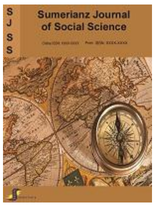
Sumerianz Journal of Social Science, 2019, Vol. 2, No. 2, pp. 20-26
ISSN(e): 2616-8693, ISSN(p): 2617-1716
Website: https://www.sumerianz.com



Original Article Open Access

Menace of Cyber Interference and Paradigm Shift in Election Security: Assessing the Fate of Democratic Election in Nigeria

Badmus Bidemi G.
Research Fellow and Academic Advisor, Political Science Department, Distance Learning Centre, University of Ibadan, Ibadan, Nigeria
Principal Administrative Officer and Assistant Electoral Officer, Independent National Electoral Commission, Oyo State Headquarters, Nigeria

Abstract

The contemporary election has witnessed tremendous changes in its security context, administration, delivery and management as a result of cyberspace and technology interference in democratic process. The noticeable trends in election security has remained the rapid movement more and more away from the regimented physical policing system which is characterised by technological ineptitude and corruption in Nigeria toward cyber security which is more efficient and effective. This study argues that cyber interference in election is imminent as more election management bodies (EMBs) continue to deploy the use of ICT and other cyber technologies for data/election material safety, efficient and cost effectiveness in management of democratic elections. However, the critical challenges remain how to curtail threats to election security created by deployment of new technologies to conduct and manage election. Given the incessant and looming danger of cyber-attack in terms of ransomeware, phishing and hacking that is gradually crippling the ability of modern states to conduct credible election. Nigerian government must create discerning approach to control excessiveness of cyber interference in its election while annexing its benefits to the fullest.

Keywords: Election; Election security; Cyber-attack; Ransomware; Phishing; Hacking.

1. Introduction

The overbearing influence of technologies on social, political and economic activities in modern societies particularly in the 21st century cannot be overemphasized. Thus, modern democracy has witnessed inextricable interference of technologies in its process, management and delivery. Importantly, the deployment of cyber technology in the administration and conduct of election has given more credence and reinforced the undisputed role of election as driving force behind the notion of democracy. By and large, the new technologies such as Electronic Voting Machine (EVM), Smart Card Reader (SCR), Electronic Ballot Printers (EBPs), E-Collation, Optical Mark Recognition (OMR), Designated Election Software and Applications, Internet Voting System (IVS) among others that are becoming widely adopted by many election management bodies (EMBs) to promote free, fair and credible election have also come with some negative consequences for election security and democracy at large.

Unfortunately, election security has been further compromised in many African countries due to undemocratic nature of power struggle and transition within their political system. For instance in Nigeria, political power remains highly prized and by implication, acquisition and wielding of such power is synonymous with unlimited opportunities in terms of access to economic, natural resources, political positions and everything humanly beneficial. Thus, losing out of political power or being out of government invariably implies little or no access to socio-economic and political benefits. As Lai Olurode (2013) succinctly argued, in a country where oil rents are highly centralized, being out of government and its related institutions might be akin to being condemned to a life of penury and despondency. Given the situation above, there are high tendencies that election security and democratic process could be highly compromised and made worse through manipulation of new technologies.

Interestingly, as democracy is becoming more and more digitalised there are numerous technological challenges confronting the contemporary democratic election worldwide and no country is totally immune from cyber-attacks or cyber interference. Put differently, the negative consequences of cyber technology in the conduct of democratic election has become imminent worldwide. However, the root causes, profiles, intensities and counter measure approach to cyber-attack varies from one country to another. Notably, many developing countries, particularly Nigeria are more vulnerable to the menace of ransomeware, phishing, doxing and hacking among others menace of new technologies against their electoral processes due to inadequate capacity to tackle some of these evolving technological challenges.

The foregoing situation has provoked debates and generates serious concerns among stakeholders about the future and security of election in Nigeria given the prevalent and indispensable role of technologies in election administration and democratic governance. More focus have been particularly placed on the best way to secure election and electioneering process against the possibilities of cyber attacks and undue technology interference.

Succinctly, the paper is divided into six sections for purposeful explication of the subject matter; introduction, conceptual clarification, technology interference in democratic election, paradigm shift in election security, cyber-attack and the safety of democratic election in Nigeria, conclusion and recommendations.

