Cybersecurity Challenges and Electoral Integrity in Nigeria's 2023 General Elections

By

Emeka J Onyetube PhD
Political and Governance Policy Department
Nigerian Institute of Social and Economic Research, Ibadan
email: ejonyetube@yahoo.com l Phone 08024348880

Abstract

Nigeria's 2023 general elections marked one of the country's most technologically driven polls, yet they also exposed critical cybersecurity vulnerabilities that shaped public trust and electoral integrity. The expanded use of digital tools, particularly the Bimodal Voter Accreditation System (BVAS) and the INEC Results Viewing Portal (IReV), was intended to improve transparency, but technical failures, cyberattacks, weak connectivity, and gaps in digital forensics undermined these expectations. These challenges created delays in result uploads, fuelled misinformation, and deepened doubts about the credibility of the process. The paper adopted a qualitative approach, analyzing secondary data from journals, election observer reports, credible media publications, and publicly available policy documents, INEC, and EU Election Mission reports, newspapers. Specifically, the paper adopted **content analysis** and **documentary methods** to investigate cybersecurity challenges and electoral integrity in Nigeria's 2023 general elections. Although the election demonstrated the potential of technology to enhance democratic accountability, it also revealed the need for stronger cybersecurity frameworks, better infrastructural support, and transparent communication. It recommends, among others, **strengthening the National Cybersecurity Policy and Strategy (2021)** to include explicit provisions for safeguarding electoral technologies, including BVAS, IReV, and electronic voter databases.

Keywords: Cybersecurity, Electoral Integrity, BVAS, IReV, Election Technology

Introduction

Background of the Study

The 2023 general elections in Nigeria represented a landmark in the country's democratic evolution, primarily because of the deployment of two digital technologies on a national scale: the **Bimodal Voter Accreditation System (BVAS)** and the **INEC Result Viewing Portal (IReV).** These technologies were intended to reinforce transparency, reduce voter impersonation, and enable citizens to track polling unit results in (near) real-time (Chatham House, 2024; Situation Room Nigeria, 2023). Specifically, BVAS is designed to authenticate voters via biometric means and scan result sheets, while IReV allows the upload of scanned images of results forms for public viewing (Chatham House, 2024; Situation Room Nigeria, 2023).

However, the implementation of these systems was accompanied by notable operational and cybersecurity challenges. Reports indicate that many polling unit officials struggled with IReV passwords or access codes, that some results uploads were delayed by system glitches or lack of internet connectivity, and that some BVAS devices failed or malfunctioned (GIGA-Hamburg, 2023; Situation Room Nigeria, 2023). In a few cases, these technical issues undermined the promise of real-time transparency, leading to public uncertainty about how results were being collated and whether the digital tools were adequately secure against cyber threats (Democracy in Africa, 2023; GIGA-Hamburg, 2023).

The larger context for this is Nigeria's cybersecurity policy environment, which includes the **National Cybersecurity Policy and Strategy 2021**, aimed at protecting critical information infrastructure and enhancing cyber resilience (NC SI / EGA, 2023). Yet, despite the existence of policy frameworks, questions remained about readiness, technical capacity, and whether electoral technology deployments were matched with sufficient cybersecurity governance, training, and institutional oversight.

While BVAS and IReV were introduced to improve electoral integrity, the 2023 elections revealed several cybersecurity-related issues that challenged both the credibility of outcomes and citizens' trust. System glitches, delayed uploads of result sheets, failures in device functionality, and disinformation propagated

online contributed to perceptions of opacity in the result-transmission process (Situation Room Nigeria, 2023; GIGA-Hamburg, 2023). Moreover, although Nigeria has a national cybersecurity strategy, there is evidence that key electoral technology deployments were not subject to sufficiently robust testing (e.g., load testing, stress testing), nor were all polling units equipped with stable internet access, thereby leaving the systems vulnerable to cyber disruptions (GIGA-Hamburg, 2023; Chatham House, 2024).

This confluence of technical failures, potential vulnerabilities to cyberattack, and public distrust poses a serious challenge to the integrity of Nigeria's democratic processes. The problem thus lies in the gap between the technological promise of BVAS and IReV and the actual cybersecurity and governance conditions under which they were deployed. It, therefore, raises issues about the challenges encountered during the deployment of BVAS and IREV in the 2023 general elections and how these challenges affected electoral integrity and public trust in the election results.

