TOWARDS EFFECTVIE GLOBAL CYBER SECURITY FOR E-ELECTORAL SYSTEMS FOR DEVELOPING COUNTRIES

BY

Zakari Mohammed, Ph.D, fnim, fnla, MNAE

Department of Library and Information Science

Ahmadu Bello University

Zaria, NIGERIA

A paper presented at the e-Nigeria Conference Held at The International Conference Centre, Abuja Between 17th and 18th November, 2015.

Abstract

The paper examined the state of electoral systems, management and process in developing countries. This was followed by the causes and consequences of election malpractices in the body polity of liberal democratic settings. It was revealed that government officials and agencies which, include Election Management Body (EMB), political parties, political gladiators and the traditional, community, religious and cultural leaders were the major role players in abetting and perpetuating election malpractices to deny the emergence of legitimate winners and production of masqueraded election results found to be incredible for acceptance. The place of technologies in election management and processes as well as electoral systems and operations were highlighted. The dimensions of cybercrime, cybersecurity and their impact on electoral systems and management in emerging democracies were x-rayed along with the way forward towards achieving global-electoral systems.

Introduction

Conceived and perceived as a veritable platform where people have the right and opportunity to determine who should be their leader and govern them according to given principles, procedures and policies enshrined in constitution, democratic ideologies and processes are rapidly being imbibed world-wide since the mid-20th century especially in both developed and developing countries of Asia, Europe, Pacific ,Oceanic, and Africa where democracy was hitherto not being accepted as the most appropriate platform to elect political leaders particularly through adult suffrage. Based on democratic principles, policies and ideals, every person who attains voting age has the right to elect at will and without any coercion persons who stand to be elected for elective positions, having met the requirements. For instance, in a democratic dispensation, and depending on the democratic policy and system of a country, persons vying for political offices may have to belong to a political party or/ and can also contest as an independent candidate. In like manner, under normal circumstance, the voters have the right to elect contesting candidates of their choice, regardless of their political party and ideology provided they are found capable, able and willing to promote and defend their rights, and also ensure their access to and utilisation of the dividends of democracy satisfactorily. Thus, consequent upon an elected government's or individual's previous

performances and pedigree in office, under liberal democracy and through voting, elected governments and indeed individuals could be elected only once or more regardless of their political ideology and party patronage.

Though it can be argued that there can be an election of any sort not necessarily under non democratic setting or platform, there can be no democracy without election to usher in an elected government and elected persons without recourse to voting through adult suffrage. It can thus be argued that democracy and democratic systems can and are ably stabilised and sustained through voting of the right candidates based on the adopted electoral system put in place in a country. As a kernel of electoral system, voting remains the ultimate civilised way and manner for people vying to secure political offices in civil societies under democratic dispensations. Krouse, R.W (1982) remarked that voting remains the principal form of political activity in representative democracy. In his own contribution, Diamond, L. (2002) submitted that elections are the litmus test of a democratic political system. It could thus be said that, voting not only provides an avenue for elective officers to come on board political arrangement and positions, it also serves as instrument for checkmating them to account for their performance while in office, as they can equally be ejected out of office through the same process and electoral system. In order to build public trust and confidence in the electoral system and ensure the integrity, validity and acceptability of election results as well as legitimise the position of the winner at a pool, the most fundamental requirements are for the Electoral Management Body (EMB) and the Judiciary to be genuinely independent, nonpartisan and impartial; while the voting exercise should be conducted freely, fairly, transparently, and credibly.

Electoral System

Essentially, whichever type of electoral system a country adopts (be it plurality/majority system, proportional representation system, mixed system, or other system), it must be that that is:

- genuinely independent; and
- promotes and supports:
  - non-partisanship;
  - dynamism;
  - fairness;
  - transparency;
  - impartiality;
  - freeness; and
  - credibility

in the body polity and among the electorates such that the voters have confidence and commitment to be cooperative, ready and willing to fully participate in elections to vote for their preferred candidates who are believed and seen to be accountable to them and will meet up to their expectations.

