International Journal of Intellectual Discourse (IJID)
ISSN: 2636-4832 Volume 8, Issue 3. September, 2025

Technology Security and Electoral Credibility in Nigeria: A National Security Review of BVAS and IReV in the 2023 General Elections

*****Femi Samuel Oladele[1] Rashida Oyoru Adamu[2] & Moshood Olayinka Salahu[3]

[1,2&3]*Department of Politics and Governance, Faculty of Management and Social Sciences, Kwara State University, Malete, Nigeria.*

*****Corresponding Author: femi.oladele131@gmail.com

Abstract

Recent electoral cycles in Nigeria have witnessed the adoption of digital innovations aimed at improving the credibility of elections. However, the 2023 general elections exposed critical vulnerabilities in these technologies, including system malfunctions, delays in result transmission, and susceptibility to manipulation. While previous studies have examined their administrative and legal aspects, limited attention has been given to the national security implications of technological failures in elections. This study addresses this gap by investigating how insecure or poorly governed electoral technology can erode democratic legitimacy, trigger post-election violence, and deepen political instability. Drawing on securitization theory and democratic legitimacy theory, the research employs a mixed-methods design, integrating trend analysis (2019–2024), incident data, and qualitative insights from expert interviews and documentary sources. The findings indicate that when electoral technology is compromised, it becomes a driver of systemic distrust and insecurity. The study recommends a security-governance approach that treats electoral technology as critical national infrastructure, supported by legal reforms, cybersecurity safeguards, and proactive counter-disinformation strategies.

Keywords: Electoral technology, democratic legitimacy, national security, electoral integrity, cybersecurity, Nigeria elections.

1. Introduction

Elections remain the most legitimate mechanism for political succession in liberal democracies (Norris, 2014). However, in fragile or transitioning democracies such as Nigeria, electoral processes are often marred by irregularities, violence, and institutional distrust, factors that directly threaten national cohesion and internal security (Omotola, 2010; International IDEA, 2021). In response to growing public disillusionment with electoral integrity, the Independent National Electoral Commission introduced technological innovations such as the Bimodal Voter Accreditation System and the INEC Result Viewing Portal to enhance transparency and credibility (INEC, 2022). These innovations were institutionalized by the 2022 Electoral Act and were central to the conduct of the 2023 general elections (Electoral Act, 2022).

While the introduction of these technologies was widely perceived as a progressive shift toward transparent, real-time election management (NDI & IRI, 2023), their implementation revealed both significant potential and disturbing vulnerabilities. Technical failures, inconsistent data transmission, and reports of selective application of technology in different regions reignited longstanding

fears about electoral malpractice (Premium Times, 2023; The Cable, 2023). These developments did not merely have electoral implications; they exposed the fragile intersection between electoral credibility and national security (CDD, 2023). In contexts where citizens perceive electoral outcomes as manipulated or opaque, the legitimacy of state authority is undermined, heightening the risk of civil unrest, voter apathy, and long-term political instability (Bratton, 2008; Gyimah-Boadi, 2022).

Furthermore, the digitization of electoral processes opens a new domain of vulnerability in the form of cyber threats, disinformation campaigns, and data breaches (IFES, 2023). In a politically volatile environment, these vulnerabilities are not only technical glitches; they are strategic threats that can be exploited by domestic actors or external interests to delegitimize institutions, incite unrest, or polarize national discourse (UNDP, 2022). Thus, Nigeria's election technologies must not be understood solely as administrative tools but as core instruments in the broader national security framework.

This study therefore examines the 2023 general elections not merely as a democratic exercise but as a techno-security event with implications for the legitimacy, stability, and resilience of the Nigerian state. It interrogates how the deployment, and in some cases, the failure, of these technologies influenced public trust, electoral violence, and the perceived credibility of national institutions. In doing so, it situates electoral technology at the heart of Nigeria's internal security architecture and proposes strategic responses for safeguarding both the vote and the nation.

1.2 Problem Statement

Despite repeated electoral reforms in Nigeria, public confidence in the electoral process remains dangerously low, often culminating in electoral violence, post-election litigation, and growing voter apathy (Adebayo, 2023; Omotola, 2010). The adoption of digital technologies such as the Bimodal Voter Accreditation System and the INEC Result Viewing Portal was expected to curb historical irregularities by promoting transparency and enhancing accountability (INEC, 2022). However, the 2023 general elections exposed a critical paradox: while these tools were deployed to increase credibility, their uneven performance, technical failures, and perceived manipulations became flashpoints for national tension (NDI & IRI, 2023).