Conceptual Review

Cybersecurity The concept of cybersecurity has become a central concern in contemporary democracies, especially as electoral processes increasingly rely on digital systems. At its core, cybersecurity refers to the practices, technologies, and institutional mechanisms designed to protect digital infrastructure from unauthorized access, manipulation, disruption, or destruction. As **Adebayo (2020)** explains, cybersecurity aims to ensure confidentiality, integrity, and availability of digital assets, a triad commonly used to assess the resilience of technological systems. In the electoral context, these assets include biometric devices, voter databases, results transmission platforms, and communication networks. Nigeria's growing dependence on digital technologies for elections has highlighted the urgency of cybersecurity preparedness. According to **Ibrahim (2021),** Nigeria's cyber ecosystem remains fragile due to poor internet penetration in rural areas, insufficient digital literacy among electoral officials, and a limited pool of trained cybersecurity professionals within public institutions. These vulnerabilities create opportunities for cybercriminals, politically motivated hackers, and foreign actors to compromise the electoral system. Such threats are not merely hypothetical; the 2023 general elections provided multiple examples of

attempted cyber intrusions targeting the Independent National Electoral Commission (INEC), confirming long-standing fears raised by experts and civil society groups.

Cybersecurity in elections is multifaceted. It encompasses protection against phishing attempts, malware infiltration, denial-of-service attacks on servers, interference with biometric systems, and unauthorized access to results databases. **Olagunju (2023)** emphasizes that election management bodies in Africa face unique challenges because many technology vendors operate outside the country, making supply-chain integrity difficult to guarantee. This raises concerns about the possibility of embedded vulnerabilities, backdoors, or software weaknesses that can be exploited during or after elections. Moreover, cybersecurity also includes safeguarding personal data. Nigeria's voter register, one of the largest in Africa, contains sensitive personal information collected for biometric authentication. **Ekhomu (2019)** warns that weak data protection regimes expose citizens to identity theft, political profiling, targeted misinformation, and other forms of digital exploitation. Thus, in the Nigerian context, cybersecurity is not just a technical matter, it is directly linked to citizens' rights, public trust, and democratic legitimacy.

Electoral Integrity: This refers to the degree to which elections meet standards of transparency, inclusiveness, fairness, and reliability. The concept has gained prominence in discussions about Nigeria's democracy, especially because elections have historically been marred by irregularities. **Nwokedi (2019)** defines electoral integrity as the ability of the electoral process to accurately capture the preferences of the electorate through secure, credible procedures. This includes registration, campaigning, voting, collation, transmission of results, adjudication of disputes, and announcement of winners.

The literature identifies both procedural and substantive dimensions of electoral integrity. Procedurally, it concerns compliance with laws, adherence to timelines, transparency of processes, and professional conduct of election officials. Substantively, it relates to whether citizens genuinely believe that their votes matter. As **Omotola (2010)** argues, elections cannot be said to possess integrity

merely because they avoid blatant fraud; rather, they must be perceived as free from manipulation, undue influence, or institutional bias.

Nigeria has experienced multiple crises of electoral integrity, ranging from ballot snatching and vote buying to legal ambiguities in the interpretation of electoral laws. The introduction of digital technology was expected to address many of these historical weaknesses, but as **Ojo (2023)** points out, technology alone cannot compensate for structural and governance shortcomings. Electoral integrity depends on the strength of institutions, consistency of legal frameworks, capacity of personnel, and trustworthiness of electoral authorities.

In recent years, the conversation around electoral integrity has broadened to include digital transparency and cyber-resilience. For example, the inability to upload polling-unit results promptly on the IReV portal during the 2023 elections not only raised concerns about technical malfunction but also eroded public confidence. **Akinola (2023)** observes that delays, system breakdowns, and poor communication can create a perception of manipulation even where no deliberate wrongdoing occurred. Therefore, electoral integrity in Nigeria must be understood holistically: as the result of technological reliability, institutional preparedness, legal clarity, and the confidence citizens place in the electoral system. In a digital election, the collapse of any of these components can undermine the entire process.