2. Conceptual Clarification

2.1. Election

According to Badmus Bidemi (2017), the essential role of election in a democratic system cannot be overemphasized, because it influence the manner of political competition and function as a major determinant of who get what, when and how. In the same vein (Rokkan, 1970), describe election as the institutionalized procedure for the choosing of office holders (representatives) by some or all of the recognized members of a society. In the same vein Joseph (1987), election is describe as important starting point for the existence of democracy, making it possible for democratic government to be ‘by person freely chosen by and responsible to the governed. To Wanyande (1987), elections represent a way of making a choice that is fair to all - one that leaves each member of the electorate reasonable hope of having his alternative elected. An election is therefore an empirical demonstration of a citizen’s liberty and political choice.

As Villalon (1998) rightly argue, elections themselves may be a strategy for maintaining power and many African elections- have been clearly intended to forestall change, or even strengthen the status quo. Properly conducted election can promote peace, boost the confidence of electorates and lead to development. Similarly, election is a huge investment by society to address critical societal questions and to choose a path forward in peace. Thus, the tangible/intangible of the election is always “trust”–in the process, outcomes, and results (Bill Sweeney, President, IFES cited in Conny and McCormack (2016). Unfortunately, the evidence suggests that elections in Nigeria are the opposite of what election should represent in the democratic system.

Interestingly, Klemens (2013) described elections as the core of the democratic process; and to cast their vote is the supreme sovereign right of every citizen. They must be able to do this free from pressure, free from inappropriate influence and free from fear. According to Dickerson *et al.* (1990) election is defined as a post mortem that investigate the record of office holders whose actual performance may have little to do with promises made when they were previously elected.

Globally, election is conceived as the heart of representative democracy. In this regard, a credible election did not only confer legitimacy on political leadership, it is also crucial to the sustenance of democratic order. Thus election offers citizens the freedom to choose their rulers and to decide on public policies (Animasahun, 2010). Generally, elections are at the core of the democratic process; and to cast their vote is the supreme sovereign right of every citizen. They must be able to do this free from pressure, free from inappropriate influence and free from fear (Klemens Mömkes, op ct).

Arguably, the significance values of election in a democratic system cannot be overemphasized, because it shapes the mode of political competition and serve as a major determinant of who get what, when and how. According to Joseph (1987) election is describe as important starting point for the existence of democracy, making it possible for democratic government to be ‘by person freely chosen by and responsible to the governed. Similarly, Wanyande (1987) stressed that elections represent a way of making a choice that is fair to all - one that leaves each member of the electorate reasonable hope of having his alternative elected. An election is therefore an empirical demonstration of a citizen’s liberty and political choice. On the other hand, Nzongolo (1997) argued that the essence of liberal democracy has been increasingly reduced particularly, in Africa to the conduct of election and introduction of multipartyism”. To International Encyclopedia of Social Science election is defined as one procedure of aggregating preferences of a particular kind.

As posited by Ayoade (1999), election is the process of actualizing representative democracy. It is a method of selecting a few people from large group such that the few people are a representative sample of the large group. To him, the few elected are supposed to be the mirror image of their electors in term of political programmes and beliefs. To Graft (1979) elections are expected to promote majority rule through the establishment of legitimate government and the exercise of popular control over the leaders of a nation. Importantly, the point of convergence in the above definitions rest on the value placed on election as a major way of actualizing democracy.

2.2. Election Security

Undoubtedly, election security is one aspect of overall security system within the state structure. Thus, it is pertinent to start the discussion on election security with the clarification of the context of security and insecurity to human and societal existence. However, the subjective nature of both content and context of security and insecurity have generated debates among scholars and security experts particularly on some of the factors that constitutes threat or pose danger to the overall well being of both human and societal values. Put differently, the condition of socio-political, economic and other environmental factors surrounding individual and society at large can serve as predetermining factors to both security and insecurity.

According to Ugwuoke and Ajodo-Adebanjoko and Nkemakolam (2014) insecurity is described as any act that poses threat to state interests in the international politics which explain part of the reasons for arms-race and proliferation of nuclear weapons for the purpose of self defence by the state. Unfortunately, foregone definition did not aptly capture the insecurity within non state actors’ interactions. To Beland (2005), insecurity is defined as a state of fear or despair due to lack of access to the means of protection.