This breakdown in technological trust raises a deeper concern beyond electoral mechanics, it threatens the internal security of the Nigerian state. When election technologies fail or are perceived to be manipulated, they erode the legitimacy of political authority, exacerbate political polarization, and trigger civil unrest (Bratton, 2008; Gyimah-Boadi, 2022). Moreover, the digitization of election infrastructure introduces new vectors for cyberattacks, disinformation campaigns, and data sabotage, challenges Nigeria's security architecture is ill-prepared to confront (IFES, 2023; UNDP, 2022). Yet, existing literature and policy responses have largely treated these technologies as administrative innovations rather than strategic national security assets (CDD, 2023).

This neglect of the techno-security interface limits Nigeria's ability to anticipate, prevent, or manage the cascading security consequences of electoral distrust. A critical analysis is therefore necessary to assess how election technologies impact not just democratic outcomes but national stability, and to rethink how electoral credibility is central to internal security and governance legitimacy.

Research Objectives

1. To examine the security implications of technological failures or manipulations in electoral processes, including post-election violence, voter suppression, and public trust erosion.
2. To analyze the vulnerabilities of Nigeria's electoral technology infrastructure to cyber threats, disinformation, and strategic sabotage.
3. To investigate how electoral technology shapes national security dynamics, particularly in terms of legitimacy, internal stability, and public confidence in democratic institutions.

2. Literature Review

2.1 Conceptual Review

This section clarifies the key concepts underpinning this study: electoral technology, electoral credibility, national security, and technological vulnerability. Each concept is reviewed through multiple scholarly perspectives to establish the analytical framework for assessing how BVAS and IReV shape Nigeria's democratic stability.

1. Electoral Technology

Electoral technology refers broadly to the application of information and communication technologies (ICTs) in the design, administration, and monitoring of elections. According to Alvarez and Hall (2008), electoral technologies encompass both hardware (such as biometric verification devices, electronic voting machines) and software (such as result transmission portals and digital voter rolls) aimed at improving accuracy and efficiency. James (2020) expands this definition by emphasising the role of technology in strengthening transparency, enabling remote oversight, and deterring fraud.

In the African context, Cheeseman et al. (2018) note that electoral technologies are often introduced as part of international donor-driven governance reforms, but their adoption is shaped by local political incentives. In Nigeria, the Independent National Electoral Commission (INEC) introduced the BVAS for biometric authentication and the IReV portal for electronic result upload during the 2023 elections, with the stated aim of eliminating manual manipulation (Okereke & Okoro, 2023). However, the technology's effectiveness has been contested, especially where delays or breakdowns occurred, raising questions about whether the tools served as safeguards or new points of vulnerability.

2. Electoral Credibility

Electoral credibility has been conceptualised in different ways. Lindberg (2006) defines it as the degree to which elections are perceived as free, fair, and competitive, regardless of whether irregularities occur. Norris (2014) approaches it from a legitimacy standpoint, where credibility rests on both procedural compliance and public perception of fairness.

Empirical studies show that credibility is a multidimensional construct combining the integrity of the process, accuracy of results, and stakeholder trust (Mozaffar & Schedler, 2002; Birch, 2011). In Nigeria, Omotola (2010) argues that credibility hinges not only on electoral laws and institutional capacity but also on the absence of elite interference. While BVAS and IReV were designed to enhance credibility, perceived selective application during the 2023 elections undermined public trust, echoing earlier warnings by Posner and Young (2007) that technology cannot compensate for weak political will.

3. National Security

The concept of national security has evolved from its Cold War focus on territorial defence to a broader, human-centric perspective. Buzan et al. (1998) and Baldwin (1997) emphasise that contemporary security includes political stability, economic resilience, societal cohesion, and protection of critical

infrastructure. In Nigeria's National Security Strategy (2019), electoral legitimacy is explicitly recognised as a security concern because contested elections can provoke unrest, erode institutional authority, and invite opportunistic violence.

From a governance lens, Ayoob (1995) situates electoral stability within the framework of state-building in fragile states, arguing that legitimacy deficits in such contexts often translate into chronic insecurity. Thus, in Nigeria's 2023 elections, technological breakdowns not only affected electoral outcomes but also became a flashpoint for potential security crises in polarised regions.

4. Technological Vulnerability

Technological vulnerability refers to the susceptibility of electoral systems to malfunction, human error, or deliberate compromise. Norris (2017) categorises these vulnerabilities into technical risks (e.g., device failure, connectivity issues), human risks (e.g., inadequate training, procedural manipulation), and security risks (e.g., hacking, cyberattacks).

In emerging democracies, Hall (2015) warns that such vulnerabilities can exacerbate rather than resolve existing electoral tensions. Nigeria's 2023 experience illustrates this point: failures in BVAS authentication in some polling units and delayed IReV uploads created a perception of deliberate obstruction, which opposition parties linked to broader claims of electoral manipulation. As Adebanwi (2023) notes, in high-stakes political environments, even minor technical issues can escalate into legitimacy crises, fuelling distrust in both electoral bodies and the state itself.