Election Technology (BVAS and IReV) Election technology refers to tools, including hardware, software, and digital platforms, designed to enhance different stages of the electoral process. In Nigeria's 2023 elections, the most notable tools were the Bimodal Voter Accreditation System (BVAS) and the INEC Results Viewing Portal (IReV). These technologies represented an ambitious attempt to modernize elections, reduce human interference, and promote transparency.

BVAS: According to Okoro and Adeniran (2022), BVAS is a biometric device that integrates fingerprint and facial recognition to verify voters at polling units. It replaced earlier systems such as Smart Card Readers, which relied solely on fingerprints and were easily manipulated. BVAS was expected to eliminate

impersonation, curb multiple voting, and strengthen the credibility of accreditation records. The device also had a back-end function: capturing images of polling-unit results (Form EC8A) and transmitting them to the IReV portal. This function was central to the public expectation of real-time transparency. However, technical failures, slow processing speeds, and network connectivity challenges undermined its performance in many locations. **Olagunju (2023)** argues that BVAS, despite its strengths, requires continuous software updates, stronger battery capacity, and better-trained personnel to function optimally.

IReV: The IReV portal was introduced in 2020 and gained prominence during gubernatorial and by-elections before being deployed nationally in 2023. According to **INEC (2022)**, the portal was designed to allow citizens, observers, and parties to monitor results as they were uploaded from polling units. This was intended to reduce suspicion, curb manipulation during collation, and foster public trust. However, the portal faced widespread delays and inconsistencies during the 2023 presidential election. **Adebiyi (2023)** notes that while IReV worked effectively in some races, its failure to upload presidential election results promptly created a credibility crisis that overshadowed other improvements. Poor internet connectivity, server overload, and possible cyberattacks were cited as contributing factors.

Broader Considerations

Election technology, as **Ojo (2023)** warns, cannot be divorced from the political and institutional environment in which it operates. Tools like BVAS and IReV can improve transparency only when supported by strong legal frameworks, robust cybersecurity, clear operational guidelines, and effective stakeholder communication. The Nigerian experience demonstrates that while technology can mitigate some forms of electoral malpractice, it can also introduce new vulnerabilities, technical, cyber-related, or perceptual, that must be addressed comprehensively.

Conceptual Clarification

The paper adopts these concepts as defined below.

Cybersecurity: Protection of digital systems, networks, and data against unauthorized access, attack, or damage.

Electoral Integrity: The degree to which an election is conducted fairly and credibly; the extent to which both the process and perception of an election are acceptable under democratic norms.

BVAS (Bimodal Voter Accreditation System): The device used in Nigeria for voter verification via biometric authentication and to aid the transmission of polling unit result sheets.

IReV (INEC Result Viewing Portal): The portal through which scanned polling unit results are uploaded for public viewing.

Disinformation: Deliberate spread of false or misleading information to influence public perceptions or undermine credibility.

Theoretical Framework

This study draws on two interrelated theoretical perspectives; the **Cybersecurity**

Good Governance Theory and the **Electoral Integrity Framework**. Together, they provide a dual lens for examining how governance structures, institutional accountability, and digital security practices shape public confidence in electoral processes.

1. Cybersecurity Good Governance Theory

The **Cybersecurity Good Governance Theory** emphasizes that cybersecurity extends beyond technological protection to include institutional capacity, transparency, accountability, and the rule of law (OECD, 2019). It argues that an effective cybersecurity system depends not only on digital infrastructure but also on how well governance systems anticipate, prevent, and respond to cyber threats Good governance, in this context, implies the existence of well-defined policies, inter-agency coordination, skilled personnel, and accountability frameworks that ensure resilience in the face of cyber incidents (OECD, 2019). When governments fail to invest in these governance dimensions such as training, monitoring, or legal enforcement, they create vulnerabilities that can be exploited during politically sensitive moments, like national elections.

In the Nigerian case, while the **National Cybersecurity Policy and Strategy (2021)** and the **Cybercrimes (Prohibition, Prevention, etc.) Act (2015)** provide a legal foundation, there are visible governance gaps in implementation and coordination between INEC, the Office of the National Security Adviser (ONSA), and the Nigerian Communications Commission (NCC). During the 2023 general elections, the limited preparedness to defend the BVAS and IReV systems against cyberattacks highlighted a governance failure not only a technical one (Situation Room Nigeria, 2023; Chatham House, 2024).

