium Times* 2022). Despite these assurances, there were widespread reports of failed electronic transmission of results from the polling station. This failure was an important aspect of the BVAS and IReV promised by INEC (Ochei 2023; Ejiofor 2023a).

Jurisdictional Complexities

The new electoral technological landscape also comes with emerging challenges such as cybersecurity threats. With technological involvement in almost all aspects of the electoral process – voter registration, identification, verification, and collation – there are real possibilities of a cybersecurity attack. All the technologies deployed by INEC (2022b) are possible targets for cybercriminals with a real threat of both local and foreign interference in elections. Cyberattacks, whether in elections or in any other process, can be classified as cybercrime (Nigeria's Cybercrime Act (2015)). One of the challenges with cybercrime is the cross-border implications of its borderless nature. The fact that criminals could potentially commit cybercrime in one country while operating from another country presents complex jurisdictional roadblocks to law enforcement agencies and cybercrime investigators (Interpol 2017; Sibe 2021). This potential threat has crystallised in recent elections. For instance, in the Osun and Ekiti elections respectively, cyberattacks from Asia were directed at the INEC website (Ufuoma 2022). Also, the Ministry of Communication and Digital Economy reported over 12 million cyberattacks during the 2023 presidential election. These attacks originated both from within and abroad, from other countries (Michael 2023).

It is noteworthy that offences under the Cybercrime Act (2015) are extraditable. Section 51 of the Act gives the Attorney General of the Federation the powers to request or receive assistance from a foreign state or authority for the investigation of offences under this Act. Nonetheless this could prove more complex and complicated than the letters of the Act suggest (Interpol 2017). Given these complexities, investigating and prosecuting electoral cybercrimes with an international dimension could prove daunting.

Forensic Readiness of the Justice System

The justice system plays an important role in the electoral system. The Electoral Act 2022 allows dissatisfied candidates to take their cases to court. With the growing involvement of technology, most of the evidence would be in digital form or from digital devices. Nigeria only allowed for the admissibility of digital

evidence with the passage of the Evidence Act 2011. There are predictable gaps in understanding technical concepts and in the forensic readiness of the justice system (Sibe 2021). For technology to play a much-desired critical role, the justice system needs to be forensically ready, with the ability to understand the delicate complexities of digital evidence.

Data Protection

National elections are a data-centric exercise. As of the 2019 elections, INEC had 84 million registered voters. With the recently-concluded voter registration exercise, this is estimated to have risen to about 96 million (Amata 2022). Having such a large citizen record with Personally Identifiable Information (PII), INEC faces the potential risk of data breaches and other information governance challenges. The reported attacks on INEC's results viewing portals in the Osun and Ekiti elections of 2022 and the national elections of 2023, is an indication of the possibility of data breaches involving PII (Michael 2023). This is even more so given Nigeria's emerging cyberthreat landscape. In a recent survey on Enterprise Security Trends in Nigeria commissioned by Microsoft (2022) and conducted by International Data Corporation (2022), data breach was seen as the top cybersecurity concern by Nigeria's chief information officers (CIO). Therefore, with the datacentric nature of INEC's operations, there is real concern about data breach.

In 2019, the Nigerian Information Technology Development Agency (NITDA) released the Nigerian Data Protection Regulation (NDPR). The NDPR seeks to regulate the collection and processing of personal data. As a major data-centric organisation, INEC faces the potential compliance risk of breaching the NDPR, as the newly-created Nigerian Data Protection Bureau has been investigating data protection breaches and penalising defaulters (*The Guardian* 2023a). Also, the Nigeria Data Protection Act 2023 has just been passed, giving the NDPR more legal and operational impetus. Therefore, to mitigate this risk, INEC needs to take technical steps to ensure the protection of citizen information.

Technical Issues

In evaluating the possible issues and challenges that INEC faced in the 2023 elections, the following sub-themes emerged:

Reliability Issues

One of the challenges faced during the deployment of technology in elections is that of the reliability of the technology deployed. For instance, Cheeseman et al. (2018) noted the multiple failures in verification devices for thumbprints in

Ghana's 2012 general elections. In Kenya's 2013 elections widespread failure of electronic voter identification kits was reported in over half the polling stations. Ali (2015) also corroborated this, citing the widespread failure of scanners, failed verification, crashed central servers, and others.

Nigeria also has a history of technological failures in elections. In the 2015 elections, there were widely reported cases of the failure of the smart card reader. Alabiosu (2016) noted that all five biometric card readers deployed to the serving president's unit failed. The rollout of BVAS has also not been without attendant challenges. For instance, Odalonu and Ogu (2022) reported technical challenges in the Anambra governorship elections. This also happened at the Ekiti and Ogun governorship elections (Iliyemi 2021).

In the 2023 elections, there were reported cases of failed BVAS. For instance, in Rivers State, the BVAS failed to accredit the wife of the governor, thereby disenfranchising her (Jaiyeola 2023). After the presidential election on 25 February, and despite its earlier claim that the BVAS has passed reliability tests, INEC admitted to glitches with the BVAS which it promised to improve in subsequent elections (*Vanguard* 2023). This was also corroborated by Okeaya-inneh (2023) and the International Centre for Investigative Reporting (2023), who both noted that voters complained of failed BVAS in certain polling units.