Paradoxically, security is the direct opposite of insecurity, therefore, to be secured, in the opinion of Ani (2009), simply implies the condition of being protected physically, emotionally, psychologically as well as from other harm, attack, terror which could be considered as non-desirable. By implication and considering the definitions of insecurity provided above. In concrete terms, security implies the state of being free from danger or injury or considerable freedom from anxiety or fear which is applicable to both individual and state actors. Broadly speaking, electoral security involves ensuring the safety of the electoral process and to create a quiet and safe environment to enable citizens to take part in the electoral process without fear, 1intimidation, before, during and after voting (UNOWA, 2009).

Generally, electoral security involves ensuring the safety of the electoral process and to create a quiet and safe environment to enable citizens to take part in the electoral process without fear, 1intimidation, before, during and after voting.

More importantly, election security is critical to the organisation, planning and process of democratic election, particularly if the motive is to achieve free, fair and credible elections. Thus, election security starting from the provision of basic protection of voters to observe political party rallies and campaigns; to ensure voters are able to cast their votes without fear or intimidation; ensuring that result forms and other election materials are protected; ensure the whole electoral process is circumscribed by security considerations; to guarantee the safety of electoral personnel, polling centres and observers/media; to create a level playing field for all political parties and candidates to canvass for support; and to maintain the overall integrity of the democratic and electoral processes. As argued by (Ani, 2009), election security in this regard, connotes the absence of physical, technological, psychological, cyber threat or software attack, terror and other unconventional manipulative methods that constitutes the state of insecurity to election and electioneering process.

As specified in the Electoral Security Framework (2010), there are four broad perspectives to electoral security which involves; physical security, personal security, information security and electoral events security. **Physical security** involve the protection of facilities and materials, including the electoral commission headquarters and its district offices; registration and polling stations; political party offices; election observer offices; and media organizations. **Personal security** as observed by Fischer (2008), focuses on the protection of electoral stakeholders, including voters, public officials, election workers, security forces, candidates, party agents, election observers and media representatives. **Information security** concerns protection of computers and communication systems employed in voter registration and vote tabulation, as well as associated sensitive election materials such as voted and un-voted ballots and voter registration lists (www.aceproject.org). Fischer further posited that **Electoral events** can be exploited by conflict. In many occasions, such events can be official, such as voter registration programs or Election Day activities, which could also involved events such as campaign rallies, political debates, and political party and coalition meetings.

2.3. Cyber-Attack

Digital meddling has remains the worst-case of cyber-attack, For instance, more often than not cyber-attack in relation to election, involves the act of hacking voting machines, sabotage the power grid that supply electricity to major equipments, or using the process of two-pronged attack: first, to black out sources of real information and second, to spread disinformation. According to Adam Meyers, the vice president of intelligence at the security firm CrowdStrike, he described the cyber-attack as a "subtle and better way to destabilize a country without a shot being fired", cyber-attack can also occur on the internet infrastructure company. A typical example was an attack on Dyn web: Dyn was hit with a so-called distributed denial of service attack that flooded some of its servers with malicious traffic until they buckled under the load. The attack specifically targeted Dyn's Domain Name System service, which acts as a directory of which web addresses correspond to which numeric IP addresses. As a result, the attack on Dyn affected people's ability to load web services l

More significantly, there are different types of cyber-attack which includes the following; (a) **service denial**: this involves disruption attack that includes the infiltration into organisation website either to slow down the website or to shut it down completely; **Porosity of vendors and contractors'** to use secure system; **Leakage in the handling of sensitive information and passwords** by **b**oth permanent and temporary election workers who might have access to sensitive information and passwords; **prevalence of Ransomware,** and **Phishing Attack**.

Ransomware: ransomware involve a situation where critical data, reporting data and other sensitive organisation software were holds into ransom on a night before the event. **Phishing** attacks: focus on instances where hackers are posing as organisation's vendors try to deceive the local or regional workers to open e-mail attachments containing malicious software and viruses purportedly sent by their headquarters office to disrupt organisation's activities, promote misinformation campaigns or to steal vital information.