Thus, the **Cybersecurity Good Governance Theory** helps explain that safeguarding electoral technology requires an integration of **technical resilience** and **governance effectiveness.** Cybersecurity lapses during elections, therefore, reflect deeper structural weaknesses in institutional accountability, political will, and policy enforcement.

2. Electoral Integrity Framework

The **Electoral Integrity Framework**, advanced by scholars such as Pippa Norris (2015, 2017), focuses on the quality and credibility of electoral processes based on principles such as transparency, inclusivity, fairness, and trust. It measures integrity not just by the legal conduct of elections, but also by citizens' perceptions of whether the process was free, fair, and technologically reliable.

In the digital age, electoral integrity now depends heavily on the security and credibility of technology used in voter registration, accreditation, and results transmission (International IDEA, 2021). When these systems are perceived as compromised through hacking attempts, data breaches, or technical failures, public trust in the entire electoral process can erode, even without evidence of deliberate manipulation (GIGA-Hamburg, 2023; Democracy in Africa, 2023).

The **Electoral Integrity Framework** thus provides a lens to analyze how cybersecurity failures such as the delayed upload of polling unit results to IReV which affect the perceived legitimacy of election outcomes. Citizens' belief in the sanctity of the ballot becomes intertwined with the perceived robustness of the technologies and institutions managing them.

Both theories intersect in a way that is particularly relevant to Nigeria's 2023 general elections. The **Cybersecurity Good Governance Theory** identifies *why* vulnerabilities occur; governance deficits, lack of institutional preparedness, or weak coordination. The **Electoral Integrity Framework** explains *how* these vulnerabilities translate into diminished trust, legitimacy crises, and political instability.

In essence, **Cybersecurity Good Governance Theory** explains the *cause* of inadequate governance systems behind cyber vulnerabilities. While **Electoral Integrity Framework** explains the *effect* of erosion of trust and democratic legitimacy due to perceived or real cybersecurity lapses. When linked, these frameworks offer a comprehensive understanding that **electoral technology integrity is not only a technical issue but a governance challenge with profound implications for democracy.** For Nigeria, this means that BVAS and IReV cannot achieve their intended purpose of electoral transparency without systemic governance reform, proper cybersecurity investment, and institutional accountability.

Research Gap

Most scholarly discussions on Nigeria's electoral process have focused on traditional forms of malpractice like vote buying, ballot snatching, and political violence (Omotola, 2010). However, very few studies have examined cybersecurity as a determinant of electoral integrity in the context of digital election management. Even fewer have applied governance-based theories to understand these dynamics.

While reports by INEC (2023), the EU Election Observation Mission (2023), and civil society groups (Yiaga Africa, 2023; Situation Room Nigeria, 2023) mention cyber threats and digital failures, they do not provide in-depth analytical frameworks linking cybersecurity governance to democratic legitimacy. This gap underscores the absence of a comprehensive academic evaluation of **how governance failures in cybersecurity management impact electoral trust** in Nigeria.

Data Sources

The study relies on **secondary data** obtained from verified and reputable sources, ensuring credibility and triangulation. These include:

Official Documents: Reports and press releases by the **Independent National Electoral Commission (INEC, 2023)**, including statements regarding cyberattacks on the INEC Results Viewing (IReV) portal and the operational deployment of the Bimodal Voter Accreditation System (BVAS).

International Observation Reports: The **European Union Election Observation Mission (EU EOM, 2023)** final report, which provides detailed assessments of digital election technologies, transmission challenges, and cyber-related incidents.

Credible Media Outlets: Articles from globally recognized media organizations such as **Punch (2024), Premium Times (2024)**, and **Premium Times (2023),** were reviewed for contextual evidence on cybersecurity breaches, misinformation, and public reactions.

Academic Publications: Peer-reviewed works on electoral technology, governance, and cyber risks in Africa such as **Sibe and Kaunert (2023)** and **IFES (2022)** offer analytical grounding and theoretical insight.

The selection of these data sources was guided by their reliability, relevance, and temporal alignment with the 2023 electoral period, ensuring a valid and evidence-based analysis.

Analytical Technique

Data were analyzed using **thematic analysis**, following the six-step model proposed by **Braun and Clarke (2006)**; (1) familiarization with data, (2) generating initial codes, (3) searching for themes, (4) reviewing themes, (5) defining and naming themes, and (6) producing the report. This analytical approach facilitates the identification of recurring patterns and discursive structures surrounding cybersecurity incidents and electoral governance.