Various major election observer groups also made statements corroborating issues of reliability with the technology deployed. For instance, the European Union Election Observation Mission to Nigeria (2023) noted that while the introduction of the BVAS and IReV raised citizens' hopes, on election day there were failures with the electronic transmission of results, particularly for the presidential election result. The Commonwealth Election Observer Group to Nigeria (2023) noted that while the BVAS functioned satisfactorily in most polling stations, there were also notable problems. The report showed that the BVAS's facial recognition function was more efficient than the fingerprint verification. This was corroborated by a joint statement by the international observation mission of the International Republican Institute (IRI) and the National Democratic Institute (NDI) (2023), which observed that while the BVAS functioned properly, the fingerprint verification appeared less effective than facial recognition. Enough is Enough Nigeria (2023), a civil society organisation, also echoed the frustrations of citizens because of malfunctioning BVAS.

Electronic Transmission of Results

The Electoral Act 2022 provided the legal basis for the electronic transmission of votes. There are many risks associated with the electronic transmission of votes. For instance, the potential risk of network failure, as recorded in the case of Kenya, where the server collapsed under heavy network traffic (Munya 2022). Ali (2015)

noted that the central server, which was supposed to store results from 33 400 polling stations through SMS, collapsed under the strain. Beyond this, there are also other emerging risks associated with electronic votes transmission, such as cybersecurity risks (interception and manipulation during transmission) which are discussed in the next sub-theme.

In the 2023 elections, many of these emerging risks crystallised. With reports of large-scale failure of electronic votes transmission, it appears that risks were left unmitigated (Eleanya 2023). A joint statement by the international observation mission of the International Republican Institute (IRI) and the National Democratic Institute (NDI) (2023) noted the challenges with electronic result transmission and real-time display of results on the IReV, particularly with the presidential elections. These made citizens raise concerns regarding the transparency of the process. The European Union Election Observation Mission to Nigeria (2023) also noted delays and frictions with the IReV portal, making it difficult to access scanned results. They indicated that some of the reasons for these included the opacity of the electoral technology, lack of robust testing of the device, and lack of training for INEC staff. The statement pointed to these as a failed opportunity on the part of INEC to improve the trust and confidence in the electoral process.

The failure of the transmission and real-time display of results were widely reported by several independent observer groups. For instance, the Commonwealth Election Observer Group to Nigeria (2023) also corroborated this by reporting that the election results were not uploaded to the IReV portal in real-time as advertised. Yiaga Africa, a not-for-profit civic group, raised concerns about the unexplained delay in uploading polling unit results. The group noted that despite the conclusion of counting several hours earlier, at 10 pm on election day presidential election results had not yet been uploaded to the IReV portal, contrary to the promises given by INEC (Kareem 2023). Okeaya-inneh (2023) also noted the poor internet connectivity in remote areas, and that presidential election results were only made public three days after the election, greatly undermining confidence in the process.

INEC's explanation for these issues was that there was a technical glitch relating to server scaling for the IReV. The Commission noted that this was simply a technical problem, and not the result of sabotage or intrusion. However, this explanation left more questions than answers, as at 10 pm on February 26 (a day after the election), fewer than 30% of the presidential election results had been uploaded (*The Guardian* 2023a). Scalability is an important feature of a good system, and INEC's excuse is surprising. The European Union Election Observation Mission to Nigeria (2023) noted that INEC missed the opportunity for a robust test of the technology before the elections.

Cybersecurity Readiness

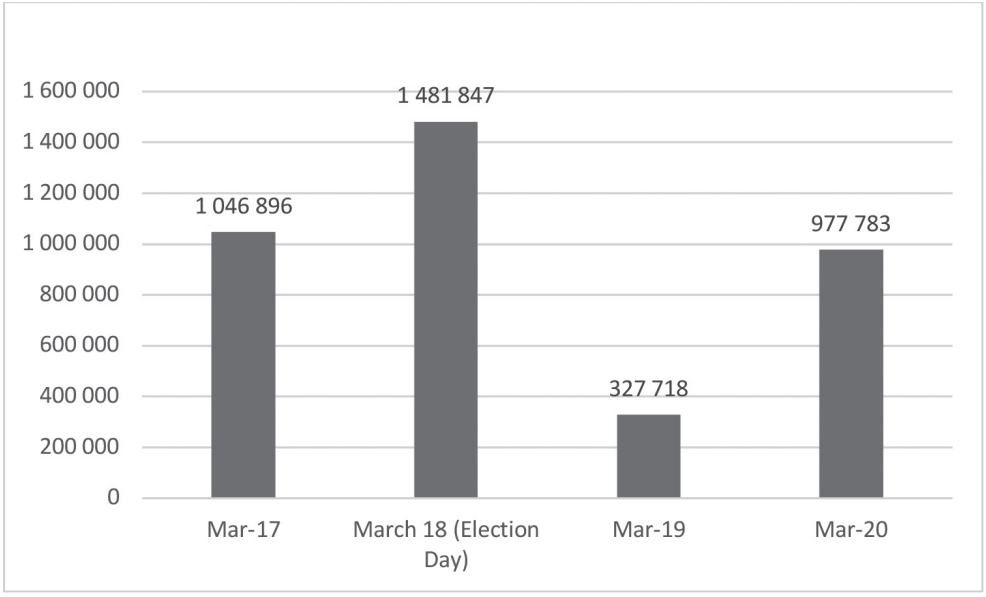
With modern technological innovations in elections, there is an emerging risk of cyberattacks and the potential of tampering with Electronically Stored Information (ESI). These risks are distributed across critical aspects of the electoral chain. For instance, there is the potential risk of intercepting votes in transit; the technical possibility of manipulating the electronic voter database; and of hacking the electronic register, the electronic collation process, and other critical technological deployments in the election value chain. Without prejudice to any specific device, there is the potential risk of manipulating the data stored on the BVAS, and also the potential risk of hacking the IReV and manipulating the result. There are potential risks of tampering with the collation process, and of cybersecurity (hacking, encryption/decryption, manipulation, etc.) of remotely manipulating electronically collated results (Sibe 2022). Given these realities, there is a real possibility that election results could be manipulated by both local and foreign cybercriminals and nation-state actors.

