Multidimensional Election Security Threats in Nigeria
Challenges, Options and Opportunities for the 2023 Nigeria General Elections
All rights reserved. No part of this book may be reproduced, stored in a retrieval system, transmitted in any form or means as electronic, mechanical, photocopying, recording, or otherwise without the prior permission of the copyright owner.

Published by Friedrich-Ebert-Stiftung Nigeria

Edited by
Chidiebere Ugwu & Abidemi Omotola

Contributors
Prof. Freedom Onuoha | Dr Chris Kwaja | Olajumoke Ganiyat Jenyo, PhD | Antonia T. Simbine, PhD | Hakeem Tijjani, PhD | Dr. Sunday Adejoh | Florence Kayemba IbokAbasi | Chidiebere Ugwu | Hanniel Hamisu Jafaru | Ekene Ikwelle | Austin C. Ekwujuru
Multidimensional Election Security Threats in Nigeria: Challenges, Options and Opportunities for the 2023 Nigeria General Elections – A Policy Brief

Introduction

The 2023 general election in Nigeria presents a unique set of challenges and opportunities for ensuring a secure and fair electoral process. On one hand, the country has made significant progress in recent years in improving the transparency and integrity of its electoral system. However, on the other hand, a number of multidimensional security threats continue to undermine the stability and legitimacy of the electoral process.

One of the most significant challenges facing Nigeria in the 2023 election is the threat of political violence and intimidation. This can take many forms, including the use of armed groups to intimidate voters, the use of state security forces to suppress opposition parties, and the use of propaganda and disinformation to manipulate public opinion. All of these tactics can undermine the integrity of the electoral process and the confidence of voters in the fairness and legitimacy of the election.
Another major challenge facing Nigeria in the 2023 election is the threat of cyber-attacks and interference. With the increasing reliance on electronic voting systems and the growing use of social media platforms to spread information and propaganda, the risk of cyber-attacks and manipulation of the electoral process has increased significantly. This can include the use of social media bots and trolls to spread false information and propaganda, as well as the targeting of critical infrastructure, such as election servers, to disrupt the electoral process.

**Election Security and the Security of Elections in Nigeria**

The conduct of elections is a very complex undertaking. The success or otherwise of an election is highly dependent on the nature of security infrastructures put in place, which makes security indispensable in the conduct of credible and violence free elections. In this context, provision of security for the
electorate, political party primaries, rallies and on the day of voting, are all components of the election cycle that are given security considerations by agencies of the state with the primary mandate of guaranteeing the security of the electoral process as enshrined in the constitution, electoral act and other policies relating to the conduct of elections. The Inter-Agency Consultative Committee on Election Security (ICCES) was then established with a view to facilitating effective election security management. In order to aid the work of the Committee, a unified Code of Conduct and Rules of Engagement for All Security Agencies in Electoral Duties was produced by the Chairman of INEC in collaboration with the heads of two other institutional partners in election security management (the National Security Adviser and the Inspector General of Police).

Within the Nigerian state, the Police is the lead agency with mandate for the security of election (Ese, 2019), which is viewed largely as an internal security issue. Though forbidden from direct participation in matters relating to elections (Ezeamalu, 2015), the military continue to play a key role in the Nigerian electoral process due to the level of insecurity in the country. In some instance, such involvement has generated mixed reactions as a result of either the utterances of the military as an institution (Abuh & Olaniyi, 2019), or the
conduct of its personnel on election duty, which borders on human rights violations (Vanguard, 2019).

Elections are the hallmarks of democracy, and they serve the purpose of peaceful change of government, thereby conferring legitimacy on the institutions that manage the electoral process in ways that respects the will of the people (Kelvin, 2018). Beyond the role of the electoral management institution in the conduct of the elections, its credibility is measured by the extent to which security is guaranteed and there is effective oversight on the agencies responsible for the provision of security. Where effective oversight of the security sector is in place, it’s always the combined effort of the legislature, executive, other independent institutions and the civil society that perform this oversight roles.