Themes were derived from recurring issues in the reviewed materials, such as *cyberattacks on electoral infrastructure, disinformation and digital manipulation, institutional preparedness,* and *public trust.* The interpretive process linked these themes to the study's theoretical foundations: **Cybersecurity Good Governance**

Theory and the **Electoral Integrity Framework** to assess how cybersecurity vulnerabilities affected democratic accountability and election credibility in Nigeria.

Theoretical Lens

The analysis is guided by the integration of **Cybersecurity Good Governance** and **Electoral Integrity** principles, which together emphasize the relationship between secure digital systems and democratic legitimacy. The Cybersecurity Good Governance perspective underscores the importance of institutional coordination, transparency, and accountability in mitigating cyber risks (IFES, 2022). The Electoral Integrity Framework, on the other hand, provides a benchmark for evaluating how technological weaknesses can undermine electoral credibility, fairness, and public confidence (Norris, 2014).

By combining these theoretical lenses, the methodology ensures that data interpretation moves beyond technical evaluations to address broader governance implications, examining how cyber threats intersect with democratic processes and citizens' trust in electoral institutions.

Analysis and Findings

Cybersecurity Threats during the 2023 Elections

The 2023 Nigerian general elections marked a major test of the country's adoption of technology in electoral processes, especially with the use of the Bimodal Voter Accreditation System (BVAS) and the INEC Result Viewing Portal (IReV). Despite the anticipated improvement in transparency, the elections were marred by a series of cybersecurity-related challenges. One of the most significant issues was the **cyberattacks targeting INEC's online platforms**. According to *Premium Times* (2023), Nigeria recorded more than **12.9 million attempted cyberattacks** on election-related digital infrastructure during the presidential and National Assembly elections. These attacks ranged from denial-of-service (DoS) attempts to phishing campaigns aimed at compromising INEC's servers.

Moreover, the **INEC Result Viewing (IReV) portal** experienced **technical disruptions** and upload failures during the presidential poll. INEC admitted that configuration errors affected the real-time transmission of results, leading to

significant public concern and fueling allegations of system manipulation (*Premium Times*, 2023; *Punch*, 2024). These interruptions revealed not only the vulnerability of Nigeria's election technology but also the lack of comprehensive cyber resilience strategies.

Another challenge involved **disinformation campaigns and digital propaganda** that spread rapidly across social media platforms. Misleading narratives about vote manipulation and system hacks amplified public distrust. Observers, such as the European Union Election Observation Mission (EU–EOM, 2023), noted that misinformation on Twitter (now X) and WhatsApp played a central role in shaping negative perceptions of the electoral process.

Furthermore, **weak data protection** mechanisms raised concerns about the **privacy of voter information.** Without a fully operational cybersecurity response unit or a coordinated monitoring mechanism, INEC was slow to detect and mitigate breaches. The events highlighted the urgent need for secure data management practices within Nigeria's electoral institutions.

Impact on Electoral Integrity

The cybersecurity vulnerabilities of the 2023 elections had **far-reaching implications for electoral integrity** and democratic trust. The technical delays and irregularities in result uploads **eroded public confidence** in INEC's ability to safeguard the electoral process (*Punch*, 2024). Citizens expressed frustration over perceived transparency gaps, especially since the IReV portal was introduced to enhance openness and real-time accountability.

Institutionally, these failures **undermined the credibility and legitimacy** of both INEC and the election outcomes. According to *Premium Times* (2023), INEC's acknowledgment of technical faults and subsequent delays in publishing results created space for political actors to challenge the process, contributing to increased **post-election litigation** and heightened political tension.

The persistence of misinformation, coupled with perceived system failures, also fueled **citizen disillusionment and apathy**. The EU–EOM (2023) reported that the

low trust in digital election technologies diminished voter enthusiasm and participation, posing a challenge for future elections.

Collectively, these findings underscore the complex intersection between **cybersecurity and electoral integrity** in Nigeria. The 2023 elections demonstrate that technological innovations, while potentially transformative, can also become sources of vulnerability when not supported by robust digital governance frameworks.