First, this should be viewed from a national perspective. The International Telecommunication Union (2020) ranked Nigeria 47th in the world in the Cybersecurity Readiness Index. This is fifth in Africa, behind Egypt, Tanzania, Ghana, and Tunisia. Therefore, Nigeria has much to do to bolster its cybersecurity readiness. While INEC insists that it has implemented the necessary controls to prevent hacking, and that the challenges experienced in the 2023 election are not because of cyberattacks or sabotage (*The Guardian* 2023), there are probable reasons to think otherwise. First, INEC itself has a history of being at the receiving end of cyber-attack. For instance, in the build-up to the 2015 general elections, INEC's website was attacked and defaced. A hacktivist identified as as the Nigerian Cyber Army later claimed responsibility (Abimboye 2015).

In the Osun and Ekiti state elections, there were also reported cyberattacks of both local and international dimension with cyberattacks from as far as Asia directed at the INEC portal (Ufuoma 2022). In the 2023 elections, the Ministry of Communication and Digital Economy reported a total of 12 988 978 cyberattacks days before and during the election (Izuaka 2023). Again, these attacks were reportedly of both local and international dimensions.

A breakdown of the attack type shows that the cyberattacks consisted of 'Distributed Denial of Service (DDoS), email and IPS attacks, SSH Login attempts, Brute force Injection attempts, Path Traversal, Detection Evasion, and Forceful Browsing' (Izuaka 2023a). The statement reveals that according to intelligence reports, cyberattacks directed at the country averaged 1.55 million per day in the days leading to the elections and peaked at a staggering 6.99 million on election day. In the gubernatorial elections, the cyberattacks directed at INEC dropped

to 3 834 244. A breakdown of these show that on Friday 17 March 2023, a total of 1 046 896 attacks were recorded; on Saturday, 18 March 2023, election day proper, a total of 1 481 847 attacks were recorded; on Sunday 19 March 2023, a total of 327 718 attacks were recorded; and on Monday 20 March 2023, a total of 977 783 attacks were recorded (Izuaka 2023b). These figures are plotted in a chart shown in Figure 2 below. Experts, however, have questioned these figures, given the emerging dynamics of global threat intelligence (Michael 2023; Okonji 2023).



Source: Based on data from Izuaka (2023b)

Figure 2: Cyberattacks directed at Nigerian Institutions during the Governorship Elections in 2023

It is noteworthy that the statement from the ministry was on behalf of a special-purpose committee set up to protect cyberspace for the elections. The committee includes the Board chairman and CEO of the Nigerian Communications Commission (NCC) together with the CEOs of the National Information Technology Development Agency (NITDA) and Galaxy Backbone (GBB) (Michael 2023). While the cyber-attack figures appear surprisingly large and possibly questionable, these are major technology agencies in the country, and such official pronouncements cannot be dismissed without interrogation.

While there is scanty information needed to make categorical statements, there are pointers to the fact that INEC does not have the right level of cybersecurity readiness. Beyond this, the Ministry of Information stated that INEC had deliberately withheld the electronic transmission of data after suspecting a cyberattack on their election infrastructure. The minister also noted that after this, INEC decided to withhold electronic transmission of the election result, in order to preserve it. While this categorical statement by the nation's information minister appears to be at variance with INEC's position that there was no cyber-attack (Daramola 2023), it does suggest INEC's lack of cybersecurity readiness.

In addition, while the Ministry of Communications and Digital Economy announced almost 13 million cyberattacks directed at the country (Izuaka 2023), INEC has not issued any statement corroborating or refuting these claims. For a public-centric process such as general elections, with mixed stakeholders who all want information and transparency, this silence suggests either lack of capacity, or as an outside possibility, complicity. Several months have passed since the elections, and INEC has not yet released any official report, or even press statement, on the cybersecurity activities during and after the elections. This is curious, and may point to a lack of capacity in an organisation that should operate independently but has not yet issued any statement, and on the contrary allows other government agencies and political appointees to make statements apparently on their behalf.

Also, it is noteworthy that in Section 41 of the Cybercrimes (Prohibition, Prevention, Etc.) Act 2015, the Office of the National Security Adviser is empowered as the coordinating body for Nigeria's cybersecurity. According to the National Cybersecurity Strategy and Policy 2021 released by the Office of the National Security Adviser (2021), the National Security Adviser (NSA) shall establish the National Cybersecurity Coordination Centre (NCCC). Neither of these two statutory organisations has issued any categorical statements with respect to coordinated cyberattacks directed at Nigeria and INEC during the 2023 elections; yet, the Minister of Information, who bears no direct constitutional or technological responsibility, has issued direct statements in this regard.