The Laws, the Technologies, the Vulnerabilities and the Elections

As Nigeria anticipates a more transparent election in the upcoming 2023 general election, the Electoral Act (2022) has transferred the mandate of introducing technology into the electioneering process to the Independent National Electoral Commission (INEC) (Electoral Act 2022). Although voting will still be cast manually via the ballot paper casting and open secret voting method, INEC has introduced different
technologies at specific stages of the election process. These technologies were introduced at the pre-election stage, election stage, and post-election stage.

For each of the stages one of the four interdependent technologies will be applied:

- INEC Voters Enrolment Device (IVED)
- Automated Biometric Identification System (ABIS)
- Bimodal Voters Accreditation System (BVAS)
- INEC Result Viewing (IReV)

For the pre-election stage, there is the INEC Voters Enrolment Device (IVED), an android device to be used for continuous voters’ registration (Mahmood. Y, 2021), and Automated Biometric Identification System (ABIS) which is used to clean the voter’s registration for duplicate and fake enrolment (Gana. N, 2022). For the election stage, there is the introduction of the Bimodal Voters Accreditation System (BVAS) which will be used for the accreditation of voters before voting and transmission of votes after collation at the polling unit (Mahmood. Y, 2022). Finally, for the post-election stage, there is the INEC Result Viewing (IReV) Portal, which is a public web portal for real-time viewing of results uploaded from the polling units (Mahmood. Y, 2022).
While the advocacy for the introduction of technologies in the electoral process is largely for transparency purposes, we should also understand that these technologies have their downsides. The potential risk of these technologies without necessary risk assessment analysis and mitigation can truly affect the overall objective of the 2023 general election process.

Potential Vulnerability of Technologies in the Electoral Process

1. **ABIS**: This device is running an Android Operating System, hence, has the potential of revealing the public IP of INEC server hosting the database of the voter's register, except if there are technologies such as VPN to create an encrypted tunnel and mitigate the risk.
2. **BVAS to IReV Portal:** There is a high tendency that cyber-attacks will be focused on both the BVAS and IReV (Jafaru. H, 2022). The objective of a cyber-attack on the BVAS will be to prevent the snapped results sheet from being transmitted to INEC Server. A cyber-attack on the IReV portal may include modification of the results on the portal or the disruption of the IReV Portal from the public. Notwithstanding, the modification of the results sheet may only be possible with the cooperation of a malicious insider, but disruption can be done with or without a malicious insider. The potency of risk that INEC should mitigate lies heavily in the possibility of both the cyber and political actors having an insider within INEC.

3. **Data Integrity:** There is a slim connection between the BVAS and IReV portal which is the transmission of results. However, the technological process for transmitting the captured election result sheet is a complex process that involves sending the captured sheet through several servers before it gets to the IReV portal. Hence the need to ensure that the integrity of the captured result sheet is secured.
4. **System Availability:** The introduction of technology in the electioneering process now means that the concern in addition to INEC Adhoc personnel will now include the technological devices that will ensure the process is transparent. While it will be difficult or impossible to bring down all the personnel before the election, it is quite easy to bring down the technologies using a denial-of-service attack methodology.

5. **Social Engineering & Insider Threat:** This is generally the most important and difficult threat to handle because it is focused on personnel to be used during the electioneering process. All the technological threats outlined above somehow depend on social engineering and insiders’ threat to be easily and effectively carried out.
The Critical roles of Women and Youth, the forgotten demography

The role of women and youth in addressing multidimensional threats to election security in Nigeria is crucial. Both groups have the potential to be powerful agents of change in promoting fair, transparent, and secure elections. The combined numerical strength of women and youth in Nigeria has always been explored and maximized by members of the political class for their electoral gains. These social clusters (women & youth) may determine the outcomes of the 2023 general elections in the country if they are mobilized either positively or negatively to participate in the electoral process.