Discussion

Implications of Weak Cybersecurity for Nigeria's Democratic Consolidation

The 2023 general elections underscored how fragile Nigeria's democratic consolidation remains in the face of weak cybersecurity infrastructure. Election technology is not merely a technical tool but a pillar of public trust and legitimacy (Daudu & Idehen, 2024). When digital platforms such as INEC's IReV portal and BVAS experience cyber disruptions or data compromise, citizens begin to question the authenticity of electoral outcomes. The resulting loss of trust undermines the electoral integrity framework, which emphasizes transparency, participation, and impartiality as essential elements of credible elections (Norris, 2014).

The Cybersecurity Good Governance Theory posits that secure information systems are integral to accountability, transparency, and effective governance (Rod & Weidmann, 2015). In this context, Nigeria's limited preparedness in preventing and responding to cyberattacks on election infrastructure weakened institutional legitimacy and hindered democratic consolidation. The breakdown of confidence in INEC's digital processes created an environment where misinformation thrived, further polarizing citizens along political and ethnic lines (EU–EOM, 2023).

Lessons from Global Best Practices in Securing Electoral Systems

Globally, nations have recognized that cybersecurity and electoral integrity are interdependent. For example, countries such as Estonia, Canada, and South Korea have institutionalized multi-layered cybersecurity frameworks that involve risk assessments, independent audits, and continuous training of election officials (Klimburg, 2021). These countries maintain public trust through transparency

mechanisms that allow citizens to verify digital processes independently, thus strengthening legitimacy.

In contrast, Nigeria's experience in 2023 highlights the absence of structured pre-election cybersecurity testing and post-election forensic audits. The International Foundation for Electoral Systems (IFES, 2022) emphasizes that adopting preventive security protocols, such as end-to-end encryption and offline backup verification, can mitigate technical failures. Integrating these global best practices would significantly enhance Nigeria's resilience against cyber threats and restore public confidence in digital democracy.

Role of Non-State Actors in Managing Digital Election Risks

The involvement of non-state actors, such as civil society organizations, media outlets, and technology firms, is pivotal in mitigating digital election risks. Civil society groups like Yiaga Africa and the Centre for Democracy and Development (CDD) played a watchdog role during the 2023 elections by exposing disinformation campaigns and demanding accountability from INEC (CDD, 2023). Similarly, media platforms such as *Premium Times* and *Punch* provided investigative reports that revealed the scale of cyberattacks and system failures, fostering transparency and public awareness.

Tech firms, particularly Meta, Google, and X (formerly Twitter), also contributed to managing misinformation through automated fact-checking and algorithmic content moderation (Meta, 2023). However, coordination between these actors and government agencies remains weak. So, strengthening multi-stakeholder collaboration is a key principle of cybersecurity governance that would enhance early detection, information sharing, and collective response to digital threats in future elections.

Institutional and Legal Gaps in Nigeria's Cybersecurity Governance Framework

Despite progress, Nigeria's cybersecurity legal and institutional architecture remains fragmented. The Cybercrimes (Prohibition, Prevention, etc.) Act of 2015, though comprehensive in addressing cyber offenses, lacks clear provisions tailored to the protection of electoral infrastructure (Akindipe, 2024). The National

Cybersecurity Policy and Strategy (NCPS, 2021) identifies election systems as critical national assets but fails to outline specific response mechanisms for cyber incidents targeting INEC platforms.

Moreover, institutional overlaps between the National Information Technology Development Agency (NITDA), the Office of the National Security Adviser (ONSA), and INEC have led to poor coordination during cyber incidents. This structural gap reflects weak cyber governance, a key determinant of democratic resilience under the Cybersecurity Good Governance Theory. Without explicit frameworks defining jurisdiction, data sharing, and emergency response, Nigeria risks recurring disruptions that compromise electoral credibility (Daudu & Idehen, 2024).

Recommendations

National Assembly should strengthen the National Cybersecurity Policy and Strategy (2021) to include explicit provisions for safeguarding electoral technologies, including BVAS, IReV, and electronic voter databases.

INEC should establish an Election Cybersecurity Incident Response Team (ECIRT) to monitor, detect, and respond to cyberattacks in real time during elections. This team should comprise representatives from INEC, ONSA, NITDA, and relevant security agencies.

There is need for enhanced inter-agency coordination between INEC, the Office of the National Security Adviser (ONSA), and the Nigerian Communications Commission (NCC) to streamline crisis management, intelligence sharing, and digital infrastructure oversight.

