COMPUTERS AS BALLOT BOXES: DIGITAL VOTING IN NIGERIA, CONSEQUENCES AND INTERVENTIONS[1]**

Abstract

The promise of the e-elections as a tool for furthering a democratic culture has been heralded with much fanfare. With the just concluded 2023 elections Nigeria general elections. There has been clamour for adoption for full scale adoption of e-election by stakeholders in the country. Globally e-voting is the current trend of exercising electoral franchise. Countries like Estonia, Namibia, Brazil, Australia have adopted it. Its advantages are immense-they include - reduction of workload, ease of compilation of election results, timely announcing of election results, eradication of human error etc. Inversely, its potential in this respect is at risk. This article whilst appreciating the clamour for full blown e-election in Nigeria over the traditional means of voting from various quarters highlights the peculiar vulnerabilities associated with it. These vulnerabilities include the compromise of e-voting devices, by viruses or other malicious software, attacks by people with privileged access to the system, either system developers, system administrators or malicious hackers, denial-of-service, attacks among others. These risks are un-associated with manual voting. The article examines the preparedness by Nigerian government to face any challenges both teething and normal that may emerge as she transitions from manual to full blown electronic elections. These issues are highlighted purposely to tease out for the reader what is at stake in the event of adoption of e- election by the Nigerian State and proffer solutions to the challenges mentioned.

Keywords: E-Elections, Hacking, Democracy, Election Piloting

1. Introduction

With the just concluded 2023 elections marred with irregularities and violence, there is urgent need to stem voter apathy as most voters especially first-time voters were disillusioned. Stakeholders advocate for adoption of full-fledged e-voting as an alternative to the lack of transparency, loss of confidence and trust in electoral process that has encapsulated Nigerian manual voting system. Given that e-voting has potential to increase inclusion of marginalized groups, especially the disabled and residents overseas by making it easier for them to cast their votes in a more convenient and user-friendly way, cross section of citizens have been intensifying campaign for the adoption of full e-voting. Proponents of the e-election argue that firstly other countries in Africa and the western world are adopting e-elections. Nigeria should be in the fore front. Secondly, they cite the incidence of violence across polling booths across the country and argue that if voters were to vote through electronic voting in the comfort of their homes, the violence would not have occurred

Nigeria like other developing countries is enamoured by the notion of western ideas without careful assessment of the challenges involved. Given our inclinations for adopting foreign trends, it is only a matter of time before e-voting is a reality. There should be caution in wholly adopting new technology in future elections in Nigeria. This article argues that electronic voting is not fool proof and extreme caution should taken to safeguard the sanctity of votes should Nigeria adopt full blown internet voting in 2027.

[1] ***Obinne Obiefuna,** LLB, PhD Nigeria, LLM Essex B L., Lecturer in Law, Department of International and Comparative Law, University of Nigeria. obinneobiefuna @gmail.com

****Adrian Osuagwu,** LLB Nigeria LLM Nigeria PhD (in view) Department of International and Comparative Law, Faculty of Law University of Nigeria Nsukka University of Nigeria Nsukka

2. Overview of Nigeria's Tortuous Electoral Journey

Voting is a formal expression of preference for a candidate for office.[2] Centuries ago, people gave their lives in other to be allowed to vote.[3] In the early medieval times starting from Roman times, participating in elections was the sole preserve of upper class citizens; slaves and the poor freeborn were disenfranchised form the voting system. Nigeria practiced its first electoral franchise in 1922 under the Hugh Clifford's Constitution. The franchise given to Nigerians in this Constitution could be termed partial suffrage. The right to vote was limited to adult males resident in Lagos and who earned an annual income of £100. Nigeria did not achieve the status of universal adult suffrage until 1979 when women in the northern part of Nigeria were allowed to vote.[4] The sacrifice of our forebears to exercise this all-important right underscores the importance of elections. Election results should be deemed sacrosanct as lot of toil, sweat, blood and lives were sacrificed to achieve participating in the electoral process. In credible elections, citizens choose their representatives which leads to greater accountability and transparency among the elected.

2.1. Elections in Nigeria: Selection or Election?

Election rigging undermines the cardinal principle of democracy which upholds the welfare of the people as the object of government.[5] From historical experience, there are a huge number of challenges in manual electoral processes, these include poorly prepared or fraudulent voters' registers, inadequacy of electoral materials, (particularly the ballot papers) leading to disenfranchisement of voters, snatching of ballot boxes from INEC officials, difficulty in transportation of electoral materials especially ballot papers after voting has been concluded. Other issues include electoral malpractices and violence. For many politicians and political contestants, winning an election is a matter of life and death.[6] Election rigging and fraud are part of their overall campaign strategy; this is done in order to, either to gain an unfair advantage over their opponents, or to disrupt the process outright when it is clear that they have lost.[7]

The Post-independence elections in Nigeria was the beginning of rigging of manual elections in her history.[8] The tone for the 1964 elections was dictated by a set of events that took place in the period that followed independence in 1960. These were the imprisonment of Chief Obafemi Awolowo and senior members of his party, the creation of the Mid-Western region out of the Western region, the disputed census figures of 1962 and 1963, boycott of the election in the Eastern, Mid-Western regions in Lagos on allegations of rigging and fraud, and claims of opponent

[2]University Of Minnesota Human Rights Library, "The Right to Vote". Available at http://hrlibrary.umn.edu/edumat/studyguides/votingrights.htmlaccessed 6th February 2023

[3] In the mid nineteenth century, the women suffragist movement was born. This was to allow women to cast their votes at elections, See J. Purvis, "Letter Bombs and IED: Were the Suffragettes Terrorists?" 6th February 2018 available at https://news.sky.com/story/women-would-have-got-the-vote-earlier-if-not-for-suffragette-terrorists-11227772 accessed 28th March 2023.

[4]E Azinge , Right To Vote In Nigeria: A Critical commentary On The Open Ballot System. (1994) Journal Of *African Law* 38 (2)173.

[5] E Odike, H Faga. I Nwakpu, "Incorporation of Fundamental Objectives and Directive Principles of State Policy in the Constitutions of Emerging Democracies: A Beneficial Wrongdoing or a Democratic Demagoguery?"Available at http://file.scirp.org/Html/1-3300458_71212.htm accessed 15th March 2023.

[6]A former Nigerian President in 2007 stated that the 2007 general election was a do or die for his party. See K Larewaju, "Nigeria: Obasanjo Explodes –April Polls Do Or Die Affair For PDP" 11th February 2007 available at http://allafrica.com/stories/200702110015.html accessed 2nd March 2023.

[7]J Bavier, "Nigeria Do- or -Die Politics" 22nd April 2011. Available at https://pulitzercenter.org/reporting/nigeria-do-or-die-politics accessed 4th April 2023.