Studies by Stakeholders Democracy Network (SDN) and others have shown that these significant segments of the Nigerian voting populations have both being victims and perpetuators of elections insecurity. Youths are usually recruited and deployed as political thugs to cart away election’s materials, disrupt the
electoral processes (especially in the strongholds of opposition political parties and their candidates) and unleash violent attacks on those with political dissenting voices so as to prevent them from participating in the electoral process.

On the other hand, most women provide espionage services to their male counterparts, as well as acting as custodians of the weapons and ammunitions they use in killing and maiming political opponents/supporters (including women and youths).

For women, participating in the electoral process and running for political office can help increase representation and ensure that their voices are heard. Women can also serve as advocates for election security and help raise awareness of issues such as vote buying and intimidation.

Youth, as the future leaders of the country, also have a vital role to play in promoting election security. By participating in voter education and awareness campaigns, youth can help ensure that their peers are informed and empowered to make informed voting decisions. Youth can also serve as advocates for election security, using their platforms to raise
awareness of issues and promote fair and transparent elections.

As Nigeria heads toward the 2023 general elections, the issue of security will determine if the elections hold or not. And the extent to which women and youth can gain positions in the political and decision-making structures will define how inclusive or restrictive Nigeria's governance process has become in over two decades of uninterrupted electoral democracy. Patriarchy, economic inequality, voter inducement, mobilisation of violence and social media are some of the core factors that will not only shape the level of women and youth participation in the 2023 elections but also election security.

The Threats

The 2023 general election in Nigeria is shaping up to be a critical moment in the country's political history. As the nation prepares to choose its next leaders, it is essential that the electoral process is fair, transparent, and secure. However, a range of multidimensional threats to election security are emerging that could undermine the integrity of the vote and the legitimacy of the outcome. The 2023 general election in Nigeria is expected to be a significant event that will shape the
future of the country. However, it is also vulnerable to various security threats that could compromise the integrity of the election. These threats can come in different forms.

One major security threat is the use of cyber-attacks to disrupt the electoral process. This can include hacking into voter databases, manipulating voter registration systems, and spreading misinformation online. These attacks can undermine the credibility of the election and lead to confusion and mistrust among voters.

Physical violence is another significant security threat in Nigeria's elections. This can include attacks on polling stations, voter intimidation, and violence against candidates and their supporters. These acts of violence can create a sense of fear and insecurity among voters, leading to low turnout and potential manipulation of the election outcome.

Voter intimidation is also a significant security threat in Nigeria's elections. This can include threats or coercion to influence voters to cast their ballots in a particular way or to stay away from the polls altogether. This can lead to a distorted election outcome and undermine the legitimacy of the election.
Shrinking Civic Space - There are indications that citizens (including women & youth) in opposing political parties in Nigeria may not have a conducive electoral space for electioneering ahead of the 2023 elections.

Some of the incumbent State Governors including Rivers, Akwa Ibom, etc are either out rightly denying opposing political parties access to public facilities (such as stadia, schools) for campaigns; or using administrative instruments like executive orders to fix exorbitant usage fees (5 million naira) that are huge enough to side-line them (especially those without the financial wherewithal).

This will likely stifle the electoral space for active participation of female and youth candidates and will place them at a disadvantage against their competitors in the ruling political parties who have access to the treasury of the State.

Secessionist Threats - the elections may renew calls for secession from different parts of the country - particularly in the Southeast where unknown gunmen suspected to be sympathetic to Indigenous People of Biafra (IPOB) have issued warnings to voters, though the organisation has repeatedly denied this claim. The delay in the release of the IPOB leader-Nnamdi Kanu
from the Department of State Security (DSS) custody after the recent Appeal Court judgement may exacerbate existing tensions in the Southeast region and is capable of impeding the electoral process (before, during & after), thereby limiting women & youth participation.

**Iswap/Boko Haram attacks on military installations** will definitely impact negatively on the turnout of voters (especially women) during political campaigns and elections. However, women and young people (including children) have been used by these terrorist cells as spies, arms suppliers/custodians, and fighters.