Hacking as related to electoral process, most hackers will try to probed and often times breached voter registration systems, either to spread apprehension, find system weaknesses and carry out other malicious acts. In the same vein, Hackers also employ other tactics to disrupt voting process, polling units report and tallies digitally to vote collection centres. More often than not, hackers attack the election information websites which could hinder voters' abilities to learn basic details like the status and location of their polling unit. As observed by Kevin Du, a network security researcher at Syracuse University cyber attacks may not have direct impact on voting machines, but cyberattack can indirectly affect voting patterns in many ways, particularly by slowing down or outright shutting down of online services (https://www.wired.com/2016/11/real-hacker-threat-election-day-data-deception-denial)

3. Technology Interference in Democratic Election

Over the past few decades, technology interference in democratic election has become pervasive and it has continued to playing crucial role in every stages of electoral cycle across the world. This assertion was further buttressed by Yves Leterme, Secretary-General, International IDEA cited in Conny and McCormack (2016), that to cater for the demands of an ever-dynamic global system, democracies must be evolving and changeable. Thus, technology represents one of the powerful tool which, when implemented properly, can modernize elections and democracy.

It is important to note that, technologies interference is not a new phenomenon in election conduct. The mid- to late 1800s marked the beginning of a technological revolution in democratic process. As technology continue to improved, electoral management bodies (EMBs) applied the various innovations to enhance the electoral management system (http://aceproject.org/ace-en/topics/et/onePage).

For instance, the creation of electricity and the invention of power stations have resulted into availability of electric typewriters, printing machine for ballot papers, and electronic voting devices and the subsequent emergence of computers which has led to e-voting and digitalised democracy. Similarly, the evolution of mass communication methods that took place in the 1900s also had electoral implications. Hence, sound, vision recording and transmission which have leading to widespread of radio, television, telephones, facsimiles, audio tapes, video tapes, compact discs and the Internet, have all been used for electoral purposes in the 21st century.

It is instructive to note that, modern technological innovations have gradually improved the management of the electoral process from the 1800s to the mid-1900s; it took the development of the computer to revolutionize democracy as a system of government. Today's computers were inspired by punch-card tabulating machines invented in the late 1800s. These in turn were inspired by punch-card weaving systems, first invented in 1801 by Joseph Marie Jacquard, a French weaver. The first modern electronic computers were developed in the 1940s and 1950s, to the point where they became commercially viable. One of the earliest electoral uses of a computer was the tabulation of the election results for the 1952 United States presidential election.

The beginning of this millennium has witnessed a number of countries turning to a variety of technological solutions in a bid to make elections more efficient, cost effective, and to strengthen stakeholder trust in each stage of the electoral cycle. Thus, various solutions adopted range from the use of geographic information systems to conduct delimitation of constituencies/boundaries and to establish the location of polling stations; the use of sophisticated databases to maintain the voter registers; mobile technology for the transmission of election results and electronic voting machines to enable citizens to cast their ballots without the need for physical presence at a designated location.

In particular, biometric technology now plays a significant role in a number of electoral processes around the world, such as voter registration and the identification of prospective voters at the polling station on election-day. The introduction of information and communications technologies (ICTs) into the electoral process is widely arousing both interest and concern among voters, election stakeholders and practitioners across the globe. Undoubtedly, technology has helped electoral management bodies (EMBs) to make their processes more transparent, effective and efficient. Given the increased of Internet penetration particularly in developing countries with poor history of communications infrastructure and media technologies, most of the developing countries have recorded tremendous improvement and the situation is further encouraging their Election Management Bodies (EMBs) to be more effective at communicating both internally with its personnel and eternally with all the stakeholders involved in the election process.

Consequently, what makes cyber election interference different from general cyber attacks are as follows; (1) nature of the target, (2) the nature of the attack, (3) the nature of the damage, and (4) the lack of an appropriate remedy, either in international law or in domestic law. In retrospect, according to Piccolino (2015) there is an increasing utilization of ICT in the electoral process, especially in Africa. Piccolino further stressed that no fewer than 25 sub-Saharan African countries including Kenya, Zambia , Sierra Leone, Democratic Republic of Congo, Malawi, Rwanda, Mali, Togo, Ghana, Senegal, among others) at one point in time have deployed ICT for elections.