[8] The pre independence elections in Nigeria recorded little or no fraud because of the following reasons, the colonialist were still at the helm of the affairs , not much was at stake as executive powers and as such the country's purse strings were still firmly in the grasp of the colonialists

intimidation across the country.[9] The 1964 federal elections saw politicians of the first republic engage in battle for supremacy. The electoral process of the first republic was therefore severely flawed. The political parties lacked restraint; there was massive rigging, intimidation, oppression, violence and wanton killings. Under these pressures, the electoral process broke down completely.

The 1965 Western regional legislative election proved to be the last straw that broke the back of the First Republic. After this election, fragile peace could no longer continue and the wanton rigging at the election ensured that the demise of the republic was only a matter of time. The country's first military coup was fallout to the problems and dissatisfaction generated by the conduct of the first republic politicians. This subsequently led to the three-year civil war and the worst humanitarian disasters the country has ever known.[10] The Republic came to an end on the heel of flawed electoral system; the ghost of the crisis trailed the Military who took over the realms of power.[11]

During the 1979 elections, Nigeria adopted the presidential system of government in hope that the action will reinforce allegiance to the federation as a whole rather than to some particular section of it. An executive presidency was seen as a focus of national unity. Political parties were required to conform to certain norms and procedures, designed to ensure that they are federal in outlook. It was presumed that these factors would be able to lead to an avoidance of the troubles of the first republic which was brought on by regionalism. The electorate cast their vote on11th August 1979.

The outcome of this election was controversial as there arose the need to interpret the meaning of 'twelve two thirds' of nineteen states as the leading candidate did not secure 25% of votes in two-thirds of twelve states and two thirds of the local governments of the thirteenth state and. Thus, the government started on the back of legitimacy crisis.

The 1983 election was among the most chaotic ever held in the country.[12] The overall perception of the 1983 election by the populace was that it was massively rigged. There were accusations and counter-accusations from the political parties of intimidation, manipulation of ballot papers, thuggery and fraud. Against the backdrop of the disputed electoral outcome, President Shagari's second term began on a most inauspicious note.

The 3rd republic was however aborted by a coup d'état. The country was taken through her longest transition to civil rule as she witnessed more than a decade of military misrule. The transition to democracy timeframe was tinkered by the military government. The elections of 1992-1993 were frequently delayed, cancelled, postponed and adjusted to produce a result predetermined by the Military.

Following the decision to return to democratic rule, the election of 1999 was welcomed with the greatest of enthusiasm. Three parties were registered for the process. These were People's Democratic Party (PDP), All People's Party (APP), and Alliance for Democracy (AD). The elections witnessed massive rigging and frauds. PDP was the clear winner as it won the presidency, majority seats in the legislature and 21 gubernatorial seats. APP had 7 states governors while AD had 6 states.

The shortcomings of the 1999 elections were discountenanced due to the fact that it was a first election after more than a decade of military rule. The electoral outcome was generally favourable; though it was clear that the 'parties lacked internal democracy and discipline. The 2003

[9]J B Osabiya, Nigeria And Democratic Elections, 2008 *Journal Of Good Governance and Sustainable Development In Africa*. 2 (3).54.

[10]NWodu, "How Nigerian Elections Democratise Violence" 4th April 2018.Available athttps://thenerveafrica.com/16445/how-nigerian-elections-democratize-violence/ accessed 3rd April2023.

[11]Ibid.

[12]Ibid.

election was described as "a coup d'etat against the people."[13] The PDP made what was considered fraudulent in-roads to opposition's enclaves. PDP won more states to take its total to twenty seven states, majority holding in the legislature and the presidency.

The 2007 elections will go into history as one of the most criticized elections ever held in Nigeria.[14]This is because of the obvious flaws and frauds that characterized the elections. The violence that occasioned left not many in doubt about the illegality of the election.[15] The non-partisanship' of INEC which is supposed to be an independent and credible body was doubted more than ever. Every aspect of the election was far from fair and there were problems in the internal dynamics of some of the parties. The PDP alongside its lack of internal discipline engaged in several litigations and legal harassments of opposition thereby further putting a clause to the credibility of the elections. The fraudulent nature of the election was put in proper perspective with the chain of annulments and reruns pronounced by the election tribunals. This election also was also one of the few elections to be postponed due to poor logistic planning. The conduct of 2011 election came within improved legal parameters and ensured that the INEC independence was guaranteed. Indeed, there was reduction in the number of litigations in the tribunals compared to the 2007 elections. The sore point of the election was the violence that erupted at the close of the process in which 1000 lives were lost. [16]The violence seriously discredited the electoral process. The Corps members who were employed as Ad-Hoc staff were severely disadvantaged as majority of them especially in the North lost their lives in the violence that ensued as a result of the election. The 2015 election was equally marred by claims of election violence. A post mortem analysis of the 2019 general elections has documented how the collation process of the election results by INEC was opaque, chaotic, vulnerable to manipulation and, in some locations, violently disrupted.[17] five states accounted for 46 per cent of incidents of concern, noting that the situation was especially bad in Rivers State, where clashes between political thugs and security personnel, "reflecting de facto proxy battles between top politicians in the state. For the just concluded 2023 elections according to Prof Sam Amadi, he accused the independent national electoral commission of rigging the election. He stated that INEC has destroyed the safeguards of the elections. INEC deliberately chose to run a very flawed election. It is not technology, it is not logistic problem, it is a deliberate plan to rig the election.[18]

3. Challenges of Existing Voting System in Nigeria

Various factors challenge the performance of the existing traditional paper ballot system of elections in Nigeria. Traditional paper ballot election involves movement of people (electorates and electoral officials) and election materials to the polling units and collation centre for casting vote, tallying and results. Transporting election results through traditional means of transportation expose the results to numerous risks such as attack by political thugs, aggrieved party members; or manipulation by corrupt INEC officials. These constraining factors negatively affect the reliability of the traditional paper ballot system and put to question, the need for its continual adoption. The factors also open up

[13]J B Osabiya Nigeria and Democratic Elections, 2008 *Journal of Good Governance and Sustainable Developmentin Africa*. 2 (3) 54.

[14]Ibid.See also M Banire, "Card Reader And The Electoral Act, Any Conflict?" March 2nd 2017 available at http://thenationonlineng.net/card-reader-and-the-electoral-act-any-conflict-2/ accessed 15thJanuary 2023

[15]Ibid.

[16] Testing Democracy, Political Violence in Nigeria. Available at https://www.hrw.org/report/2003/04/10/testing-democracy/political-violence-nigeria accessed 18th January 2023

[17] Josiah Oluwole, How Security Operatives, INEC Officials, compromised 2019 Election Results https://www.premiumtimesng.com/news/headlines/349513-how-security-operatives-inec-officials-compromised-2019-election-results-report.html?tztc=1 accessed 29th April 2023

[18]Chuks Okocha INEC Deliberately Rigged 2023 General Election, Amadi Alleges, https://www.thisdaylive.com/index.php/2023/04/05/inec-deliberately-rigged-2023-general-election-amadi-alleges/ accessed 29th April 2023

a window for e-voting option for the simple reason that in e-elections, results are compiled and communicated electronically.