In recent times, military and para-military infrastructures have been attacked in Borno, Katsina, Kaduna, Taraba & Niger States, including the Zuma Rock security checkpoint where hundreds have been decimated, and their arms/ammunitions carted away.

Undoubtedly, the aim of the perpetrators is to unleash terror and instil fear in both the State security actors and the citizenry. This will definitely have grave impact on the voters’ confidence in the election’s security process.

**Militarization of the 2023 Elections** - Historically, young people (mostly cultists and militants) have been
recruited, armed and clothed in state security uniforms and integrated into the ranks of conventional military and para-military formations to prosecute electoral violence to the advantage of leading political parties in different locations. We observed this in Rivers State and elsewhere in the Niger Delta region during the 2015 & 2019 elections cycles.

**Emerging Trends in Electoral Fraud** - Corrupt political actors in Nigeria are now generating photocopies of PVCs and database of phone numbers of registered voters in their constituencies with the sole aim of buying their votes and possibly influencing their electoral choices. This has been spotted in places like Rivers State, and spells doom for the credibility of the 2023 elections outcomes. Again, women and youths are more vulnerable to this trap and bait owing to the growing poverty and unemployment trajectory in the country.

**Cultism** - Many studies have established the nexus between cultism and electoral violence in Nigeria, especially in the southern part of the country. It is also interesting to note that cult groups are polarized along political lines and are highly populated by the youths (both males and females) and are available tools in the
hands of desperate political actors for the perpetuation of electoral violence and fraud.

**Illicit Campaigns Financing** of political campaigns and candidates by such economic saboteurs as the notorious yahoo boys/girls/men/women, as well as drugs peddlers in an attempt to launder their criminal proceeds, and shields from prosecution. This will no doubt exacerbate the proliferation of small and light arms and weaponry around the 2023 elections season.

**Manipulation of election results** is another security threat that could compromise the integrity of the 2023 general election in Nigeria. This can include altering the results of the vote count, manipulating voter lists, or undermining the credibility of the election process. These actions can lead to disputes over the outcome of the election and potentially result in violence or unrest.

To address these and other security threats, Nigeria will need to adopt a range of measures to strengthen the resilience and integrity of its electoral system. This could include measures to improve the security of voting systems and infrastructure, such as implementing stronger cybersecurity protocols and enhancing the transparency of the electoral process.
Additionally, Nigeria will need to work to address the root causes of political violence and intimidation, such as addressing issues of inequality, injustice, and corruption.

**Options and Opportunities**

**Towards Effective Security Sector Oversight of the Electoral Process**

(i) **Strengthen Civil-Military Relations**: While the security sector is critical in ensuring security for the conduct of elections, the civilian population is key to providing the information required for action by the security agents. In this context, attention should be given to strengthening the relevant departments within the military structures, towards a more harmonious relations with the civilians. On the part of the civilians, key voices such as religious and traditional leaders, women and youth groups, as well as other social networks should be utilized as the link between the military and the civilian population.

(ii) **Strengthen Police - Community Relations on Peaceful and Credible Elections**: Though different forms of police-community platforms exist across the country, they were established largely to deal with issues relating to public safety and order, with little focus on elections. This critical platform should be strengthened through specialized training given to its
members with focus on how citizens can better collaborate with the police and other security agents in securing elections.

(iii) **Integrate Civil Society into ICCES**: Civil society will serve as a key link between ICCES and the people, as well as supporting them to establish an observatory for the monitoring adherence to the code of conduct and rule of engagements by security agents. By taking such a proactive step, the civil society is better placed to play a critical role of serving as bridge-builders between ICCES and the people.

(iv) **Strengthen Capacity for Early Warning and Early Response**: Security agencies should work with communities towards putting in place effective and comprehensive mechanisms for tracking early warning signs and responding to them. The fact is that the challenge is often not about early warning it has more to do with the extent to which they are responded to, using the existing infrastructure. On its part the government should provide the security agencies with the necessary equipment that are needed to make their work easy, and result driven in ways that increases citizens’ trust.