Digital Forensic Readiness

Even the most secure system does suffer attacks. Therefore INEC needs to be ready to carry out a full-scale forensic investigation in the event of a cyberattack. Does INEC have the technology (hardware and software), technical personnel, processes, and systems to commission digital forensic investigations if there is an incident? Also, given the involvement of technology in the Electoral Act 2022, most post-election cases will rely on digital evidence. Does INEC have the capabilities

to collect, preserve, and analyse digital data and present results in a forensically sound manner? Can INEC carry out a forensic investigation that could rely on digital artifacts to recreate the events and scenarios critical to solving electoral disputes beyond a reasonable doubt? How forensically ready is INEC?

While there is little or no information on the digital forensic readiness of INEC, there are facts pointing to their lack of readiness. First, a keyword search on Google and Google Scholar search engines for 'INEC's digital forensic laboratory', 'Digital Forensic Unit of INEC' and 'Forensic Department of INEC' did not return any meaningful result in this regard. Also, a search on the INEC portal did not reveal the presence of a dedicated digital forensic unit or expert personnel in this regard. Beyond this, the lacklustre way the Commission handled the alleged cyberattacks is an obvious pointer to their lack of digital forensic resources. If there were attacks, as alleged, the Commission should have commissioned digital forensic investigations. Almost three months after the presidential election, INEC has not made any clear statement corroborating or refuting the alleged attacks, nor initiated any arrests (through the relevant law enforcement agency) in this regard.

Given the lack of information on the digital forensic readiness of INEC, the Commission appears to rely solely on the law enforcement agencies for digital forensic investigation, rather than having first level in-house digital forensic investigative capability. The sad reality is that the Nigerian law enforcement agencies themselves are not ready, from a digital forensic readiness standpoint. They lack the requisite resources to cope with Nigeria's rising caseloads (Sibe 2021; Sibe & Muller 2022). Given the fact that these cases may end up in court, it is sad to note that the Nigerian justice system is also not forensically ready (Sibe 2021). With these emerging realities, INEC, as presently constituted, does not have the right level of digital forensic readiness to tackle the emerging threat landscape efficiently.

SUMMARY OF FINDINGS

This article examined existing literature to analyse technological innovations and emerging risks in elections in Nigeria, with Estonia as a case study. The article shows that the BVAS and IReV, like other technological innovations, can improve the quality of our elections if properly implemented. The two sets of tables below summarise the findings of this study. Table 1 shows a comparative analysis of key themes in technological innovations in Estonia and in Nigeria. Table 2 depicts a summary of the findings from this study.

Table 1: Comparative analysis of key themes in technological innovations in Estonia and in Nigeria

S/N	Themes	Estonia
1	Electronic voting	Remote voting via the internet (iVoting)
2	Legal framework	Riigikogu Election Act 2002
3	Vote change	Votes cast electronically can be changed during the defined window
4	Votes verification	Voters can verify votes cast electronically
5	Voter identification	Relies on existing national ID
6	Voter anonymity	Uses advanced encryption technology
7	Vote transmission	Transmitted via the internet, using encryption technology to ensure voter anonymity
8	Trust and transparency	Source code released publicly Robust stakeholder demonstrations
9	Audit	o Use professionals and specialists for the audit process o Use cryptographic proofs that can be relied on for independent verification
10	Pilot testing	Went through public evaluation and pilot tests
11	Stakeholder evaluation	Went through robust multi-stakeholder evaluation
12	Single point of failure	Centralised architecture

Table 2: Summary of key findings

S/N	Themes	Research Findings	Literature
1	Legal and regulatory framework	o Technological engagement in a public-centric process such as an election requires an enabling law o The Electoral Act 2022 provides the legal framework for the use of technology in elections in Nigeria	Munya 2022; O'Meara 2013; Maaten 2004; Sibe 2015; and Sibe 2022
2	Reliability engineering	o Pilot tests are important in large-scale rollout of technology, such as in elections o INEC did not carry out robust reliability tests involving critical stakeholders o Reports of reliability issues in the 2023 election	Cheeseman et al. 2018; Ali 2015; Yusuf & Akuva 2020; Alabiosu 2016; Odalonu & Ogu 2022; Abodunrin et al. 2018; Sibe 2015; and Sibe 2022

3	Impact of technology on Nigeria's elections	o Technology has improved the quality of elections in Nigeria o Technology has improved voter confidence in the electoral process	Yusuf& Akuva 2020; Munya 2022; Enwere & Ladan-Baki 2015; Agbu 2016
4	Existing technological infrastructure	o INEC relies on existing technological infrastructure outside of their control, such as internet service, network coverage, and electricity o Reports of poor network coverage given as an excuse for some cases of failed result transmission	Sibe 2022; Maaten 2004; Ehin et al. 2022
5	Privacy and security concerns	o Privacy and confidentiality are critical expectations of electoral systems. o Voting systems should ensure voter anonymity o Need for NDPR compliance	Nurse, et al. 2017; Sibe 2015; Sibe 2022; Babalola 2021
6	Challenges with INEC's technologies	o Reported challenges with BVAS: - Failed facial recognition - Failed result transmission o Failed IReV during the 2023 election	Odalonu & Ogu 2022; Yusuf & Akuva 2020; Alebiosu 2016; Sibe 2015
7	Cybersecurity readiness	o Need for cybersecurity readiness o Potential risk of hacking and manipulating the data stored on the BVAS, IReV o Potential risk of interception of electronic transmission of votes o Reported cyberattacks in the 2022 and 2023 elections	Sibe 2022; Nurse, et al. 2017; Chaum 2009; Heiberg et al. 2011 September; Springall et al. 2014 November; Yavuz 2018; Ehin et al. 2022
8	Digital forensic readiness	o Need for forensic readiness o No literature available that suggests that INEC is forensically ready o INEC relies on law enforcement agencies for digital forensic investigation. Nigerian law enforcement agencies are not forensically ready	Sibe & Muller 2022; Sibe 2021; Sibe 2022;