Issues bordering around franchise continue to heat Nigerian political discourse. Disenfranchisement of a large number of Nigerian immigrants living in foreign countries pose serious concerns as they are desirous of exercising their fundamental human rights.[19] In addition, electoral officials, security personnel on duty during election posted to places other than their polling units find it difficult to exercise their voting rights. The existing voting system does not support absentee voting; hence agitation from various quarters within Nigeria and abroad to explore viable voting system that allows voting right for those Nigerian citizens in Diaspora and the above mentioned category of citizens.[20]

Inadequate transparent mechanism is equally a problem of the existing voting system in Nigeria. Electoral officials manually collate, count and announce election results. Hence, the method is prone to danger of human error and deliberate manipulations. The susceptibility to rigging of the manual method of voting allows electoral officials with corrupt motives and their accomplice to easily rig election at every stage of the process unnoticed. Furthermore, the manual system allows for multiple voting, voting by non-eligible persons; intimidation of voters by scaring them away from casting vote or forcing them to vote candidates against their wishes. The above circumstances also inspired calls for exploration of robust election methods through IT.

Following complaints of irregularities in the 2019 election, INEC decided to improve on voters' accreditation for all elections by introducing the IREV INEC Result Viewing Portal and the BVAS Bimodal Voter Accreditation System. These technologies were designed to guarantee transparent accreditation and upload of polling unit results for citizens to view in real-time on Election Day in order to curb fraud.

4. E-Voting, the Bane of Electoral Fraud in Nigeria?

Adopting robust IT policies and programs has been termed the most effective solution to the problems of weak democratic practice in Nigeria.[21] Advocates of e-voting point out that electronic voting can reduce election costs and increase civic participation by making the voting process more convenient. Critics maintain that without a paper trail, recounts are more difficult and may open the door for electronic ballot manipulation and that poorly-written programming code, could affect election results.

These advocates of e-voting postulate that the advantage of e-voting over the conventional voting system is obvious. They uphold that convenience is an attribute of e-voting that enhance participation and remedy apathy associated with traditional voting methods. E-voting makes it easier for people to make their views known and cast their votes, an important requisite for constructive democratic process.

Abu-Shanab, Knight and Refai postulate that using e-voting improves the convenience, efficiency and effectiveness of the election process; reduces cost of organizing election, increases participation and improves integrity of election process in general.[22] Issues associated with inaccuracy, insecurity, fraud and forgery inherent in the conventional manual method of voting makes e-voting system an appealing option. According to Kozakova, modern democracy would

[19]INEC, NASS Make Case for Diaspora Voting available at http://www.inecnigeria.org/?inecnews=inec-nass-make-case-for-diaspora-votingaccessed 9th March 2023. See also F Falana "Voting Rights Of Nigerian Diaspora" 2nd May 2018 available at https://www.thisdaylive.com/index.php/2018/05/02/voting-rights-of-the-nigerian-diaspora/ accessed 9th March 2023

[20]Ibid.

[21] G Onu, A P Chiamogu, "E-Governance and Public Administration in Nigeria: A Discourse." 2012 *International Journal of Management*. Vol.2 (9), 1-8.

[22] E Abu-Shanab, M Knight, H Refai, "E-Voting Systems: A Tool for E-Democracy." *Journal of Management Research and Practice* Vol. 2, .(2010), pps.264-274.

maximally benefit from effective implementation of electronic voting technology.[23] Voting is not a cost-free activity as cost of transportation; searching for polling booth and travelling on election day are tangible cost that entail spending time and efforts.[24] Assessing the tangible cost of voting vis-a-vis immediate benefits of same often guides the decision of the voter to either vote or not. The easier voting becomes for citizens especially among the younger age, the more likely they are to participate in elections. Hence, a voting system that requires less effort such as punching a button or clicking a computer mouse is likely to gain more acceptance.

Such voting system increases voters' conveniences and confidence in electoral procedure, and is capable of improving the decline of voter turnout and perceived political apathy in Nigeria.[25]

4.1. Challenges of Transition to E-Voting System in Nigeria.

Polling place e-voting and remote e-voting systems of election have been used in different democratic societies. USA, Australia, Estonia, Japan, Brazil and India are at various stages of e-voting adoption. In Africa, Namibia was the first country that transitioned to e-voting in her 2014 general elections. Most ICT development projects and initiatives in developing countries are greeted with implementation, sustenance and maintenance challenge owing to lack of critical evaluation of the social environment in which these projects are transplanted.

Developing countries embrace western ideas, western culture and technology without assessing the readiness to sustain these ideas, the financial cost, and economic capital, intellectual capacity of citizens to absorb and appreciate these imported ideas. Due diligence studies are rarely commissioned to access the practicability of such foreign ideas.[26] The end result sometimes amount to the failure of these ideas in developing countries as well as the loss of the finance earmarked for these projects/ ideas .[27] For instance despite the enormous amount of funds channelled to the 2015 general elections to acquire the card reader, 41 % of the card reader failed; INEC had to resort to manual verification and accreditation.[28]This has stressed the need to address the challenges that arise from adoption e-elections.

---

[23] P Kozakova, "Can "E-Voting" Increase Turnout And Restore Faith In Politics?". Available at http://www.eotwonline.net/2011/09/01/can-e-voting-increase-turnout-and-restore-faith-in-politics/ accessed 9th May 2018.

[24] Ibid.

[25] M Burmester, E Magkos, "Towards Secure And Practical E-Elections In The New Era". Available at http://link.springer.com/chapter/10.1007/978-1-4615-0239-5_5 accessed 9th April 2023

[26] https://www.electoralcommission.org.uk/__data/assets/electoral_commission_pdf_file/0008/13220/Electronicvotingsummarypaper_27194-20114__E__N__S__W__.pdf accessed 9th April 2023

[27] The 2023 election cost three hundred and fifty five billion naira. See Dike Onwuameze, Rewane: 2023 May Be Nigeria's Costliest Elections Ever in History https://www.thisdaylive.com/index.php/2022/07/11/rewane-2023-may-be-nigerias-costliest-elections-ever-in-history/ accessed 9th April 2023

The 2015 election cost Nigeria $625 million .The country's huge cost of elections has surpassed that of the world's largest democracy, India, with a population six times bigger than Nigeria's. Nigeria, with 67 million registered voters, spent $625 million during the 2015 elections, translating into $9.33 per voter, according to data prepared by the National Institute for Legislative Studies (NILS) in 2015 the cost of running elections a cross country comparison. This figure is higher than the $600 million the Electoral Commission of India (ECI) said it spent during the 2014 general elections in which 553.8 million people voted out of 815 million registered voters. Nigeria's $625 million was spent in funding expenditure that included information technology systems and infrastructure; for instance the card reader, the NILS data said. See National Institute for Legislative Studies (NILS) article, "The Cost of Running Elections- a Cross Country Comparison" 10th of December 2015 available at http://nils.gov.ng/docs/cost_of_elections.pdf accessed 7th May 2018. See also N M Abdallah, "Nigeria's Election among the World's Most Expensive" 7th May 2018 available at https://www.dailytrust.com.ng/nigeria-s-elections-among-world-most-expensive.html aaccessed 9th April 2023.