In the opinion of Odeyemi and Mosunmola (2015) several countries around the world especially, in the advanced democratic nations like the United States of America, Britain, Germany, France among others have since deployed ICT tools to manage their electoral process. In recent time, there is widespread use of social media platforms in 2008 by Barack Obama in the build up to the 2008 United States of America presidential election. In Africa, particularly in Nigeria the history of ICT deployment dates back to the 1960s, whereas, a comprehensive and policy based effort in terms of ICT deployment began with the introduction of the National Policy on information technology. The Federal Executive Council in Nigeria promulgates a National Information Technology policy in March 2001 and its enforcement commenced in April of the same year with the establishment (through the Ministry of Science and Technology) of the National Information Technology Development Agency (NITDA), charged with the regulation and implementation.

Contrarily, cyber election interference has widely become a global threat and it has inspired the interests of many democratic leaders across the globe. In recent time many Western countries particularly the US, Italy, Germany, France, and Ukraine among others have experienced cyber interference in their democratic process as a result of cyber attacks which posed serious challenges to their ability to conduct free, fair and credible elections. Pathetically, as earlier mentioned what make the cyber attacks on election process and conduct more severe includes but not exhaustively limited to the following; the nature of cyber-attack target, the extent of damage, the style of the attack, and the absence of an appropriate measure, either in international law or in domestic law to apportion punishment.

4. Paradigm Shift in Election Security, Cyber-Attack and the Safety of Democratic Election in Nigeria

According to Lai Olurode (2013), theorizing about election security remains daunting and hazardous for several different but related factors. The first factor is the ever changing security architecture within and beyond national boundaries as well as their intersections. Second factor, is the diverse variables and the complex nature of the relationship that exist among those factors. Third, there are numerous national and international stakeholders in security architecture which may be guided by different interests rather than security concerns and motivated by non security parameters.

In planning, coordination and deployment strategies and logistics pertaining to electoral processes, a well-coordinated security is a fundamental requirement for successful election administration and management. Thus, there is need for adequate security to ensures the free movement of electoral staff, voters, candidates, observers and other stakeholders on Election Day, which, in turn adds to the credibility of the electoral process. Similarly, adequate security is an important pre-condition for the deployment of valuable electoral assets and sensitive materials to registration and polling sites. Adequate security increases the level of participation of political parties, candidates and voters in an election. It also enables a more objective coverage of events by the media and easier circulation of voters' education, message and materials

Ironically, the credibility and acceptability of elections in Nigeria have been very contentious and often litigious because of the inability the stakeholders to secure such elections either in the period leading to pre-election, Election Day and post-election processes. Such failures to secure elections often led to political crises and governance failures with subsequent interruptions of the democratic governance through military interventions (Mike, 2013).

More often than not, as Igimi further posited, the failed elections with consequent democratic regime failures have often been preceded by one or more of the aforementioned breaches of the electoral process due to challenges of security, often posed by the activities of hoodlums called party thugs and compromised officials at different stages of the election process. Therefore, any election management body truly concerned about securing elections, must focus on software issues like trust building of stakeholders, ensuring the fidelity of technology used in election processes, education of voters and other role players in security issues and their role in assuring security and the institutionalization of a credible electoral process through a reliable legislative electoral framework, managed professionally, with impartiality and integrity.

It is instructive to note that election play very important role in the process through which power is formally allocated, in a process where power relations are defined, redefined or reassured (Ayoade, 1999). Unequivocally, election has been widely regarded as internal affairs of the country holding such election, thus any attempt to intervene direct or indirectly by external actors is consider as breach of territorial sovereignty of an independent state. However, the revolutionalised of information and communication technology and the globalisation pressure have change the security perspective on election and encourage the use of cyber-attack in terms of ransomeware, phishing and hacking among others by both individuals and states actors to indirect or cynically intervene in election of either home or foreign country.

Succinctly put, the invention of new technologies and globalisation reality, particularly the emergence Internet and other ICT devices have created a paradigm shift in election security and encouraged both external actors and states to indirectly or cynically intervene in the process and actual conduct of election in other countries. Shockingly, the predicted impact of such external intervention through cyber-attacks methods such as ransomeware, phishing and hacking techniques in the conduct of election in other clime is horrific and subterfuge of election outcome. To scholar like Barya (1993), such intervention in democratic affairs of foreign states particularly by the Western nations is regarded as attempt to promote the ideology of free enterprise worldwide, to create a new credible source of legitimacy for hegemonic and thereby ensure leverage over specific countries which are considered economically and politically useful to specific western countries. Whereas, from individuals' perspective such intervention could be motivated by various reasons such as personal economic benefits, to predetermine the outcome of election, for vengeance intention and terrorism mission among others.