9	Jurisdictional challenges	○ This study identified emerging cybercrime risks in the 2023 elections ○ The cross-border nature of cybercrime poses jurisdictional roadblocks in investigating and prosecuting cybercrime	Sibe 2022; Sibe 2021; Interpol 2017
10	Transparency of technology	○ Need for transparency ○ Estonia publishes source code ○ INEC needs to do more to engender transparency and build trust	Ehin et al. 2022
11	Integrity of voting system	○ Voting systems should be robustly tested for integrity ○ Citizens should be able to verify end-to-end the integrity of voting systems	Chaum 2009
12	Auditing	○ Electoral systems should be open to vote auditing ○ Estonia utilised designated auditors ○ INEC rely on staff to audit the process ○ INEC needs independent professionals – auditors, information assurance experts, forensic experts, cybersecurity experts, reliability engineers, and others	Ehin et al. 2022; Nurse et al. 2017
13	Public awareness	○ Need for proper public awareness when introducing new technology	Yusuf & Akuva 2020; Sibe 2015
14	Training	○ Need for more training ○ INEC ad-hoc staff show poor knowledge of the technology deployed	Yusuf & Akuva 2020
15	Single point of failure	○ Centralised architecture for electoral technology could be a source for a single point of failure ○ The centralised structure of Kenya's election in 2012 was a source of a single point of failure ○ IReV failed in the 2023 presidential election INEC's press release suggested a central point of failure	Ali 2015; Yavuz 2018

CONCLUSION

Over the past two decades, INEC has deployed technology to improve the quality of elections. From the digitisation of the voter register to the use of the direct data capture machine, and now the use of the Bimodal Voter Accreditation System, INEC has continued to rely on technology to improve the quality of Nigeria's elections. However, while these deployments have continued to improve the integrity, quality, and efficiency of Nigeria's elections, there are associated emerging risks. This study reviewed the historical and existing technological deployments in elections and identified the challenges faced by INEC in the 2023 elections.

These challenges include reliability, with reported failures of BVAS and the IReV portal; failure of BVAS to electronically transmit results from the polling units as promised; poor understanding of the inner workings of the BVAS and other associated technologies; reported cyberattacks on a large scale; lack of transparency; single point of failure; lack of a framework for a stakeholder audit of the electoral system; and poor cybersecurity and digital forensic readiness. These emerging challenges need to be mitigated to improve the quality of Nigeria's elections.

Findings from this study could potentially shape policy and may be useful to INEC as they plan for future elections. Specific recommendations include the following:

- There is a need for a more robust reliability tests with professionals and stakeholders. For instance, technology experts, reliability engineers, and related professional groups should be enlisted to join in the reliability tests. This would help detect reliability issues early, as well as build confidence in the electoral process.
- INEC needs to improve on its state of cybersecurity readiness and capability. The dangerously high figure of reported attacks is a sad reminder of the potential risk of cyberattack in an election.
- INEC needs to improve its digital forensic readiness. There are no completely secure systems. To this end, it is important for INEC to develop in-house competency in digital forensics.
- In the 2023 elections, there were reports of poor network coverage in certain rural areas. INEC needs to work with the relevant organisations and experts to ensure proper network coverage and bandwidth tests for contingent preparation.
- The reported cyberattacks are an indication of the possibility of data breach. Given the large voter database with PII, INEC needs to take reasonable steps to ensure data protection and NDPR compliance.

- There were reports of staff exhibiting poor knowledge of the election technology, indicating that more training is needed for both permanent and ad hoc INEC staff.
- More stakeholder engagement and public awareness campaigns are needed.
- There is a need for a proper election risk management system that looks at the risks, not in silos, but across the entire election value chain.
- The IReV failed in the presidential election, and days later, updated election results had not yet been reflected on the portal. Therefore, there is a need for a robust business continuity plan (BCP) and disaster recovery plan (DRP). This is even more important, given the barrage of cybersecurity attacks reported by the authorities.

REFERENCES

Abimboye, M 2015, '*INEC website hacked*', *Premium Times*. ww.premiumtimesng.com/news/top-news/179539-inec-website-hacked.html

Adebayo, T-H 2015, 'INEC says card-reader test successful, admits 41% fingerprint failure', *Premium Times*, 10 March. https://www.premiumtimesng.com/news/headlines/178264-inec-says-card-reader-test-successful-admits-41-fingerprints-verification-failure.html.