[28] H Adebayo, "INEC Says Card Reader Test Successful, Admits 41% Fingerprint Failure", 10th March 2015 available at https://www.premiumtimesng.com/news/headlines/178264-inec-says-card-reader-test-successful-admits-41-fingerprints-verification-failure.html accessed 6th March 2023.

4.2. Legal Challenges.

The legality of the use of the SCR in the 2015 general elections was one crucial aspect of the debates that critics of the card reader contested. A careful study of the Nigeria's electoral jurisprudence is needed to determine whether the use of the smart card reader by INEC falls within the confines of the law. This debate is important because Nigeria does not run a full blown electronic voting system.[29]S.52 (1) (b) of the Electoral Act 2010 barred (INEC) from conducting elections in Nigeria by means of electronic voting. This bar was however lifted by the Electoral Amendment Act 2015. Specifically, Section 52(2) of the 2015 Amendment Act states that "voting at an election shall be in accordance with the procedure determined by the Independent National Electoral Commission." With the amendment of the law INEC was on *terra firma* when it determined to use the card reader machine for the accreditation of voters for the 2015 general election.INEC in exercise of the powers conferred on it by this section replaced manual accreditation with electronic accreditation. In *Shinkafi v Yari*,[30] Okoro J.S.C. rightly noted that "… the function of the card reader machine is to authenticate the owner of a voter's card and prevent multiple voting by a voter."

Subsequently On 14th of February, 2018, the Nigerian National Assembly passed the Electoral Act No. 6 2010 (Amendment) Bill 2018. This law section in 52 (2) gives the Independent National Electoral Commission (INEC) the express power to conduct Electronic Voting (E-voting) or any other method of voting as it may determine from time to time. This piece of legislation was however vetoed by the President. In his letter of veto, the president gave the reason for his veto by stating that the amendment bill was unconstitutional.[31] Where the National Assembly fails to override the veto of the president, S.52 (2) of the Electoral Act 2010 as amended in 2015 by the wordings of its provisions encompasses electronic voting. The only qualification is that INEC would be the sole body to decide how elections are to be conducted in Nigeria whether by electronic means or manual means.

4.3. Technology Concerns in Electronic Voting

E-voting faces a wide variety of potential attacks more than those considered in traditional elections. Issues of security of the systems, voter confidence needs to be tackled in e- elections. Election software is not just an ordinary application that has to be kept safe. Given that political power, control of the purse strings of a nation, are at stake in elections for public office, the incentive to cheat is enormous, and the consequences of a fraudulent outcome could threaten social order and national sovereignty.[32]These challenges faced in e-elections include insider attacks from system administrators, cybercriminals working for dishonest candidates, "hacktivists" seeking to disrupt elections as a form of political protest, and even sophisticated nation-states applying offensive cyber warfare capabilities. These attackers' goals can be roughly divided into three categories: (1) Tampering with the election outcome, e.g., to favour particular candidates; (2) Discovering how people voted, e.g., to retaliate against those who voted against the attacker's preferred candidates, as

[29] O Ezeigbo, "No Electronic Voting In 2019 says INEC" 12th April 2018. Available athttps://www.thisdaylive.com/index.php/2018/04/12/no-electronic-voting-in-2019-says-inec/ accessed 15th March 2023. Nigeria practises what may be termed a quasi e- voting system as the deployment of card readers is for verification and accreditation of voters and not for casting of votes proper.

[30](Unreported suit no 907/2015 of 8th January, 2016).

[31]The National Assembly has stated that it would override the veto see H. Umoru, "Election Reordering: Senators Commence Move To Override Buhari's Veto" 14th March 2018 available at https://www.vanguardngr.com/2018/03/election-re-ordering-senators-commence-moves-to-override-buharis-veto/ accessed 15th February 2023.

[32]JA Halderman "Practical Attacks On Real World E Voting". Available at https://jhalderm.com/pub/papers/ch7-evoting-attacks-2016.pdf accessed 9thApril 2023.

a means of enforcing vote buying or coercion; and (3) Disrupting or discrediting the election process, e.g., through denial of service attacks.

Defending against all these potential attacks simultaneously is difficult, for several reasons. Countermeasures against vote tampering—such as backups, logs, and receipts—tend to make it harder to strongly protect ballot secrecy. Likewise, mechanisms for protecting ballot secrecy such as encrypting voted ballots and avoiding incremental backups—make detecting and responding to compromise more difficult. [33]Election software may create large numbers of opportunities for bugs and vulnerabilities to occur. even if the code that's supposed to be running an election system is perfect, there is no way to guarantee that it is the actual code (and the only code) that is running on election day.[34]

Election systems are critical infrastructure, as important to defend as the power grid or financial system. Yet most deployed e-voting systems have been built to the same level of quality as typical commercial IT projects, far below appropriate level for critical infrastructure. These challenges have been compounded because many e-voting system vendors and election officials have shied away from rigorous public security scrutiny. They've used electoral laws, intellectual property claims, computer intrusion statutes, and non-disclosure agreements to create impediments for concerned citizens and security researchers.[35] It is untenable that officials and sceptical researchers are sometimes at odds, since ultimately both groups are working to see elections conducted well, and since voters have good reason to be worried about the current state of e-voting security.[36]

4.4. Hacking, Cyber Attacks and E-Elections.

Cyber-attacks have emerged as a new threat to information technology systems around the world. Consequently, the use of the internet for the e-voting will expose INEC to cyber-attacks. The threat of cyber-attacks in e-elections is real, as real as the nightmare of desperate politicians snatching ballot boxes and rigging the elections.Even the strongest nations in the world are not immune to it. The discovery in June 19 2017 of a website containing the personal information of 198 million US voters is another vulnerability of e-voting.[37] Privacy of voters is severely compromised by IT equipment long after elections have been won and lost.