Interlinkages Between Concepts

These concepts are not isolated. The deployment of electoral technology (BVAS, IReV) is expected to enhance electoral credibility, which in turn reinforces national security by mitigating electoral violence and political alienation. However, when technological vulnerabilities undermine this credibility, it can have destabilizing consequences, eroding the legitimacy of democratic institutions and precipitating security crises. Thus, managing the techno-security nexus in electoral processes becomes a national imperative.

2.2 Theoretical Framework

This study adopts a dual-theoretical lens, Securitization Theory and Democratic Legitimacy Theory, to interrogate the national security implications of BVAS and IReV deployment in Nigeria's 2023 general elections. These theories offer a complementary framework: while securitization theory helps to explain how electoral integrity becomes a national security issue, democratic legitimacy theory provides insight into how technological failure undermines state authority and stability.

1. Securitization Theory

Securitization Theory, as developed by the Copenhagen School (Buzan, Wæver & de Wilde, 1998), posits that issues can be transformed into matters of national security through a process of discursive framing. In this context, a political actor (e.g., a state or institution) identifies a particular issue as an existential threat to the state or society, thereby justifying extraordinary measures to address it. The theory shifts attention from objective threats to perceived threats, as constructed in political and public discourse.

Applying this to Nigeria's electoral context, the increasing politicization of electoral integrity and the technological platforms that support it, BVAS and IReV, can be understood as a process of securitization. When the public perceives these technologies as manipulated or malfunctioning, electoral outcomes lose legitimacy, and this delegitimization can provoke unrest, fuel ethnic and political polarization, and destabilize fragile democratic institutions. Thus, electoral technology, once a procedural tool,

becomes a matter of national survival and public order, a securitized issue.

In effect, securitization theory helps us understand why elections are not just democratic exercises but also security flashpoints. When trust in electoral technology breaks down, the discourse quickly shifts from democratic participation to existential crisis, undermining not only electoral outcomes but also national unity and internal stability.

2. Democratic Legitimacy Theory

Democratic Legitimacy Theory focuses on the normative justification of authority and governance in democratic systems. According to this theory, a government's authority is legitimate only if it derives from procedures that are transparent, inclusive, and reflective of the electorate's will (Beetham, 1991; Lipset, 1959). In electoral democracies, legitimacy depends not only on the act of voting but on the perception that the vote counts and that the system is fair and credible.

In this light, technologies like BVAS and IReV are not merely administrative instruments, they are mechanisms of legitimacy production. When they function effectively, they signal that the electoral system is transparent and trustworthy. However, when they fail or are perceived as tools of elite manipulation, as occurred in parts of the 2023 general elections, they undermine both procedural legitimacy (i.e., fairness of the process) and outcome legitimacy (i.e., acceptance of results).

This delegitimization has wider national security implications. In a highly polarized and conflict-prone state like Nigeria, electoral illegitimacy often leads to public protests, court disputes, inter-communal tensions, and even violence, all of which weaken state authority and erode internal peace. Democratic Legitimacy Theory, therefore, provides a normative and institutional lens through which to understand how electoral technology performance directly affects national cohesion and state legitimacy.

By integrating Securitization Theory and Democratic Legitimacy Theory, this study approaches electoral technology as both a symbolic anchor of state legitimacy and a potential trigger of national insecurity. BVAS and IReV, if mishandled, can transform routine democratic contests into existential battles over state control and public trust. Their success or failure thus has implications that extend far beyond electoral administration into the core of Nigeria's security and governance architecture.

2.3 Empirical Review

The empirical literature on electoral technology in Nigeria has expanded considerably in recent years, particularly with the introduction of biometric verification systems like the Bimodal Voter Accreditation System (BVAS) and the INEC Result Viewing Portal (IReV). These innovations, introduced to enhance electoral integrity, have attracted widespread academic and policy interest. However, most existing studies focus narrowly on their administrative efficiency or democratic implications, leaving underexplored the critical link between electoral technology and national security. This section engages with current empirical findings across three interrelated areas: performance and credibility, technological failure and public trust, and the security risks associated with electoral distrust.

Field-based evidence largely supports the proposition that BVAS has improved the credibility of voter accreditation. Udeh et al. (2023), in a survey conducted across four of Nigeria's six geopolitical zones, report that 67 percent of respondents believed that the deployment of BVAS curtailed voter impersonation and reduced incidents of overvoting. These findings are reinforced by the Policy and Legal Advocacy Centre (PLAC, 2023), which observed that BVAS significantly

increased the reliability of the accreditation process by ensuring one-person-one-vote compliance. The implication of this data is clear: BVAS functioned, in most cases, as a procedural enhancement, reducing the scope for manual manipulation and illegal accreditation.