INEC should implement data protection and digital literacy programmes for electoral officials and citizens to promote cyber hygiene, reduce susceptibility to misinformation, and protect sensitive electoral data.

INEC should establish strong collaborate with social media companies such as Meta, Google, and X (formerly Twitter) to flag and remove coordinated disinformation campaigns that threaten electoral integrity.

Conclusion

The 2023 Nigerian general elections revealed critical vulnerabilities in the nation's electoral cybersecurity framework. Despite technological innovations like the BVAS and IReV portal, recurring cyberattacks, misinformation campaigns, and system malfunctions exposed how fragile Nigeria's digital electoral infrastructure remains (EUEOM, 2023; Premium Times, 2023). These challenges eroded public trust and raised concerns about institutional credibility and transparency in democratic governance.

Effective electoral integrity in the digital era demands a holistic cybersecurity strategy that aligns technology with governance principles of accountability, participation, and transparency (Rod & Weidmann, 2015; Daudu & Idehen, 2024). Strengthening institutional coordination, embedding cybersecurity into electoral policies, and fostering partnerships between government, civil society, and the private sector are vital for resilience.

Ultimately, Nigeria's experience serves as a wake-up call for African democracies transitioning toward digital governance. Proactive governance reforms and regional cooperation on election cybersecurity are essential to protect democratic institutions and ensure that future elections reflect the genuine will of the people (Akindipe, 2024; IFES, 2022).

References

Adebayo, T. (2020). *Cybersecurity and democratic governance in Africa*. Lagos: Routledge Nigeria.

Adebiyi, A. (2023). Transparency and technology in Nigeria's 2023 elections. *Journal of African Elections*, 22(1), 14–30.

Akindipe, D. (2024). *Spate of cybercrimes in Nigeria: Evidence of gaps in the legal frameworks.* Adeleke University Law Journal, 4(1), 105–112. https://aulj.adelekeuniversity.edu.ng/index.php/aulj/article/view/13

Akinola, O. (2023). *Election technology and public trust in Nigeria's 2023 elections*. Journal of African Governance.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Centre for Democracy and Development (CDD). (2023). *Disinformation and electoral accountability in Nigeria's 2023 general elections.* Abuja: CDD West Africa.

Chatham House. (2024). *Nigeria Presidential Elections 2023: Legal, regulatory and electoral technology framework.* Chatham House. https://www.chathamhouse.org/sites/default/files/2024-05/2024-05-15-nigeria-electtions.pdf

Daudu, S. O., & Idehen, S. O. (2024). *Legal and institutional framework for combating cybercrimes in Nigeria.* LexScriptio: Journal of the Department of Jurisprudence and Public Law, 1(1), 251–272. https://journals.kwasu.edu.ng/index.php/lexscriptio/article/view/142

Democracy in Africa. (2023). *Why did digital technology fail in Nigeria's 2023 elections?* Retrieved from https://democracyinafrica.org/why-did-digital-technology-fail-in-nigerias-2023-elections/ (democracyinafrica.org) Accessed 09/10/25

Ekhomu, O. (2019). *Cybersecurity and information protection in Nigeria*. Lagos: CSI Books.

European Union Election Observation Mission Nigeria (2023). *European Union Election Observation Mission Nigeria 2023: Final report*. https://www.eeas.europa.eu/eom-nigeria-2023/european-union-election-observation-mission-nigeria-2023-final-report_en Accessed 09/10/25

GIGA-Hamburg. (2023). *Overpromising and Underdelivering? Digital Technology in Nigeria's 2023 Presidential Elections.* Retrieved from https://www.giga-hamburg.de/de/publikationen/giga-focus/overpromising-underdelivering-digital-technology-nigerias-2023-presidential-elections (GIGA Hamburg) Accessed 09/10/25

Ibrahim, A. (2021). *Digital vulnerability and national security*. Abuja: Centre for Cyber Studies.

IFES. (2022, October 13). *Cybersecurity is fundamental to elections: Understanding cybersecurity throughout the electoral process.* International Foundation for Electoral Systems (IFES). https://www.ifes.org/publications Accessed 09/10/25

Independent National Electoral Commission (INEC). (2023). *Report on the 2023 general elections.* Abuja: INEC Press Office.