Various local incidents support the stance that one should thread with caution in adopting of e-elections in Nigeria for example, during the accreditation exercise for presidential and national assembly elections in 2015, INEC website was hacked by a group which called itself Nigerian cyber army. The group said they hacked and took control of the website to protect results from being manipulated by anyone, through any means. They also claimed to be protecting the rights of Nigerians to elect their leaders. Analysis of the actions of the group portrays a worrisome trend. It shows that our cyberspace is not safe; websites of government establishments as well as private firms could as well be compromised by hacking. Inversely, this group could hijack INEC website and manipulate the information fed to INEC's website by the SCR. They may favour a selected candidate and amount to election rigging and stolen mandate which is the bane of manual elections in Nigeria. INEC confirmed the hack and stated that the hack will not affect the election results. It also said it was currently investigating the incidence.**[38]** Incidentally there has been no arrest or prosecution of these cybercriminals. In Nigeria we have a cybercrime specific legislation, the Cybercrime

[33] Ibid.
[34]Ibid.
[35]Ibid.
[36]Ibid.
[37]L Newham, "The Biggest Cyber Security Disasters Of 2017" available at https://www.wired.com/story/2017-biggest-hacks-so-far/ accessed 14th February 2023
[38]M Ibrahim, "Updated; Hacked INEC Website Restored", 28th March 2023 available athttps://www.thecable.ng/breaking-inec-website-hacked accessed 17th March 20238.

Prohibition Prevention Act, 2015. This should be invoked to bring the hackers to book. We equally boast of large police force whose duty is to eradicate crime. Statistics have shown that there is little conviction for cybercrime three years after passing the legislation. There is urgent need to regulate our cyberspace if the government is committed to introducing e-voting system of election. Nigeria has an inglorious reputation regarding cybercrime. She is ranked third in the world behind UK and US in internet crimes.[39]With the proliferation of cybercriminals in Nigeria, it is a given that they will become tools in the hands of unscrupulous politicians to rig elections**.** If this is unchecked, e- voting in Nigeria would be plagued with the same challenges of rigging, fraud, stolen mandate that bedevils manual voting. Lack of political will to ensure a functioning system in our society is a handicap that INEC has to surmount to ensure that a free and fair election is conducted.She will have to assure Nigerians that it has the capability to withstand cyber assaults on the new voting system if such attempts are made.

4.5. Financial challenges of E-Voting for Nigeria.

The 2015 election was Nigeria's costliest election owing to the use of SCR. This cost is set to increase if full e-voting is adopted in Nigeria; the cost of acquiring the electronic equipments, software, training of personnel, maintenance, support, public enlightenment needs to be factored in to weigh the benefits of embracing e-voting. Nigeria is in the throes of recession.[40] The slump in global oil price hit the economy hard, as such the economic situation of the country may not guarantee INEC the funds to run e-elections. The necessary costs for secure and reliable systems must be able to be reasonably met by the public purse. Where this is not possible, plans to adopt finance draining projects should be stalled. Precious foreign reserve should be channelled into worthwhile projects like the health sector, education sector among others.

5. Security Challenges of E-Voting System: Case Studies

Electronic voting machines are essentially general-purpose computers running specialized election software. Computer scientists have long been sceptical that voting systems of this type can be made secure. Experience with computer systems of all kinds show that it is exceedingly difficult to ensure the reliability and security of complex software to detect and diagnose problems when they do occur. The challenges faced by the Great Britain, The US, Brazil, India, Netherlands, Australia, Estonia will be analysed in this section

5.1. The Challenges faced by some selected Countries

(i) Great Britain

The UK trialled e-voting in the 2007 local government elections in various councils namely Shrewsbury & Atcham, Sheffield, Rushmoor and Swindon councils.[41] In the aftermath of the elections, the UK Electoral Body commissioned a report on the outcome of these e- elections.[42] It was found that a significant number of polling stations experienced technical problems at some time or another on polling day, resulting in 28 hours of total downtime (3% of voting hours). Furthermore, three of the councils experienced difficulties in setting up the polling stations, a complex logistical exercise that involves putting networked technology into a variety of locations. In the long run they

[39] "Nigeria Third In Global Internet Crimes Behind UK and US ,says NCC." available at https://www.vanguardngr.com/2017/08/nigeria-3rd-global-internet-crimes-behind-uk-u-s-says-ncc/ accessed 3rd March 2023

[40]Breaking Nigeria out of Recession-NBS ,5th September 2017 available at https://www.vanguardngr.com/2017/09/breaking-nigeria-recession-nbs/3rd March 2023

[41] Prior to this E- election was also trialed in 2003.

[42] Electoral Commission. Report available at https://www.electoralcommission.org.uk/__data/assets/electoral_commission_pdf_file/0008/13220/Electronicvotingsummarypaper_27194-20114__E__N__S__W__.pdf accessed 4th March 2023

had to allow the e-voters to switch to a paper vote on the production of suitable identification documentation.

There was particular concern for cost and value for money, with costs for e-voting varying from approximately £600,000 to £1,100,000. The cost per e-voter was extremely high in some council, varying from about £100 to £600. Similarly different confusing terminology was used for the password, including 'username,' 'password' and 'passcode'. Sometimes the name used was confusing, such as referring to a password but requiring a numeric code. This caused a number of electors to fill in their registration form incorrectly. The Report equally found that call centre logs and additional anecdotal evidence revealed that a significant number of electors subsequently forgot their password or passcode on attempting to vote. In some instances, there were inconsistencies in the date format accepted by the voting interface. The quality and testing arrangements were found to be inadequate.

Equally, the level of security assurance of the elections was below that associated with other government IT projects, and best practice in security governance was not followed. The Electoral Commission recommended that trialling of e- elections is not explored further until measures that would address the problems highlighted in the findings are put in place. Britain moved back to casting ballots by post and voting manually at polling stations.

(ii) India

India, the world's largest democracy, is also the world's largest user of e-voting. In the 2014 parliamentary election, more than 550 million voters cast their ballots on 1.4 million machines.[43] Indian EVMs lack upgradable software and interfaces for digitally loading ballot designs or offloading results. Instead, workers press buttons to reset the machines and set the number of candidates on the ballot. After the election, the control unit shows the vote total for each candidate on an LED display. The Election Commission of India has never permitted a rigorous independent security review of the machines, and has kept many details of their design secret, but it has maintained that they are "fully tamper-proof."[44] This claim was challenged in 2010 by researchers.

The researchers collaborated with an anonymous government whistle-blower.[45] The researchers demonstrated two attacks that involve physically tampering with the machines' hardware. The first attack was to replace the LED display in the control unit with a look-alike that would substitute fraudulent totals when showing the election results.[46] The dishonest display contained a hidden Bluetooth radio that the attacker would use to select the winning candidate on a smartphone app. The second attack was a digital form of ballot box stuffing—which had been a widely reported problem in India prior to the introduction of e-voting. The researchers constructed an inexpensive hand-held device that could be attached to the EVMs' memory chips to quickly modify the vote records. A few months after the researchers published their study, one was arrested by authorities demanding to know who provided the machine[47] . The arrest drew national and international attention and led the leaders of India's major political parties to ask the Election Commission to implement a paper trail and other security measures.[48] In 2013, the Supreme Court

[43] See footnote 47 above.