However, this technical success at the front end of the electoral process was not mirrored in the transmission and collation phases. The IReV portal, introduced to allow citizens real-time access to polling unit results, failed to deliver on its promise during the presidential election. According to Yiaga Africa's Election Observation Report (2023), less than 40 percent of presidential results were uploaded within the first 24 hours. These delays triggered widespread allegations of tampering and selective transparency. The empirical pattern, therefore, reveals a bifurcated outcome: while the accreditation process was technologically robust, the collation and result-sharing process failed to uphold the same standard, opening the door to credibility challenges.

This credibility gap has been empirically linked to the erosion of public trust. Adebayo and Odukoya (2023), drawing from focus group discussions in Lagos and Kano, found that voters interpreted the IReV malfunction not merely as a technical glitch but as a deliberate act of electoral subversion. Participants widely viewed the failure as evidence of elite manipulation of digital platforms, reinforcing long-standing distrust in state institutions. In similar terms, Ajayi (2022) had previously cautioned that without institutional safeguards and real-time monitoring, electoral technologies in Nigeria could easily become new instruments for old patterns of electoral fraud. These findings underscore the danger of over-relying on technology in environments where political culture and institutional trust remain weak.

The threat to electoral trust was further amplified by the digital ecosystem. Iroanya (2023) study of social media reactions during the 2023 elections documented a sharp rise in disinformation and politically charged narratives, many of which were targeted at undermining confidence in the IReV system. These narratives often encouraged protests, cast doubt on electoral outcomes, and in some cases, called for civil disobedience. What this suggests is that technological failure, when coupled with a hyper-polarized media space, can serve as a catalyst for broader societal unrest.

Some studies have gone further to establish a direct link between failed electoral technology and violent conflict. For example, the centre for Democracy and Development (CDD, 2023) reported over 120 election-related violent incidents during and after the 2023 elections, many of which were precipitated by disputes over result transmission. These incidents were especially pronounced in states such as Rivers, Lagos, and parts of the North-Central zone, where electoral contests were highly competitive. Adebisi and Afolabi (2022) focusing on the security sector, argue that post-election instability is often exploited by armed groups and political thugs to assert local dominance. Their study draws a critical connection between electoral illegitimacy and the weakening of internal sovereignty, where loss of public trust in electoral processes translates into loss of state authority.

From a regional comparative perspective, Banda and Musavengana (2021) examine electoral digitalization across Nigeria, Kenya, and Zimbabwe. They conclude that electoral technologies only function effectively where they are backed by legal safeguards, institutional credibility, and infrastructural reliability. Where these are lacking, as was evident in Nigeria's 2023 elections, technology does not insulate against fraud or conflict. Rather, it may

amplify both, by raising expectations it ultimately cannot fulfil.

Despite the richness of these findings, a major empirical gap remains. The dominant approach in most studies is to analyze electoral technology within the framework of administrative efficiency or democratic development. There is insufficient attention to the securitization of electoral technology, how its failure can function as a threat multiplier, triggering unrest, weakening institutional legitimacy, and endangering national cohesion. This study departs from that approach by foregrounding BVAS and IReV not only as tools of democratic deepening but as instruments whose mismanagement carries tangible consequences for Nigeria's national security.

3. Methodology

This study adopts a qualitative descriptive research design to explore the relationship between electoral technology and national security during Nigeria's 2023 general elections. The choice of a qualitative approach is informed by the need to capture nuanced perspectives, lived experiences, and contextual realities that cannot be meaningfully reduced to numerical patterns. Drawing on an interpretivist epistemology, the study prioritizes depth of understanding over statistical generalization, focusing on how the deployment and breakdown of technologies such as the Bimodal Voter Accreditation System (BVAS) and the INEC Result Viewing Portal (IReV) influenced public trust, political legitimacy, and national stability.

The target population comprised stakeholders directly or indirectly involved in the conduct, monitoring, and security management of the 2023 general elections. From this population, ten key informants were purposively selected to ensure diversity of insights. The respondents included: three senior INEC officials, two security analysts with election monitoring experience, two leaders of civil society organisations focused on electoral reform, and three accredited election observers from both local and international missions. This sample size was chosen to balance depth with manageability, allowing for intensive engagement with each informant while ensuring representation across critical stakeholder categories.

Data collection employed semi-structured interview questions, designed to elicit detailed narratives while maintaining flexibility to probe emerging themes. Questions covered areas such as the operational efficiency of electoral technology, incidents of malfunction or sabotage, public perception of BVAS and IReV, and the perceived security implications of technological breakdowns. This format was selected to encourage open-ended responses, enabling participants to elaborate on complex issues in their own terms.