The damaging impacts of cyber-war on electoral process, economic and the overall democratic values is more lethal than what the police and other security apparatus can avert and it has provoke debates from scholars and other stakeholders on the imperative for states to take collective actions against either individual or state actors for engaging in cyber-war or internet-war to disrupt or discredit election and democracy in other countries. This is important because, the attack and the identity of the hacker raise particular concerns in the election context. First, because elections are usually held at a periodical interval, discovering security breaches and unlawful influences as close to the period of lection is crucial in guaranteeing the integrity of the election.

As Lily (2016) observed, a later identification of either the identity of hacker(s), security breaches or unlawful interference in election process has a great potential to provoke a crisis of constitutional proportions. For instance, a belated announcement that votes were improperly tabulated, and the victory should have been given to another candidate would raise questions even larger than those of *Bush v. Gore*. Such an attempt is described by many security experts in response to Russian interference in the U.S. elections as "better way to destabilize a country without a shot being fired.

According to Van and Jacqueline (2017), cyber attack on the activities of organisations and states is not a new phenomenon. However, what distinguished cyber meddling in election process from general cyber attacks are as follows; (1) choice of the target, (2) the nature of the attack, (iii) the gravity of the damage, and (iv) the absence of both domestic and international law for curative measure. The choice of the target as Jacqueline stressed is unique in two major ways. First, the targets are publically owned infrastructures or institutions. Thus, any attack on state's institutions or infrastructures will automatically provoke questions and agitations about violations of territorial sovereignty of an independent state both in the abstract and in concrete sense. Importantly, some of the targets are not computers but citizens. For instance, the available information, whether true of false, could be disseminated to manipulate the behavioural patterns of a sovereign's citizens and thus damage the state through citizens' action(s). Notably, the intimate target of cyber interference in elections is to touch the state's apparatus and its citizens that make it distinct from other forms of cyber attacks.

Unfortunately, the damages from technology interference in election have the potential to be multitude in terms of its far reaching impacts. The scope of cyber election interference, however, has the potential to be far broader. By implication, the hacking of state voting systems might be limited to the physical computer systems, which could encourage the dissemination of fake news in order to influence citizen votes or use to manipulate the voter's choice of candidate during election. Therefore, cyber interference in election also has the tendency to weaken citizen confidence in the democratic process and in the integrity of their government.

Generally, the experience from the past few decades have shown that no country is totally immune against cyber-attack either against election, government institutions or government infrastructures. Hence, states have been affected by a variety of cyber interference in their elections, ranging from misinformation campaigns, to theft of information, to damage to voting machines. As Adam (2013) pointed out, the first sign of this new era of hybrid war came in a five-year string of hacking attacks against the United States from 1998 to 2003 known as "Moonlight Maze." While many details remain undiscovered, hackers traced to Russia stole thousands of U.S. military documents containing sensitive information, including encryption technologies.

In the same vein, subsequent cyber-attacks in Estonia in 2007, Georgia in 2008, and in Ukraine suggest that no country is actually safe from cyber-attack as some country fully determined to sharpen their cyber capabilities either to attack an independent state or as a source of defence against external cyber aggressors. For instance, hackers in some cases are using Kremlin IP addresses, launched crippling distributed denial of service attacks, taking down local government websites, the country's Internet infrastructure, and paralyzing its financial industry (Andreas, 2013).

There is no doubt that cyber-attacks are increasingly growing in publicity, occurrences and consequences, thus, turning the modern foreign policy into a hallmark of cyber episodes. The critical aspect of cyber-attacks remain the state-supported interference in elections which includes a number of events: such as; hacking of email and doxing that happened in the 2016 U.S. presidential election, the cyber-attacks on the Bundestag surrounding the 2015 German Parliamentary elections, the dissemination of "fake news" circumferential of 2016 Italian referendum votes. According to Hillary (2015), in the US specifically, the touchstone of the cyber episode campaign begins with Clinton's email saga while she was serving as U.S. Secretary of State and she was using a private email server.