[44] Ibid.

[45] S Wolchok, E Wustrow, J Alex Halderman, H K Prasad, A Kankipati, S Krishna Sakhamuri, V Yagati, R Gonggrijp. Security Analysis of India's Electronic Voting Machines. *In ACM conference on Computer and Communications Security*, (2010) CCS'10, pages 1–14.

[46] Ibid.

[47] J A Halderman. "Electronic Voting Researcher Arrested Over Anonymous Source", August 2010. Available https://freedomto-tinker.com/blog/jhalderm/electronic-votingresearcher-arrested-over-anonymous-source/. accessed 9th May 2018

[48] Ibid.

of India ruled in *Swamy v. Election Commission of India,*[49] that such a paper trail was "an indispensable requirement of free and fair elections" and directed the government to fully implement the paper trail.

(iii) The United States,

The use of electronic machines was the most widely deployed electronic voting platform in the U.S. In the November 2006 general election, they were used in 385 counties representing over 10% of registered voters. More than 33,000 of the machines were in service. The first major study of these machines was carried out in 2003 and many design errors and vulnerabilities were discovered.[50] The manufacturers responded that the findings were "unrealistic" and pointed out that the researchers did not test with a real voting machine or a production version of the software.[51] Public concern in light of the revelation led the State of Maryland to authorize two security studies. It was confirmed by the studies that the system was at high risk of compromise. Problems with a software update mechanism that could allow malicious parties to replace the programs that operated the machines were equally discovered.[52]

The same year, researchers at Princeton University conducted independent research on e-voting machine- named TS and reverse engineered its hardware and software. They confirmed that anyone who had physical access to the machine—or to a memory card that would later be inserted into a machine - could install malicious software. Where the malicious software is installed, the machine would launch Windows Explorer in place of the election software, allowing an attacker to manipulate the software and files on the machine.

The researchers also found that a hacker can install vote-stealing malware that modified all of the vote records, audit logs, and protective counters stored by the machine, so that even careful forensic examination of the files would find nothing amiss.

Furthermore there could be malware installed that can allow the attacker to interactively control which candidate would receive what fraction of votes. The malware parsed each new ballot as it was cast and then switched the minimum number of votes necessary to ensure that the favoured candidate always had at least the desired percentage of the total.

It was also discovered that the possibility of developing a voting machine virus is real. To prove this point, the researchers developed a voting machine virus that could spread the vote stealing code automatically and silently from machine to machine during normal pre- and post-election activities. Once installed, the virus copied itself to every memory card inserted into the infected machine. If those cards were inserted into other machines, they too would become infected. As a result, an attacker could infect a large population of machines while only having temporary physical access to a single machine or memory card. Once the virus infected a machine, removing it would require factory service, since the malicious boot-loader disabled in-field software updates.

Following these vulnerabilities, two states in the US commissioned comprehensive security reviews of their election technology that encompassed products from several major e-voting vendors. In 2007, California Secretary of State Debra Bowen organized a study, the California Top-to-Bottom Review[53] that examined electronic voting systems in the state. The study discovered vulnerabilities

[49] Unreported Civil Appeal No. 9093 of 2013. Judgment, October 8, 2013.Available at http://supremecourtofindia.nic.in/outtoday/9093.pdf aaccessed 9th May 2018.

[50] T Kohno, A Stubblefield, A Rubin, D Wallach, Analysis Of An Electronic Voting System in IEEE Symposium On Security And Privacy 2004. P. 2.

[51]"Diebold Election Systems. Technical Response to The Johns Hopkins Study on Voting Systems", 2003 Available at http://www-personal.umich.edu/ ~wmebane/gov317/diebold/technical.25jul2003.htm accessed 24th March 2023.

[52]Ibid.

[53] California Secretary of State's Office. "Top-to-Bottom Review of Voting Systems, Main Website", 2007. http://www.sos.ca.gov/elections/ voting-systems/oversight/top-bottom-review/ accessed 20th March 2023.

that attackers could exploit to install malicious software on the voting machines. These flaws could be used to spread a vote-stealing virus that would propagate even more efficiently and be more difficult to detect than the virus developed by the Princeton team. Furthermore, the electronic voting machine (EVM) failed to protect ballot secrecy, since the digital ballot records were retained in the order in which they were cast and contained a time stamp for each vote. This would allow election workers who observed the order in which individuals cast their ballots to discover how those individuals voted. The study concluded that the vulnerabilities in the EVM system result from deep architectural flaws. These flaws could allow vote-stealing code to spread virally and compromise both the integrity of the election result and the secrecy of voters' ballots. Secretary Bowen decertified DRE voting machines from all three vendors and then recertified them for limited use subject to stringent security and post-election auditing requirements.[54]

Similarly in 2007, Ohio Secretary of State Jennifer Brunner initiated a similar state-wide voting review.[55] The study examined systems from Elections Systems in place for voting in that state. They found yet more vulnerabilities that had been overlooked in the earlier security reviews. In the wake of these studies, most U.S. states moved away from e voting. By the 2014 general election, 70% of American voters were casting ballots on paper.[56]

Another challenge highlighted by the study was surrounding the life-cycle of e-voting machines. The question was whether they can be safely discarded when they are taken out of service. Some EVMs still contain vote records from real elections.[57] This seriously hampers the privacy of the voters by storing their personal information over and above time stipulated. Thus, every time the EVMs are rigorously assessed, researchers have found serious vulnerabilities.

5.2 Internet Voting

Conducting elections for public office over the Internet raises severe security risks, beyond even those facing poll-site systems. Election servers must be accessible from the public Internet, exposing them to the potential for remote compromise and denial of service. Voters interact with these servers from their own devices, which are frequently infected with malware. Several researchers have catalogued threats to internet voting, even as others have proposed systems and protocols that may be steps to solutions someday.[58] Although a number of states and countries have forged ahead with systems for collecting votes online, every such system that has received rigorous independent security scrutiny has been shown to have significant vulnerabilities. Among the practical challenges to secure internet voting is the inadequacy of election software security.

While this approach is suitable for the economic and risk environment of typical home and business users, it is not appropriate for critical security systems, such as voting applications, due to the severe consequences of failure. Architectural brittleness in web applications is complicated, and small mistakes in the implementation and configuration of web applications can result in total compromise.[59] This is illustrated by the vulnerabilities in the Washington, D.C. and New South Wales web-based Internet voting systems, described below. In both cases, vulnerabilities resulting from small oversights jeopardized the integrity of election results. Internet voting systems necessarily use servers that are accessible from the public Internet. Consequently, they expose what

[54]Ibid.