Primary data from the interviews were triangulated with secondary sources, including election observation reports from Yiaga Africa, Policy and Legal Advocacy Centre (PLAC), and Centre for Democracy and Development (CDD); official INEC documents; peer-reviewed academic literature; and verified media reports on disinformation campaigns and election-related violence.

Data analysis followed a thematic content analysis framework, with coding guided by both deductive categories derived from the securitization theory and democratic legitimacy theory, and inductive codes emerging from the interviews. This theoretical integration allowed the study to move beyond administrative performance metrics, situating electoral technology within broader questions of national cohesion, political trust, and internal security.

The study's geographic focus included flashpoint states Lagos, Rivers, Plateau,

and Kano, selected for their high electoral stakes, documented technology-related disruptions, and security sensitivities. While geographically and temporally bounded to the 2023 elections, the methodological rigour and triangulated evidence base ensure that the findings contribute meaningfully to both scholarly debates and policy considerations on electoral technology and security in fragile democracies.

4. Results and Discussion

Data Presentation

Introduction to Data Presentation

This section presents the quantitative findings of the study, derived from a multi-stage data collection process spanning 2019 to 2024. The data were compiled through a combination of official election reports, publicly available datasets from the Independent National Electoral Commission (INEC), credible media archives, and secondary academic analyses. The aim was to track the operational performance of Nigeria's electoral technologies, specifically the Bimodal Voter Accreditation System (BVAS) and the INEC Result Viewing Portal (IReV), and to examine their intersection with electoral security incidents over time.

The process began with the extraction of annual performance indices for BVAS and IReV, including deployment coverage, reported failure rates, result upload timeliness, and public trust levels. Public trust scores were obtained by averaging the results of nationwide opinion polls conducted by reputable survey organizations, normalized to a 0–100 scale. Each year's figures were cross-verified against at least two independent sources to enhance reliability.

The second dataset documents the security dimension of electoral technology, capturing five indicators: the number of physical and cyberattacks on electoral infrastructure, reported cases of result manipulation, election-related violent incidents, deaths linked to electoral violence, and confirmed technology hacks or sabotage. Incident counts were compiled from verified national security agency reports, election monitoring organizations, and triangulated media accounts. The period under review shows progressive expansion in technology deployment, paralleled by notable fluctuations in both performance efficiency and security risks.

The two tables presented below (Tables 4.1 and 2) outline these trends in detail. Table 4.1 illustrates performance metrics and trust patterns for BVAS and IReV between 2019 and 2024, while Table 2 presents recorded incidents linking electoral technology to security outcomes over the same period. The partial 2024 figures reflect preliminary data available at the time of analysis.

Table 4.1: Trend Analysis of Electoral Technology Performance Indices (2019–2024)

Year	BVAS Deployment Coverage (%)	BVAS Reported Failures (%)	IReV Result Upload Timeliness (%)	Public Trust Index in Electoral Tech (%)	Notes/Remarks
2019	60	15	N/A	45	BVAS pilot introduction in select states; no IReV deployment
2020	75	12	N/A	50	Expanded BVAS use; limited tech-related incidents
2021	80	10	30	52	IReV introduced in

					pilot states; delays reported
2022	85	8	50	55	Incremental tech improvements; mixed public trust
2023	95	5	38	42	Full BVAS deployment; IReV failures impact trust
2024*	97	4	45	44	Ongoing improvements; trust recovering slowly

Source: Researcher's computation from Independent National Electoral Commission (INEC) official election result releases, Nigeria Security Tracker (Council on Foreign Relations), reports from accredited election observer missions, and verified Nigerian media reports (2019–2024).

Table 4.2: Incidents Related to Electoral Technology and Security (2019–2024)

Year	Number of Attacks on Electoral Infrastructure	Reported Cases of Result Manipulation	Election-Related Violent Incidents	Deaths Linked to Election Violence	Reported Technology Hacks or Sabotage
2019	12	18	22	8	5
2020	10	15	19	5	4
2021	14	20	25	10	8
2022	17	23	30	12	10
2023	25	35	45	20	18
2024*	20	28	38	15	12

Source: Researcher's computation from Independent National Electoral Commission (INEC) official election result releases, Nigeria Security Tracker (Council on Foreign Relations), reports from accredited election observer missions, and verified Nigerian media reports (2019–2024).

The data trends between 2019 and 2024 and reveal critical insights into the deployment, functionality, and security challenges of Nigeria's electoral technology systems. Table 1 illustrates the progressive increase in BVAS deployment coverage, alongside a gradual reduction in reported failures, indicating enhanced technical reliability at the voter accreditation stage. However, IReV's performance, particularly in timely result uploads, remains inconsistent, reflecting ongoing operational and infrastructural challenges. This inconsistency correlates with fluctuations in the public trust index, which notably declined in 2023 following the IReV-related controversies.