INEC. (2022). *Guidelines for the use of BVAS and IReV in the 2023 elections*. Abuja: Independent National Electoral Commission.

International Foundation for Electoral Systems (IFES). (2022). *Securing election technology: Lessons from global experiences.* Washington, DC: IFES Publications.

International Foundation for Electoral Systems. (2022, November). *Lessons on the use of technology in elections* (Election Case Law Analysis Series, Part 3). https://www.ifes.org/sites/default/files/2022-12/Lessons%20on%20the%20Use%20of%20Technology%20in%20Elections%20and%20the%20Impact%20on%20EDR_Final_0.pdf Accessed 09/10/25

International Institute for Democracy and Electoral Assistance (International IDEA). (2021). *Electoral technology handbook.* https://www.idea.int/publications/catalogue/electoral-technology-handbook

Klimburg, A. (2018). *The darkening web: The war for cyberspace*. Penguin.

Meta. (2023, November 27). *Our approach to elections | Transparency Center.* Meta Platforms. https://transparency.meta.com/features/approach-to-elections/

National Cybersecurity Strategy Indicators (NC SI / EGA). (2023). *Nigeria: National Cybersecurity Policy and Strategy 2021.* Retrieved from https://cert.gov.ng/ngcert/resources/NATIONAL_CYBERSECURITY_POLICY_AND_STRATEGY_2021.pdf (ncsi.ega.ee) Accessed 09/10/25

Norris, P. (2015). *Why elections fail.* Cambridge University Press.

Norris, P. (2017). *Strengthening electoral integrity.* Cambridge University Press.

Nwokedi, C. (2019). Electoral integrity and democratic consolidation in Nigeria. *African Journal of Political Science*, 13(2), 45–58.

OECD. (2019). *Good governance for critical infrastructure resilience: The cybersecurity dimension.* OECD Reviews of Risk Management Policies, OECD Publishing Paris. https://doi.org/1-.1787/02f0e5a0-en

Ojo, E. (2023). *Nigeria's 2023 elections: Innovations, challenges and lessons*. Ibadan: Safari Books.

Okoro, N., & Adeniran, A. (2022). Biometric technologies and electoral reform in Nigeria. *Journal of Communication and Governance*, 8(1), 22–37.

Olagunju, B. (2023). Cybersecurity risks and election management in Nigeria. *African Journal of Security Studies*, 5(1), 1–18.

Omotola, J. S. (2010). Elections and democratic transition in Nigeria under the Fourth Republic. *African Affairs, 109*(437), 535–553. https://doi.org/10.1093/afraf/adq040

Omotola, J. S. (2010). Electoral governance and democratic consolidation in Nigeria. *African Studies Review*, 53(2), 3–25.

Premium Times. (2023, March 15). *Nigeria recorded 12.9 million cyber attacks during presidential, NASS elections – Minister*. https://www.premiumtimesng.com/business/business-news/587712-nigeria-recorded-12-9-million-cyber-attacks-during-presidential-nass-elections-minister.html Accessed 09/10/25

Premium Times. (2024, February 23). *INEC gives details of IReV failure during 2023 presidential election*. https://www.premiumtimesng.com/news/top-news/671063-inec-gives-details-of-irev-failure-during-2023-presidential-election.html Accessed 09/10/25

Punch. (2024, February 23). *INEC admits IReV portal experienced challenges during 2023 presidential election*. https://punchng.com/inec-admits-irev-portal-experienced-challenges-during-2023-presidential-election/ Accessed 09/10/25

Rod, E. G., & Weidmann, N. B. (2015). Empowering activists or autocrats? The Internet in authoritarian regimes. *Journal of Peace Research*, 52(3), 338–351.

Sibe, R. T., & Kaunert, C. (2023). Technology, cyber security and the 2023 elections in Nigeria: Prospects, challenges and opportunities. *Journal of African Elections*, *22*(2), 68-85.

Situation Room Nigeria. (2023). *Report on Nigeria's 2023 General Elections.* https://situationroomng.org/wp-content/uploads/2023/06/Situation-Room-Report-on-Nigerias-2023-General-Election.pdf Accessed 09/10/25

Yiaga Africa. (2023). *Post-election survey on trust and technology in Nigeria's 2023 general elections.* https://yiaga.org