Adenekan, S 2022, '2023: INEC clears air on mode of transmitting election results', *Premium Times* 21 August. https://www.premiumtimesng.com/news/top-news/549890-2023-inec-clears-air-on-mode-of-transmitting-election-results.html?tztc=1

Adeshina, SA & Ojo, A 2020, 'Factors for e-voting adoption-analysis of general elections in Nigeria', *Government Information Quarterly*, vol, 37, no. 3, p. 101257.

Agbu, O 2016, 'Election rigging and the use of technology: the Smart Card Reader as the Joker in Nigeria's 2015 Presidential Election', *Journal of African Elections*, vol. 25, no. 2, pp. 90-111.

Agiri, EJ & Morka, BC 2022, 'X-Ray of Ekiti State Governorship Election in Nigeria, 2022', *African Journal of Humanities and Contemporary Education Research*, vol. 5, no. 1, pp. 147-156.

Anichukwueze, D 2022, '2023: No Going Back On Electronic Transmission Of Results, INEC Reassures', *ChannelsTV*, 26 October. https://www.channelstv.com/2022/10/26/election-results-will-be-electronically-transmitted-in-real-time-inec-assures/

Alebiosu, EA 2016, 'Smart card reader and the 2015 general elections in Nigeria', *Journal of African Elections*, vol. 15, no. 2, pp. 69-89.

Allen, PL 1906, 'Ballot laws and their workings', *Political Science Quarterly*, vol. 21, no. 1, pp. 38-58.

Ali, T 2015, 'How (not) to deploy an Electronic Voting System'. https://tribune.com.pk/story/889594/how-not-to-deploy-an-electronic-votingsystem

Amata, D 2022, '2023 Election: Completed PVC registration across Nigeria in 5 charts', https://www.dataphyte.com/latest-reports/elections/2023-election-completed-pvc-registration-across-nigeria-in-5-charts/

Ayed, AB 2017, 'A conceptual secure blockchain-based electronic voting system', *International Journal of Network Security & Its Applications*, vol. 9, no 3, pp. 01-09.

Chaum, D, Carback, RT, Clark, J, Essex, et al. 2009, 'Scantegrity II: End-to-end verifiability by voters of optical scan elections through confirmation codes', *IEEE transactions on information forensics and security*, vol. 4, no. 4, pp. 611-627.

Cheeseman, N, Lynch, G, & Willis, J 2018, 'Digital dilemmas: The unintended consequences of election technology', *Democratization*, vol. 25, no 8, pp. 1397-1418.

Commonwealth Election Observer Group to Nigeria 2023, *Interim statement of the Commonwealth Observer Group to Nigeria's 2023 general elections*. https://thecommonwealth.org/interim-statement-commonwealth-observer-group-nigerias-2023-general-elections

Cortier, V & Wiedling, C 2017, 'A formal analysis of the Norwegian E-voting protocol', *Journal of Computer Security*, vol. 25, no. 1, pp. 21-57.

Daramola, K 2023, 'Lai: why INEC withheld uploading of results during presidential poll', *The cable*, 4 April, https://www.thecable.ng/lai-why-inec-withheld-uploading-of-results-during-presidential-poll

Ehin, P, Solvak, M, Willemson, J, & Vinkel, P 2022, 'Internet voting in Estonia 2005–2019: Evidence from eleven elections', *Government Information Quarterly*, 101718.

Ejiofor, A 2023, INEC's Dramatic U-turn on electronic transmission of election results, *Thisday Newspaper*, 16 April, https://www.thisdaylive.com/index.php/2023/04/16/inecs-dramatic-u-turn-on-electronic-transmission-of-election-results

Eleanya, F 2023, 'INEC fails Nigeria on e-transmission of results', *Business Day*, 28 February, https://businessday.ng/technology/article/inec-fails-nigeria-on-e-transmission-of-results/

Enough is Enough Nigeria 2023, *EiE election call centre report*. https://eie.ng/resources/publications/

Enwere, C & Ladan-Baki, I 2015, 'Understanding the Role of Technology in Free and Fair Elections in Developing Countries', *Journal of Social and Administrative Sciences*, vol, 2, no. 3, pp. 135-143.

Estonian National Electoral Committee (NEC) 2022, *Internet voting in Estonia*. https://www.valimised.ee/en/internet-voting-estonia

European Union 2023, *Election Observation Mission to Nigeria (2023). General Elections – 25 February and 11 March 2023*. https://www.eeas.europa.eu/sites/default/files/documents/2023/EU%20EOM%20NIGERIA%202023_FIRST%20PRELIMINARY%20STATEMENT%20_27_02_2023.pdf

Garnett, HA & James, T 2020, 'Cyber elections in the digital age: Threats and opportunities of technology for electoral integrity', *Election Law Journal: Rules, Politics, and Policy*, vol. 19, no. 2, pp. 111-126.

Hancock, DR, & Algozzine, B 2017, *Doing case study research: A practical guide for beginning researchers*, Teachers College Press, New York.

Heiberg, S, Laud, P & Willemson, J 2011, September, 'The application of i-voting for Estonian parliamentary elections of 2011', In *International Conference on E-Voting and Identity*. pp. 208-223. Springer, Berlin, Heidelberg.