(v) **Monitor the Activities of Non-State Security Actors**: Though non-state security actors have played important role with respect to insurgency in Adamawa
State, they have been active in the conflicts between farmers and pastoralists. INEC should work with other security agencies in ensuring they monitor their activities towards ensuring they operate within the ambit of the law.

Towards Effectively Curbing Cyber Threats

(vi) Media fact-checking tools: There is urgent need for the Federal government through the National Broadcasting Regulatory Commission to establish a media fact-checking tools like the Politifacts which finds out when politicians are making false claims; Truth-O-Meter that tells the voters whether the politician is saying the truth or not, and Flip-O-Meter that tells when politicians are flip-flopping promises during campaign. This is because fact-checkers treats people as rational actors - it equips eligible voters with right information needed to make right and informed political decisions. As a corollary, fact-checker would help political actors to articulate issue-based campaign programmes reflecting the peculiar challenges of Nigerian state rather than relying on disinformation, misinformation and hate speeches as viable means of gaining access to political power.

(vii) Employing Technology exposure approach: since some of the important tool INEC might consider
using to avoid crashes are designing system, testing, set-up, configuration, piloting and auditing followed by contingency planning for the forthcoming election, The EMB should have back-up for the new technologies, also have advanced network monitoring capabilities to determine with some degree of certainty, the nature of events that occur in its systems and adoption of error detection software. Having a strategy on ground would allow the EMB to react quickly, apply contingency plans from back-up as a means to achieve data integrity in his data base against hackers.

**(viii) Employing Human exposure approach:** INEC should adopt monitoring physical access to servers to prevent insider attacks on the election data base with the organization website. This can be achieved through doubling up IT experts, when logging into sensitive servers, never using wireless networks for sensitive LANs to avoid close proximity, fraudulent Wi-Fi access attacks, control regularly by the ICT supervisor for compliance and abuse. Also, adoption of data security strategy to avoid having outdated or underutilized election systems that can lead to inefficient data management.

**(ix) Employing Political Exposure approach,** INEC should carefully plan and execute procurement
processes for election technology and develop sound communication and consultation mechanism on cyber security issues. Also, greater collaboration is required with the law enforcement agencies and intelligence personnel. In terms of legal and regulatory procedure, development of strategy document, operational plans, and training material and other manuals and guidelines are required on time.

Towards Effective Engagement of Women and Youth

(x) Capacitation Through Awareness Creation: Need for capacity-building programmes targeting women and youth that will enable them to understand how some political leaders use the politics of exclusion or tokenistic co-optation to subvert inclusive democracy in Nigeria. In this wise, civil society organisations should partner with the media and other relevant structures in the society (traditional and religious bodies, professional associations, and community-based groups) to intensify awareness creation and sensitisation programme for the youths on the need to shun violence and resist the temptation of politicians incentivising them to serve as their thugs.
Strategic Engagements for Force Multiplication: Incentivising women and youth-led organisations to embark on aggressive advocacy and campaign to conscientize and mobilise young persons to form a critical mass as they did during the #EndSARS movement and vote massively for credible candidates at the local, state and federal level elections. This is possible through collaborative initiatives like utilising technology for political mobilisation and participation during the 2023 general elections. This will enable women and youth optimise their demographic strength and leverage the same to bring about positive change in terms of increasing the number of women and youth in elective positions as well as electing credible persons committed to promoting an inclusive governance agenda.

Monitoring of Campaign Finance: Nigeria’s anti-graft agencies should partner with the INEC to evolve a robust collaborative mechanism for undertaking detailed and effective monitoring of political and electoral financing in Nigeria. Such collaborative frameworks should be deployed towards preventing and punishing corrupt practices such as vote buying. In addition, voter education campaigns should be expanded to counteract the effects of vote buying on voting behaviour.
(xiii) **Neutralising Violent Entrepreneurs and Actors:** State security and intelligence outfits need to discreetly and proactively neutralise violent youth wings or militias of politicians and political parties to prevent their mobilisation or deployment for political thuggery and election-related violence. This requires timely conduct of threat assessment, profiling of criminal elements or political thugs, proactive deployment for visibility policing, and strategic communication to counter violent incentives and narratives.