[55] Ohio Secretary of State's Office. Evaluation and Validation of Election-Related Equipment, Standards and Testing (EVEREST), 2007. http://siis.cse. psu.edu/everest.html accessed 9th March 2023.

[56] C Bennett. States ditch electronic voting machines, November 2, 2014. Available at http://thehill.com/policy/cybersecurity/222470- states-ditch-electronic-voting-machines accessed 13th March 2023.

[57]JA Halderman "Practical Attacks On Real World E Voting". Available at https://jhalderm.com/pub/papers/ch7-evoting-attacks-2016.pdf accessed13th March 2023.

[58] Footnote 47 above.

[59]Ibid.

might otherwise be a regional election to attackers from around the globe. Over the past decade, attackers have become increasingly sophisticated, and critical systems such as election software now face potential attacks from advanced cybercriminals and even state-sponsored attacks.[60] In addition to compromising the central voting server, attackers could launch denial-of-service attacks aimed at disrupting the election, they could try to redirect voters to fake voting sites, and they could conduct widespread attacks on voters' client machines, perhaps using pre-existing botnet infections. These threats correspond to some of the most difficult unsolved problems in Internet security and are unlikely to be overcome soon.

While Internet-based financial applications, such as online banking, share some of the threats faced by Internet voting, there is a fundamental difference in ability to deal with compromises after they have occurred. In the case of online banking, transaction records, statements, and multiple logs allow customers to detect specific fraudulent transactions - and, in many cases, allow the bank to reverse them. Internet voting systems cannot keep such fine-grained transaction logs without violating ballot secrecy for voters. Even with these protections in place, banks and merchants suffer billions of dollars of online fraud every year but write it off as part of the cost of doing business.[61] Fraudulent election results cannot be written off.

(i) Internet Voting System Challenges: The Washington D.C. Experience.

In 2010, the District of Columbia developed an Internet voting pilot project that was intended to allow military and overseas absentee voters to cast their ballots using a website. Prior to deploying the system in the general election, the District held a unique public trial: they conducted a mock election during which anyone was invited to test the system or attempt to compromise its security.[62] A team from the University of Michigan test run the system. Within 36 hours of the system going live, the Michigan team had gained nearly complete control of the election server. They successfully changed every vote and revealed almost every secret ballot. Election officials did not detect their intrusion for nearly two days and might have remained unaware for far longer had the intruders not deliberately left a prominent clue. This case study was the first to analyse the security of a government Internet voting system from the perspective of an attacker in a realistic pre-election deployment. The story, which the Michigan team recounted in a later research paper,[63] dramatically illustrates the dangers and challenges that face Internet voting in practice. The key finding to the research were the ease which they could steal secrets. As soon as they had beached the server, they began collecting crucial secret data, including the database username and password, the public key used to encrypt the ballots, and log, history, and configuration files. This information would aid the attackers in compromising the system again if their infiltration was discovered and cut off. The hackers could also change past votes. They modified all the votes that had already been cast, replacing them with ballots marked with write-in votes for other candidates. Although the system encrypted voted ballots, the attackers simply discarded the encrypted files and replaced them with forged ballots that they encrypted using the public key they had stolen. Furthermore, they were able to compromise the secret ballot. The attackers installed a backdoor that let them view any ballots that voters cast after the attack. This modification recorded the votes, in unencrypted form, together with the names of the voters who cast them, violating ballot secrecy.

[60]See the allegation that Russia tampered in 2016 United States Presidential election has been confirmed by US intelligence officers. The then President Obama expelled Russian diplomats for American soil to register his displeasure.

[61] LexisNexis. "True Cost of Fraud Study", August 2014. Available at http://www.lexisnexis.com/risk/downloads/assets/ true-cost-fraud-2014.pdf.accessed 13th March 2023.

[62] DCBOEE press release. "Board announces public test of Digital Vote by Mail service" September 2010. Available at, http://www.dcboee.org/popup. asp?url=/pdf_files/nr_588.pdf. Accessed 13th April 2023.

[63] S Wolchok, E Wustrow, D Isabel, J A Halderman. "Attacking the Washington, DC Internet Voting System." In *Financial Cryptography and Data Security*, Pages 114–128.

The final problem discovered by the Michigan team—and perhaps the most devastating, from an operational perspective - was that one of the election administrators had uploaded a file to the mock election server that contained the login credentials for all of the real voters who were eligible to vote online. An attacker who stole these credentials from the known-insecure test server could have used them to cast votes in the real D.C. election, which was set to begin only days later. Since these credentials had to be delivered by postal mail, there was no time to send replacements. Based on these results, the D.C. Board of Elections and Ethics decided not to allow online ballot during the real election. Voters were still able to download, print ballots and post their votes by postal mail. The D.C. trial equally illustrated that, due to the brittleness of the web platform, small mistakes - like using double quotes in place of single quotes in one line of a complex program - can be enough to compromise all the votes in an online election.

(ii) The Estonian Experience

Several countries have experimented with casting votes over the Internet, but none uses Internet voting for binding political elections to a larger extent than Estonia.[64] When Estonia introduced its online voting system in 2005, it became the first country to offer Internet voting nationally and, in recent national elections, more than 30% of ballots were cast online.[65] Many Estonians view Internet voting as a source of national pride, but one major political party has repeatedly called for it to be abandoned.[66] Although Estonia's Internet voting committee maintains that the system is as reliable and secure as voting the traditional way. Its security has been questioned by critics from Estonia and abroad.[67] Rather than proving integrity through technical means, Estonia relies on a complicated set of procedural controls. Security researchers have questioned whether these controls are adequate to secure modern elections, pointing out that the threats facing national elections have shifted significantly since the Estonian system was designed.

Cyberwarfare, once a largely hypothetical threat, has become a well documented reality, and attacks by foreign states are now a credible threat to a national online voting system. As recently as May 2014, attackers linked to Russia targeted election infrastructure in Ukraine and briefly delayed vote counting. Given that Estonia is an EU and NATO member that has borders with Russia, multiple states with significant offensive cyber capabilities might be motivated to interfere in its elections. Despite these concerns, the system was not subjected to a detailed independent security analysis until 2014, when a team of international researchers published a paper pointing out a variety of weaknesses.[68] The team observed operations during the October 2013 local elections, conducted interviews with the system developers and election officials, assessed the software through source code inspection and reverse engineering, and performed tests on a laboratory reproduction of the system. Although Estonia uses a number of safeguards - including encrypted web sites, security chips in national ID cards, and a smartphone-based vote confirmation system, the researchers showed that they all can be bypassed by a realistic state-level attacker. [69] They demonstrated client-side malware that steals the voter's credentials and then silently replaces the cast vote. Such malware could be delivered by pre-existing botnet infestations or by infecting the voting machine before it is delivered