Complementing these performance trends, Table 2 documents a rising pattern of security incidents linked to electoral processes, with spikes in attacks on electoral infrastructure, technology sabotage, and election-related violence particularly marked in 2023. These figures suggest a tangible connection between technological vulnerabilities and broader national security risks, underscoring the critical importance of securing electoral technology to uphold democratic legitimacy and political stability.

4.2 Thematic Analysis

1. Technological Failures and Electoral Trust Deficit

Despite increased BVAS deployment, rising from 60% in 2019 to over 95% in

2023, trust in electoral technology has declined (from 52% in 2021 to 42% in 2023). This paradox, seen in Table 1, highlights the growing divergence between institutional investment in election tech and public perception of its reliability. While BVAS largely succeeded in voter accreditation, significant IReV failures during result upload compromised transparency.

As one INEC official in Lagos observed:

"BVAS mostly worked well, but IReV glitches caused delays… this gave space for rumors to spread."

Election observation reports by Yiaga Africa (2023) confirmed this, citing over 30% of polling units nationwide where results were either delayed or never uploaded. In Plateau and Kano States, observers from the Centre for Democracy and Development (CDD) noted discrepancies between physical results and IReV uploads, igniting accusations of manipulation.

This digital malfunctioning shaped the post-election narrative, deepening distrust. The Public Trust Index, adapted from Afrobarometer data and local surveys, dropped sharply after the 2023 elections. As captured in Table 4.1 nd media commentaries (Premium Times, March 2023), many citizens associated IReV's failure with "deliberate institutional sabotage," eroding the gains made from BVAS deployment.

2. Electoral Technology as a Security Vulnerability

The 2023 elections marked a turning point in the securitization of Nigeria's electoral infrastructure. Table 2 shows a surge in attacks on electoral facilities (from 17 in 2022 to 25 in 2023), with an accompanying rise in reported technology-related sabotage. An INEC cybersecurity officer stated:

"There were clear signs of cyber interference attempts targeting IReV servers… meant to destabilize the process."

This aligns with reports by SBM Intelligence (2023) and the CDD, which noted at least 18 coordinated cyberattacks against electoral platforms, particularly during transmission phases. Several appeared to originate from within Nigeria, but some bore hallmarks of foreign digital intrusion, highlighting the hybrid nature of electoral threats.

Newspaper analysis from The Guardian and Daily Trust (February–March 2023) also reported digital blackouts in specific local government areas (e.g., Obio/Akpor in Rivers State and parts of Kogi), where results transmission was delayed for over 48 hours, fueling claims of systemic manipulation. The securitization theory helps frame this as a shift from routine administrative glitches to matters of national security and legitimacy.

3. From Technical Failures to Political Violence

Failures in electoral technology have increasingly translated into physical insecurity. In 2023 alone, Nigeria recorded 45 incidents of electoral violence and 20 election-related deaths (Table 2), the highest since 2019. In several hotspotssuch as Kano, Rivers, and Lagos, violence erupted following perceived manipulation of IReV data or its late arrival.

As a security field officer in Kano noted:

"Delays in result announcements… coincided with outbreaks of violence."

According to CLEEN Foundation's 2023 Election Security Report, technology-induced uncertainty played a catalytic role in sparking riots, especially where political margins were slim. This validates findings from Omodia and Ibietan (2021), who argued that the credibility of elections in fragile democracies depends not only on legal processes but on public perception of technological impartiality.

In Rivers, citizen protests turned violent when INEC offices failed to upload results 24 hours after voting. A civil society leader interviewed remarked:

"People doubted not just the election, but the government itself… voter skepticism turned into protest."

4. Electoral Technology and Democratic Legitimacy

The 2023 electoral crisis revealed the fragility of democratic legitimacy when technological systems collapse. As shown in Table 1, public trust in electoral technology fell by 13 percentage points between 2022 and 2023, despite improved infrastructure deployment. This suggests that perception, not performance alone, determines institutional credibility.

Democratic legitimacy theory is instructive here. When citizens perceive electoral outcomes as technologically compromised, confidence in institutions, and the state, is weakened. Interview data and press commentary from Sahara Reporters (March 2023) show a growing sense among Nigerians that

"electoral innovations are being used to mask elite manipulation."

This erosion of legitimacy has serious national security consequences. When democratic institutions are seen as rigged, whether manually or digitally, violent contestation becomes rationalized, especially among youths and political foot soldiers.

Extended Implications for Policy and Security Governance

The adoption of electoral technology in Nigeria, particularly the BVAS and IReV platforms, has fundamentally reshaped not only electoral administration but also the architecture of national security. While these tools were introduced to improve transparency and deter electoral fraud, the 2023 general elections exposed latent vulnerabilities that demand urgent policy and governance attention.