In Germany, there was reported case of cyber attacks to indirectly influence German public opinion in her September 2017 election by Russia. According to Janosch Delcker (2016), cyber meddling by Russia in German was an attempt to remove German Chancellor Angela Merkel, who has visibly critiqued of Russian policies in both Ukraine and Syria. More so, it was widely acknowledged that Russian interfered in two major ways. First was the information warfare, and second were cyber-attacks. For instance, there was a fake story that deeply captured public consciousness: fake news about refugees from the Middle East gang-raping a 13 year-Old Russian girl in Berlin which went viral. The consequence of the fake news was an uncontrollable protest which grew into violent that forced German's foreign minister to make a public statement debunking the propaganda (Damien, 2016).

Similarly, Italy was not spare of cyber interference in her electioneering process. In the build up toward the 2016 election in Italy, there is lots of dissemination of false information and news through different social media platforms. As argued by Alberto and Craig (2016), the fake news was targeted against Prime Minister Renzi through blogs, social media accounts and websites from Russia to spread fake news across their virtual networks. In the aftermath, Prime Minister Renzi lose the election and the situation provoked concerns that such instability might trigger a deeper crisis in the vulnerable Italian banking sector (Damien, 2016). In the same manner, in France, hackers stole and published gigabytes of leaks from center-left French candidate Emmanuel Macron on the eve of the French election. Pathetically, Ukarine's election was also hit by cyber interference, when Russian hacker group called CyberBerkut attempted to publish false election results in 2014 by compromised the website of the Ukrainian Central Election Commission and modified the website to declare Dmytro Yarosh as the winner.

5. Conclusion

Thus, for many African nations and Nigeria in particular, the danger and threats of cyber-attack or cyber interference in election are imminent as more and more election management bodies (EMBs) continue to deploy the use of ICT and other cyber technologies for efficient and cost effective management of democratic elections. Therefore, EMB and Nigerian government must be conscious of the current trends in election security which is shifting rapidly more and more toward cyber security than the regimented physical policing system. For instance, the former vice president and the presidential candidate of the Peoples Democratic Party (PDP) Atiku Abubakar that petitioned the Presidential Election Tribunal challenging President Muhammadu Buhari re-election and alleging Independent National Electoral Commission (INEC) of conniving with the ruling party All Progressive Congress (APC) for infiltrating into INEC server to manipulate election result figures in favour of the APC's candidate. However, the allegation is yet to be confirmed or proved but this suggest the possibility of the imminent cyber interference in Nigerian elections which demand more serious scientific and technological approach first, to ensure the integrity of election is protected, second, to further boost peoples' confidence in democratic process and third, to checkmate the future possibility of undue cyber-attack or cyber interference in election and democracy at large.

References

Adam, E. (2013). *Moonlight maze," a fierce domain: Conflict in cyberspace, 1986 to 2012, eds. Jason healey and karl grindal.* Cyber Conflict Studies Association.

Ajodo-Adebanjoko, A. and Nkemakolam, O. (2014). Corruption and the Challenges of Insecurity in Nigeria: Political Economy Implications. *Global Journal of Human-Social Science: F.*, 14(5): 11-16.

Alberto, N. and Craig, S. (2016). Italy's most popular political party is leading europe in fake news and kremlin propaganda, buzzfeed. Available: https://www.buzzfeed.com/albertonardelli/italys-most-popular-political-party-is-leading-europe-in-fak?utm_term=.cnnVK073G#.xeaRkyLGQ.

Andreas, S. (2013). *The estonian cyberattacks," a fierce domain: Conflict in cyberspace, 1986 to 2012, eds. Jason healey and karl grindal.* Cyber Conflict Studies Association. 174-93.

Ani, K. J. (2009). Inter-Religious Socialization as a Peace Education Subject for Conflict Management in Nigeria. *Maiduguri Journal of Peace, Diplomatic and Development Studies,* 2(2): 40-42.

Animasahun, K. (2010). regime character, electoral crisis and prospects of electoral reform in Nigeria. *Journal of Nigeria Studies,* 1(1): 1-33.