Ileyemi, M 2021, '#AnambraDecides2021: Review BVAs, security challenges before 2023 – TMG tells INEC', *Premium Times*, 11 November. https://www.premiumtimesng.com/news/more-news/494898-anambradecides2021-review-bvas-security-challenges-before-2023-tmg-tells-inec.html

INEC 2015, *Fact sheet on PVC and card reader.* https://inecnigeria.org/wp-content/uploads/2019/02/FactSheet-on-PVC-and-Card-Readers.docx

INEC 2022a, *Regulations and guidelines for conduct of elections, 2022*. https://inecnigeria.org/wp-content/uploads/2022/06/REGULATIONS-AND-GUIDELINES-FOR-THE-CONDUCT-OF-ELECTIONS-2022_updtd.pdf

INEC 2022b, *Get used to new electoral Act, we'll scrupulously apply the laws, INEC chairman tells parties.* https://www.inecnigeria.org/?page_id=11329#:~:text=The%20INEC%20Chairman%20said%20the,Prof..

International Centre for Investigative Reporting 2023, *BVAS malfunction mars election in Rivers*, 25 February. https://www.icirnigeria.org/bvas-malfunction-mars-election-in-rivers/

International Data Corporation 2022, *Cybersecurity Nigeria: A digital transformation imperative*. https://info.microsoft.com/rs/157-GQE-382/images/EN-CNTNT-Whitepaper-CybersecurityADigitalTransformationImperative-SRGCM7029.pdf

International Republican Institute (IRI) and the National Democratic Institute (NDI) 2023, *Preliminary Statement of the Joint NDI/IRI International Observer Mission to Nigeria's 2023 Presidential and Legislative Elections*, 27 February https://www.iri.org/resources/preliminary-statement-of-the-joint-ndi-iri-international-observer-mission-to-nigerias-2023-presidential-and-legislative-elections/

International Telecommunication Union 2020, *Global cybersecurity index 2020.* https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

Interpol 2017, *Global cybercrime strategy.* https://www.interpol.int/en/Crimes/Cybercrime

Izuaka, M 2023, 'Nigeria recorded 12.9 million Cyberattacks during presidential, NASS elections – Minister', *Premium Times*, 23 March, https://www.premiumtimesng.com/business/business-news/587712-nigeria-recorded-12-9-million-cyberattacks-during-presidential-nass-elections-minister.html

Izuaka M 2023b, 'Nigeria recorded 3.8 million Cyber attacks during gubernatorial, state assembly elections – Minister', Premium Times, 22 March, https://www.premiumtimesng.com/news/top-news/589670-nigeria-recorded-3-8-million-cyberattacks-during-gubernatorial-state-assembly-elections-minister.html

Jaiyeola, T 2023, 'How BVAS, IReV failed first election's stress test', 6 March. https://punchng.com/how-bvas-irev-failed-first-elections-stress-test/

Jega, A & Hillier, M 2012, 'Improving elections in Nigeria: Lessons from 2011 and looking to 2015', *Africa Programme Meeting Strategy*, Chatham House. https://www.chathamhouse.org/sites/default/files/public/Research/Africa/040712summary.pdf

Jibia, MS, & Zake, M 2020, 'Electronic technology literacy and performance of elections in selected states in Nigeria', *International Journal of Science and Technology*, vol. 67.

Kareem, K 2023, 'International observer groups flag Nigeria's presidential election', Dataphyte, 1 March. https://www.dataphyte.com/latest-reports/international-observer-groups-flag-nigerias-presidential-election/

Maaten, E 2004, 'Towards remote e-voting: Estonian case', In *Electronic voting in Europe-Technology, law, politics and society, workshop of the ESF TED programme together with GI and OCG,* Gesellschaft für Informatik eV, Bregenz, Austria.

Martens, T 2011, 'Technical aspects of the internet voting system', *National Electoral Committee*. http://vvk.ee/public/EH_Overiview_03-11.pdf.

Michael, C 2023, 'INEC server records 12m cyberattacks during presidential poll', *Business Day*, 12 March. https://businessday.ng/news/article/inec-server-records-12m-cyberattacks-during-presidential-poll-pantami/

Microsoft 2022, 'As cloud adoption increases, data breaches top the list of security concerns for Nigerian CIOs', https://news.microsoft.com/en-xm/2022/10/03/as-cloud-adoption-increases-data-breaches-top-the-list-of-security-concerns-for-nigerian-cios/

Munya, P 2022, 'Electronic governance and election administration', In OJ Iba, CN Dickson, AJ John (Eds.), *Public administration: theory and practice in Nigeria,* pp. 266-282. Chananprints.

Nurse, JR, Agrafiotis, I, Erola, A, et al. 2017, July, 'An Assessment of the Security and Transparency Procedural Components of the Estonian Internet Voting System', *International Conference on Human Aspects of Information Security, Privacy, and Trust*, pp. 366-383, Springer, Cham.

Ochei, A 2023, 'Explainer: Is INEC in breach of law on e-transmission of results?', *Businessday Newspaper*, 1 March, https://businessday.ng/

nigeriadecidesliveupdates/article/explainer-is-inec-in-breach-of-law-on-e-transmission-of-results/

Odalonu, BH, & Ogu, HN 2022, 'Voting Behaviour and Pattern of Voting in 2021 Gubernatorial Election in Anambra State, Nigeria', *African Journal of Humanities and Contemporary Education Research*, vol. 4, no. 1, pp. 01-17.