The deployment of digital electoral infrastructure cannot be divorced from the political economy within which it operates. INEC's procurement and logistical management of BVAS and IReV were shaped by opaque contracting processes, inadequate vendor accountability, and patronage-based allocations. According to BudgIT (2023), over ₦117 billion was allocated to election technology and logistics in the 2023 election cycle, yet widespread logistical failures were recorded in low-income and opposition-leaning areas. These failures contributed to a perception of state complicity in disenfranchisement, reinforcing patterns of political exclusion that fuel structural insecurity.

In this context, electoral technology becomes more than a neutral tool; it is a site of political contestation and elite bargaining. As long as procurement lacks transparency and oversight, confidence in the integrity of the electoral process will remain fragile, regardless of the sophistication of the technology.

When placed in comparative African context, Nigeria's experience reveals a recurring pattern: electoral technology often collapses in environments of weak legal safeguards, elite polarization, and limited civic literacy. Kenya's 2017 experience is instructive, the Supreme Court annulled the presidential election due to irregularities in the Kenya Integrated Election Management System (KIEMS), noting that "technology failed to deliver what the Constitution demands." Conversely, Ghana's smoother 2020 election, despite using similar biometric tools, benefitted from consistent public education, bipartisan consensus, and judicial predictability. These comparisons underscore the fact that technology alone does not guarantee security or legitimacy. It must be embedded in a broader political and institutional culture of accountability.

The post-2023 electoral landscape also revealed how digital technology can be weaponized through disinformation campaigns. Analysis by the Centre for Democracy and Development (2023) recorded over 1,800 coordinated online disinformation threads on platforms like

WhatsApp, Facebook, and Twitter, targeting INEC's credibility and spreading false results. These campaigns intensified in regions where IReV had delays or was completely offline, such as parts of Kogi, Rivers, and Abia.

The national security implication here is stark: information disorder can transform public distrust into physical violence, especially in volatile electoral contests. The absence of a coordinated response mechanism for digital falsehoods leaves the state vulnerable to hybrid threats, where perception warfare complements physical disruption.

At the institutional level, Nigeria's electoral framework remains underprepared to deal with the complexity of digital threats. The 2022 Electoral Act does not clearly define sanctions for cyber manipulation, systemic IReV sabotage, or vendor negligence. Moreover, INEC's independence is compromised when it lacks prosecutorial powers, cybersecurity autonomy, or a judicial fast-track mechanism for resolving tech-related disputes.

This regulatory lag creates a dangerous vacuum. While the front-end of elections is digitized, the back-end oversight, accountability, and enforcement is analog, reactive, and politicized. Without reform, Nigeria's digital elections will remain high-risk ventures, vulnerable to internal subversion and external interference.

5. Conclusion and Recommendation

Conclusion

In light of the evidence and thematic insights presented, it is clear that electoral technology has shifted from a peripheral administrative tool to a central actor in Nigeria's national security landscape. The failure of platforms such as BVAS and IReV during critical electoral junctures not only undermined public confidence but also exposed the fragile intersection between legitimacy, trust, and stability in a digital democratic era. This transition underscores the urgent need to reconceptualize electoral integrity as a security priority, not merely a governance concern.

The Nigerian state now faces a dual imperative: to secure its democratic processes not just from fraud, but from systemic breakdowns that threaten national cohesion. As democratic legitimacy becomes increasingly digitized, so too must the strategies that protect it evolve, grounded in institutional reform, digital resilience, and anticipatory governance. Electoral credibility is no longer an aspiration; it is a security imperative. Without this reorientation, the promise of reform will continue to generate disillusionment, and the crisis of confidence may deepen into a broader democratic retreat.

5.2 Recommendation

Based on the evidence, thematic insights, and strategic concerns identified in the research, the following targeted recommendations are offered to strengthen Nigeria's electoral process as a pillar of national security:

1. Institutionalize Electoral Technology as a Critical National Infrastructure

The Independent National Electoral Commission (INEC) should work with the National Security Adviser and the National Assembly to formally designate BVAS, IReV, and related platforms as Critical National Digital Infrastructure. This designation would prioritize them for cybersecurity protection, intelligence coordination, and disaster response, similar to how power grids and banking systems are secured.

2. Establish a Joint Electoral Cybersecurity Task Force (JECyTF)

A multi-agency task force comprising INEC's ICT unit, the Nigerian Communications Commission (NCC), the National Information Technology Development Agency (NITDA), and the Directorate of State Services (DSS)

should be created. Its mandate would be to anticipate, detect, and mitigate cyber threats, algorithmic bias, and coordinated sabotage during the electoral cycle.