Ayoade, J. A. A. (1999). *Aims and objectives of election monitoring', in ayoade. J.A.A. (ed) handbook of election monitoring in nigeria.* Vantage Publishers Ltd: Ibadan. 16.

Badmus Bidemi, G. (2017). leadership questions and the rhetoric of free and fair elections: A prognosis of the 2007 and 2015 elections in nigeria. *International Journal of Political Science,* 3(2): 33-46.

Barya (1993). Lily hay newman, the real hacker threat to election day? Data deception and denial, wired. Available: https://www.wired.com/2016/11/real-hacker-threat-election-day-data-deception-denial/

Beland, D. (2005). The Political Construction of Collective Insecurity: From Moral Panic to BlameAvoidance and Organized Irresponsibility. Center for European Studies, Working Paper Series 126.

Conny, B. and McCormack (2016). *democracy rebooted: The future of technology in election.* Atlantic Council: Washington, DC: USA.

Damien, M. (2016). russia steps into berlin 'rape" storm claiming german cover-up, bbc news. Available: http://www.bbc.com/news/blogs-eu-35413134

Dickerson, M., Micheal, W. and John, H. (1990). Demographic, personality, cognitive and behavioral correlates of off-course betting involvement. *Journal of Gambling Studies,* 6(2): 165-82.

Electoral Security Framework (2010).

Fischer, J. (2008). *elections in fragile states.* Princeton University.

Graft, D. W. (1979). *1979 election: The Nigeria citizens guide to parties, politics, leaders and issues.* Daily Times: Lagos.

Hillary, C. (2015). Private email set up for 'convenience,' bbc news. Available: http://www.bbc.com/news/world-us-canada-31819843

Janosch Delcker (2016). russian hacking looms over germany's election, politico. Available: http://www.politico.eu/article/russian-influence-german-election-hacking-cyberattack-news-merkel-putin/

Joseph, R. (1987). *Democracy and prebendal politics in Nigeria: The rice and fall of second republic.* Cambridge University Press.

Klemens, M. (2013). *opening remarks of deputy head of mission, embassy of the federal republic of germany to nigeria' in lai olurode (ed) election secuity in nigeria: Matter arising. Friedrich elbert stiftung (ifes).* Abuja: Nigeria.

Lai Olurode (2013). *Election security in Nigeria: Is there silver lining? In lai olurode (ed) election security in Nigeria: Matter arising. Friedrich elbert stiftung (ifes).* Abuja: Nigeria.

Lily, H. N. (2016). the real hacker threat to election day? Data deception and denial, wired. Available: https://www.wired.com/2016/11/real-hacker-threat-election-day-data-deception-denial/

Mike, I. (2013). *Election security in theory and practise: Prospective of a resident electoral commissioner' in lai olurode (ed) election secuity in nigeria: Matter arising. Friedrich elbert stiftung (IFES).* Abuja: Nigeria.

Nzongolo, N. (1997). The State and Democracy in Africa' Cited in the 'State and Democracy in Africa' Ntalaja and Vargaret Lee (eds.) Harare AAPS Books.

Odeyemi, T. and Mosunmola , O. (2015). *Stakeholders, ICT platforms and the 2015 general elections in nigeria. Paper presented at the national conference on the 2015 general elections in nigeria: The real issues, july 27- 28, INEC, .* Abuja.

Piccolino, G. (2015). What other African Elections tell us about Nigeria‟s Bet on Biometrics. Available: www.washingtonpost.com/blogs/monkeycage/wp/2015/03/10/whatother-african-elections-tell-us-about-nigerias-bet-on-biometrics/

Rokkan, S. (1970). *citizens, elections, parties.* Universitetforlaget: Oslo.

UNOWA (2009).

Van, D. V. and Jacqueline (2017). the law of cyber interference in elections. Available: http:ssrn.com/abstract=304328

Villalon, L. (1998). *The african state at the end of the twentieth century: Parameters of critical juncture,' in, villalon, l. & haxtable, p. (eds), the african state at a critical juncture: Between disintegration and re-configuration.* Lynn Rienner: London.

Wanyande, P. (1987). *Democracy and the One-Party State: The African Experience'. In Oyugi, W & Gbonga, A. (Eds). Democracy Theory and Practice in Africa.* Jmes Curry: London.