(xiv) **Framework for Responsible Use of Social Media:** Civil society organisations and media practitioners should initiate robust engagement with government agencies to evolve an acceptable guideline as a useful framework for promoting a culture of responsible use of social media in Nigeria. This will encourage users to exercise due diligence to avoid perpetrating unwholesome acts or sharing content in the social media that is capable of creating tension and violence before, during and after the elections.

Towards Effective Engagement of ICCES

(xv) **Monitoring:** Supervision and Shaming - Election-related actors, including voters, election workers, political parties, and the electoral administration, are
expected to operate impartially and professionally. While electoral monitoring missions serve a variety of purposes, the primary focus is on observing and documenting violence.

(xvi) **Mediation: Transfer of Trust to a Third Party** - In the technique of negotiation known as mediation, an outsider tries to involve the parties in a process whose goal is to resolve a dispute or conflict through communication and compromise. The foundation of mediation in tense situations is trust-building. When the participants in election disputes or violent acts do not trust one another, they may nevertheless be able to trust a neutral third party who is committed to mediating the situation. Mediators may make an effort to take into account the worries of each actor, look for agreements, and be successful in persuading the actors to agree to alter their behaviour. A variety of different actors participate in election-related mediation: electoral management bodies may send out mediation teams; local NGOs and/or community organizations may support and coordinate mediation efforts; and international organizations or states may take on higher-level mediation between the disputing parties (Hoglund and Jarstad, 2011:38).

(xvii) **Legal Measures: Setting Standards** - This strategy’s most crucial mechanism is that the law clearly defines the rules of engagement and establishes the criteria
for political activity. This approach is transparent and open to ensure that both politicians and regular persons are aware of the judicial norms. It offers a legal framework for controlling behaviour and aids in resolving conflicts through adjudication and judicial remedies. The election law frequently lays forth the basic judicial framework to handle electoral violence. Such legislation could outline the legal restrictions on the use of force, the purpose and authority of the organizations in charge of managing elections, and the requirements for candidates (Hoglund and Jarstad, 2011:38).

(xviii) Law Enforcement: Deterrence and Accountability

The legislative restrictions on the use of violence are powerless instruments if electoral laws are not upheld. By presence, supervision, investigations, arrests, and use of force, the police and other security forces, in some cases, ensure that electoral laws are upheld. The ongoing debate and possible establishment of an Electoral Offences Tribunal (EOT) may help curtail election-related insecurity.

(xix) Self-Regulation: Cultivation of Political Tolerance

By taking such actions, society as a whole can foster democratic norms of tolerance and moral commitment to nonviolence. Political parties and community-based organizations, including commercial cooperatives, religious institutions, and
civil rights organizations, among others, can play important roles as agents of violence prevention from below. Local agreements between electoral stakeholders and cooperatively agreed-upon discussions are included in the self-regulation strategy. The election-related parties use this tactic to try and control both their own and other people's behaviour. This bottom-up, neighbourhood-based approach has evolved into institutionalized peace mechanisms in South Africa (Hoglund and Jarstad, 2011:38).

(xx) **Creation of a Research Component within ICCES** - ICCES should create a research component in which investigation would be conducted before the election. There should be a collaboration between ICCES and academics.

(xx) **Domestication of ICCES** - ICCES should be decentralized in a way that its arms at both local government and state levels would be more active. This would allow quicker understanding of issues of electoral security within communities. The operational management scope of ICCES operations should be broader than it is at the moment. This is essential for the crucial security mechanism to have a widespread impact.
ICCESS should be Gender Inclusive - ICCES should have gender inclusiveness by admitting female civil society groups and more female security agents into its security operations. The women groups would assist the Committee in conducting risk assessments for women, which can be incorporated into the entire security assessments. This would, to a great extent, address violence against women before, during and after elections and as well, tackle gender inequality.
REFERENCE