3. Enact Legal Reforms on Digital Electoral Accountability

The Electoral Act should be amended to define clear penalties for technological manipulation, system failure due to negligence, and vendor fraud. This would close the current legal gap where technology vendors and officials escape liability even in cases of demonstrable failure. A dedicated Digital Electoral Offences Tribunal could ensure expedited hearings and enforcement.

4. Improve Public Communication and Disinformation Response Capacity

INEC must establish a real-time electoral information war room, in partnership with civil society and digital platforms, to counter false narratives and build digital trust. Lessons should be drawn from Ghana's 2020 Electoral Commission media center model, which issued timely clarifications and reduced information vacuums.

5. Reform Procurement and Logistics for Transparency and Equity

All contracts for electoral technology should be subjected to open competitive bidding under the Open Contracting Data Standard (OCDS). More importantly, the logistics chain must be decentralised and independently monitored to ensure timely delivery of sensitive materials, particularly to rural and conflict-prone zones.

6. Integrate Electoral Technology Training into National Security Curriculum

Security agencies, particularly the police and DSS, must be trained not only in election policing but also in recognising, preventing, and responding to digital electoral threats. This would enhance coordination during crises and foster a shared understanding of the electoral process as a security concern, not merely a political one.

7. Build Democratic Literacy around Technology

Finally, voters and party agents must be sensitised through nationwide digital literacy campaigns on how electoral technology works, what its limitations are, and how to report and escalate irregularities. This reduces vulnerability to disinformation and enhances participatory trust.

These recommendations, taken together, reposition electoral technology as a core element of Nigeria's national security strategy not just a democratic accessory. They seek to move Nigeria beyond reactive post-election conflict management toward preventive, system-wide digital resilience.

References

Adebayo, B. (2023, March 1). Nigeria's presidential election results under scrutiny amid claims of irregularities. CNN. https://www.cnn.com/2023/03/01/africa/nigeria-election-results-intl

Bratton, M. (2008). Vote buying and violence in Nigerian election campaigns. Electoral Studies, 27(4), 621–632. https://doi.org/10.1016/j.electstud.2008.04.013

BudgIT. (2023). Tracking the 2023 elections: Funding, logistics, and transparency gaps. BudgIT Foundation. https://yourbudgit.com

Centre for Democracy and Development. (2023). Nigeria's 2023 elections: Lessons for electoral integrity and democratic resilience. CDD. https://www.cddwestafrica.org

Centre for Democracy and Development. (2023). Disinformation and the 2023 elections: Trends, impact and countermeasures. CDD West Africa. https://cddwestafrica.org

Electoral Act, 2022. Federal Republic of Nigeria Official Gazette.

Gyimah-Boadi, E. (2022). Public trust in institutions and democratic backsliding in Africa. Journal of Democracy, 33(2), 112–126. https://doi.org/10.1353/jod.2022.0036

Independent National Electoral Commission. (2022). INEC guidelines and regulations for the conduct of elections. INEC. https://www.inecnigeria.org

Independent National Electoral Commission. (2022). Manual for election officials (Revised ed.). INEC Publications.

Independent National Electoral Commission. (2023). Report on the 2023 general elections. INEC Press.

International Foundation for Electoral Systems. (2023). Safeguarding election technology from cyber threats. IFES. https://www.ifes.org

International Foundation for Electoral Systems. (2023). Technology and trust in elections: Nigeria case study. IFES. https://www.ifes.org

International Institute for Democracy and Electoral Assistance. (2021). The global state of democracy 2021: Building resilience in a pandemic era. International IDEA. https://www.idea.int

National Democratic Institute & International Republican Institute. (2023). Joint election observation mission report: Nigeria 2023 general elections. NDI/IRI. https://www.ndi.org

National Democratic Institute & International Republican Institute. (2023). Joint election observation mission final report: Nigeria's 2023 general elections. NDI/IRI.

Norris, P. (2014). Why electoral integrity matters. Cambridge University Press.

Premium Times. (2023, February 27). Nigeria decides 2023: INEC's failure to upload results sparks outrage. Premium Times. https://www.premiumtimesng.com

Premium Times. (2023, March 2). IReV failures and electoral confusion: INEC's technology under scrutiny. Premium Times. https://www.premiumtimesng.com

The Cable. (2023, February 27). What went wrong with BVAS and IReV: Tech failures, vendor lapses and election day chaos. The Cable. https://www.thecable.ng

The Cable. (2023, March 2). How technology failed in Nigeria's 2023 elections. The Cable. https://www.thecable.ng

Transition Monitoring Group. (2023). Post-election report on technology use and voter confidence in Nigeria. TMG Publications.

United Nations Development Programme. (2022). Cybersecurity and elections in Africa: Emerging threats and responses. UNDP. https://www.undp.org.