[64] D Jones, B Simons. "Broken Ballots, Will Your Vote Count?" (Chicago: The University of Chicago Press, 2012) 9.
[65] Estonian Internet Voting Committee. Statistics about Internet voting in Estonia, May 2014. Available at http//www.vvk.ee/voting-methods-in-estonia/ engindex/statistics. Accessed 8th May 2018.
[66] Estonian Public Broadcasting. Center Party Petitions European Human Rights Court Over E-Voting, 2013. http://news.err.ee/v/politics/ 4ee0c8a2-b9c2-4d28-8ae4-061e7d9386a4. Accessed 8th May 2018.
[67] H Lipmaa, I Paper-voted (and why I did so), 2011. http: //helger.wordpress.com/2011/03/05/paper-voted-andwhy-i-did-so/. Accessed 8th April 2023.
[68] D Springall, T Finkenauer, Z Durumeric, J Kitcat, H Hursti, M MacAlpine, and J A Halderman. Security Analysis of The Estonian Internet Voting System. In ACM Conference on Computer and Communications Security, CCS'14, pages 703–715. ACM, 2014.
[69] Ibid.

to voters. They also demonstrated server attacks that target the centralized vote counting server. By introducing malware into the server, a foreign power or dishonest insider could arbitrarily change the reported results. The researchers also observed serious lapses in the operational security practices of Estonian election officials. These include administrators downloading security-critical software over unsecured Internet connections, typing secret passwords and PINs on camera in videos published to YouTube during the election, and preparing the voting software for public distribution on insecure personal laptops among other examples. While practices like these might be considered acceptable risks or understandable accidents in a low-security system, a critical system such as a national election platform calls for much stricter procedural controls.

The 2014 study concluded that there are multiple ways that state-level attackers, sophisticated online criminals, or dishonest insiders could successfully attack the Estonian Internet voting system, and that such an attacker could plausibly change votes, compromise the secret ballot, disrupt elections, or cast doubt on the integrity of results. Since these problem stem from basic architectural choices and fundamental limitations on the security and transparency that can be provided by procedural controls, the researchers recommended that Estonia suspend the use of the system.[70]

(iii) The Australian Experience

The world's largest deployment of online voting to-date was during the March 2015 state election in New South Wales, Australia. In this election, absentee voters had the option to use a web-based online voting system called iVote. Voters registered and cast their votes using websites managed by the electoral commission. Upon online registration, they were given an iVote ID number and asked to choose a six-digit PIN. These allowed them to log in to an online voting application written in JavaScript and HTML. After casting their votes, they received twelve-digit receipt numbers. Optionally, voters could call a telephone verification service and enter their receipt numbers to hear an automated system read back their votes. Prior to the election, the commission performed its own security studies and officials declared that the vote was completely secret. It's fully encrypted and safeguarded; it can't be tampered with. [71] While online voting in the March 2015 election was underway, two researchers performed an independent, uninvited security analysis of public portions of the iVote system.[72] They discovered critical security flaws that had been overlooked by the commission's analyses and testing. The researchers tested the main iVote server, cvs.ivote.nsw.gov.au, and showed the system could be exploited and malicious JavaScript maybe injected into the iVote web application. They demonstrated that malware could steal the voter's PIN and the content of their secret ballot then substitute a different vote of the hacker's choosing.

The researchers revealed many ways of committing electoral fraud including compromising insecure WiFi access points, poisoning ISP DNS caches, attacking vulnerable routers, and hijacking prefixes. These attacks are especially practical in the context of a large election, since the attacker can opportunistically target any insecure hosts or infrastructure in the region where voting is taking place. The researchers equally showed that hackers could circumvent detection by performing a variety of tricks to reduce the probability that a given voter would notice a problem. For instance, they could misdirect the voter to a fake verification phone number that reads back the voter's intended choices. Even more simply, the attacker could delay submitting the real vote and displaying a receipt number for a few seconds, in hopes that the voter does not intend to verify and leaves the

[70]Ibid. This call was not heeded as Estonia continues to practice Internet voting.

[71] ABC News. "Computer Voting May Feature in March NSW Election," February 4, 2015. Available at http://www.abc.net.au/news/2015-02-04/computervoting-may-feature-in-march-nsw-election/6068290. accessed 13th January 2023

[72]J A Halderman, V Teague, "The New South Wales Ivote System: Security Failures and Verification Flaws in A Live Online Election". In International Conference on E-Voting and Identity, August 2015.

website. The attacker would intercept a voter's online registration session and assign him or her the iVote ID and PIN of a like-minded person who had already voted, preferably one who cast a simple vote likely to be repeated. Later, if the victim's choices match those of the first voter, all of the verification will look right to both voters. The attacker can safely reuse the target voter's registration credentials to get a new iVote ID and PIN and cast an arbitrary vote.

The electoral commission responded the report by modifying the iVote server configuration to disable Piwik[73]. They equally recognised that there is not yet a "secure and reliable electronic voting system which removes all the known risks"[74]

6. Recommendations

To safeguard against these, there should be a comprehensive electoral modernisation framework with a clear vision, strategy and effective planning on how e- elections should be run in Nigeria. Furthermore e-voting systems need to be engineered to a level of security quality far greater than that of typically information technology systems. INEC should provide convincing evidence that this level of quality has been achieved, by being transparent about their security measures and engineering processes. They should invite ethical hackers to highlight the vulnerabilities of BVAS if any.

Furthermore, full training for staff involved in election and certification of the equipment by manufacturers should be paramount to avoid a repeat of the embarrassment of switched off BVAS and IREV that failed to translate results in real time. These measures will serve as a check to ensure that e-voting system is not deemed a failure when it is fully rolled out.

7. Conclusion

Democracy relies on voters having well-founded trust in the processes used to collect and count their votes. Unfortunately, when it comes to real-world e-voting systems, it has been shown that vote rigging, electoral fraud is capable of transpiring online. From our case studies, majority of the countries who initially embraced e-voting have reverted to manual elections as the massive vulnerabilities were highlighted. Others preserved paper trial as a measure against e-rigging. Hackers will always attempt to hijack electoral results either to favour a candidate for financial gain or for fun. Judging by the mood of the country and our antecedents to favour foreign ideas, it is easy to predict that Nigeria would embrace full scale electronic voting in no distant time. Given Nigeria's reputation with cybercrime, her peculiar problem with idle youth. It is predictable that when Nigeria transforms her manner of voting to full e-voting in all ramification, unscrupulous people may hijack the e-voting process.

[73] By the time the vulnerability was fixed, online voting had been taking place for five days, and 66,000 votes had already been cast. The closest seat in the parliamentary results was eventually decided by a margin of 3,177 votes, less than 5% of this number. Ibid

[74] Digital Democracy Commission publication 26th January 2015 available at http://www.digitaldemocracy.parliament.uk/documents/Open-Up-Digital-Democracy-Report.pdf accessed 3rd February 2023