Okeaya-inneh, A 2023, 'High tech failed to make Nigeria's presidential election transparent', D&C, 26 March. https://www.dandc.eu/en/article/nigerian-voters-are-frustrated-because-digital-election-tools-did-not-deliver-promised

Okonji, E 2023, 'Cybersecurity Expert Asks Pantami to Breakdown 12.99m Cyberattacks in Four Days', *Thisday,* 17 March. https://www.thisdaylive.com/index.php/2023/03/17/cybersecurity-expert-asks-pantami-to-breakdown-12-99m-cyberattacks-in-four-days/

Shchebetun, IS, Nikitenko, LO, Pysarieva, EA, Turchenko, OH, & Afanasieva, MV 2020, 'Electronic and Internet Technologies in the Election Process', *Test Engineering and Management,* vol. 83.

Sibe, RT 2015, 'Revisiting the use of card reader in 2015 elections', *Business Day*, 12 November. https://businessday.ng/analysis/article/revisiting-the-use-of-card-reader-in-the-2015-elections-1/

Sibe, RT 2021, 'Lack of forensic resources in Nigerian Internet fraud agency', [PhD Thesis], University of the Cumberlands.

Sibe, RT 2022, 'Electoral Act 2022: technical implications, emerging risks and forensic possibilities', *Business Day,* 6 March. https://businessday.ng/news/article/electoral-act-2022-technical-implications-emerging-risks-and-forensic-possibilities/

Sibe, RT & Muller, SR 2022, 'Digital Forensic Readiness of Cybercrime Investigating Institutions in Nigeria: A Case Study of the Economic and Financial Crimes Commission (EFCC) and the Nigeria Police Force', *Proceedings of the International Conference on Research in Management & Technovation, Da Nang City, Vietnam*. 10.15439/2022M9438.

Springall, D, Finkenauer, T, Durumeric, Z, et al. 2014, 'Security analysis of the Estonian internet voting system', *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security,* pp. 703-715.

The Guardian 2022, 'INEC to deploy 200,000 BVAS in 2023 general elections', 29 July. https://guardian.ng/news/inec-to-deploy-200000-bvas-in-2023-general-elections-okoye/

The Guardian 2023a, 'Alleged data breach: NDPB investigates two Nigerian banks', 30 January. https://guardian.ng/news/nigeria/alleged-data-breach-ndpb-investigates-two-nigerian-banks/

*The Guardian 2023b, '*Anxiety, parties kick as INEC delays result upload, collation', 27 February. https://guardian.ng/news/anxiety-parties-kick-as-inec-delays-result-upload-collation/

Thisday 2023a, 'INEC's dramatic u-turn on electronic transmission of election results', 16 March. https://www.thisdaylive.com/index.php/2023/04/16/inecs-dramatic-u-turn-on-electronic-transmission-of-election-results/

Tsahkna, AG 2013, 'E-voting: lessons from Estonia', *European View*, vol. 12, no. 1, pp. 59-66.

Ufuoma, V 2022, 'Hackers attacked our result portal during Ekiti, Osun elections', *International Centre for Investigative Reporting*. https://www.icirnigeria.org/hackers-attacked-our-result-portal-during-ekiti-osun-elections-inec/

Vanguard 2023, 'INEC admits glitches, vows to use BVAS in gov, assembly elections', 4 March. https://www.vanguardngr.com/2023/03/inec-admits-glitches-vows-to-use-bvas-in-gov-assembly-elections/

Yavuz, E, Koç, AK, Çabuk, UC, & Dalkılıç, G 2018, March, 'Towards secure e-voting using ethereum blockchain', In *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, pp. 1-7.

Yusuf, A & Akuva, II 2020, 'Smart card reader machines and general elections in Nigeria from 2015 to 2019: gains and challenges', *Studies in politics and society,* vol. 9, no. 1.

DOI: 10.20940/JAE/2023/v22i2a5

NIGERIA'S 2023 PRESIDENTIAL ELECTIONS
The Question of Legitimacy for the Tinubu Administration

Akinbode Fasakin

Akinbode Fasakin is an adjunct faculty at the Department of Political Science and Law, Swedish Defence University, Stockholm, Sweden

ABSTRACT

This article raises concerns about the legitimacy crisis likely to confront the government of Nigeria's President Bola Tinubu, following the nature of the conduct and outcome of the 2023 presidential elections. While legitimacy is crucial to government and governance, citizens' compliance and cooperation with the government, and how elections and their outcomes are perceived can influence the government's legitimacy. The study reveals how INEC'S conduct, Tinubu's personality crisis and the burdens facing the ruling APC in a pluralistic society, as well as the emerging youth category, would affect Tinubu's legitimacy as Nigeria's president. The analysis relies on careful observation of Nigerian politics and elections as well as the views expressed by experts, political parties, local and international observers and newspaper reports before, during and after the 2023 elections. It offers an empirical contribution to our understanding of the relationship between elections and the legitimacy of Nigeria.

Keywords: presidential elections, Bola Tinubu, legitimacy, Nigeria, political parties

INTRODUCTION

Nigeria held its seventh presidential and National Assembly (NASS) elections in February 2023. While the elections were marred by some irregularities, they were also adjudged by observers to be *relatively* free, fair and credible (Habib 2023; *Premium Times* 2023). The political parties in the elections shared the votes and NASS seats .[1] Unlike previous elections, where hundreds of lives were lost

1 INEC Chairman, Mahmood Yakubu, stated that seven and eight political parties respectively won seats at the Senate and House of Representatives.