However, it has been discovered that the developing countries especially in African sub-regions, such as Nigeria, evolving in the emerging liberal democratic dispensation, have embraced a hybrid of proportional representation electoral system where political seats are zoned to accommodate minority groups, geographical locations, and other primordial sentimental considerations to sustain the nascent democracy in the countries. For instance, for a candidate to be declared a winner, he or

she must not only have had the highest total vote cast in the election, but must have had certain minimum percentage score win (e.g.2/3) spread across the delineated political zones. As a matter of principle, an electoral system should impact on the:

- ❒ unity rather than on the disintegration of political party system;
- ❒ help to ease rather than aggravate unnecessary political conflicts;
- ❒ shape public policy outcomes of elections; and
- ❒ the behaviour, motivation and ideological structures and inclinations of political gladiators which may include religious, racial, ethnic, linguistic and other primordial predispositions and considerations.

Ideally, the perspectives of an electoral system should include an electoral formula that effectively accommodates and fits the type of electoral system adopted(be it plurality/majority system, proportional system, mixed system and other systems); ballot system structure delineating whether voters are at liberty to vote for a political party (party- centred election), a candidate(candidate-centred election) or a combination of both to express their choice and preferences; and the electoral constituency and size showing the number of elected representative and seats per electorate.

Internal Democratic Approach to Election and Consequences

In order to effectively implement a semblance of proportional representation electoral system (candidate-centred cum party-centred), especially for general elections in some developing countries, it has been observed that an element of internal democracy is observed. To this end, as a prelude to qualify to contest for a general election, the respective political parties organise internal zonal primary elections to choose a winner from among those contesting under their respective political parties for an elective position in the respective zones. Consequently, the winners are given the political party flag at a public rally usually organised by the political parties to accord them the mandate and support to participate in the up-coming general elections along with the other contestants from other respective political parties. Such method of certifying and legitimising the candidature of a contestant within the frame work of obtaining dual mandate from the political party and the electorate (closed-list approach) tends to bread confidence, support and commitment in them to ensure the candidates' success at the pool. Similarly, it boosts the morale of the candidates; have more confidence and belief in the supremacy of the party; builds confidence and commitment on and in the Electoral College; and also promotes and demands of them for the accountability of their stewardship.

On the other hand, deducting from the recent political see saw antecedents in some African countries such as Nigeria, Egypt, Sierra Leone, Congo, Kenya, Rwanda, Guinea, Burundi, Burkina Faso; etc. where in some cases party and national constitutions were revised to either suit an anointed candidate or elongate his/her tenure, such approach to screening and legitimising the candidature of contestants to contest for elective positions is seen to promote:

- ✖ imposition of especially unpopular candidates on the electorate;
- ✖ election corruptive tendencies;
- ✖ god-fatherism ;
- ✖ money politics;

- insubordination of the party members during voting exercise in the name of anti-party or protest vote to dislodge the imposed or unpopular candidates supported by the party;
- party overzealousness, high-handedness and autocracy;
- intra and Inter-party conflicts;
- liquidation or extinction of minority interests in the scheme of political parties;
- yielding to external and internal pressures of powers-that-be by the Electoral Management Body (EMB);
- the EMB partisanship and non-neutrality;
- manipulation of votes and screening/election results of the electoral college;
- manipulation of screening guidelines; and
- other forms of election/screening malpractices to favour anointed candidates.

Electoral Malpractice Perspectives

It has been observed that election malpractices take place in both developed and developing democratic nations. However, it is most prevalent and sometimes very crude in the developing democracies. Situational analysis of electoral malpractices especially in developing countries revealed that they were usually supported, perpetuated and abetted directly and indirectly by critical role players in the society such as the incumbent government officials and agencies at the centre or at the lower level; the political parties; political gladiators; political god-fathers; traditional and community leaders; religious, ethnic, cultural and tribal leaders; the EMB officials at the centre or at lower level; law enforcement and para-military agencies; the judiciary; the contesting candidates and the electorate. Electoral malpractices are in different dimensions and natures such as:

- political rascality, thugry and banditry resulting into ballot box seizures and illegal stuffing or defacing of ballot papers to demean the prospects of opposition candidates;
- killing and maiming of opposition politicians;
- collusion with unscrupulous law enforcement agents and EMB officials to produce fake ballot papers, manipulate election results, and thumb print and/or stuff fake ballot papers in ballot boxes;
- deliberate ineffective monitoring of election processes to effectively stop election rigging;
- strategic tactics to insecure election materials and results;
- and other forms of electoral irregularities and malpractices that could effectively render election exercise and the results fictitious; embarrassing; unbelievable; unacceptable; unimaginable; outrageous; incredible; and quantitatively and qualitatively fraudulent; scandalous ;and unrealistic for any rational decision making.

ICT Applications in Electoral Management and Processes

There is no doubt in the fact ICTs are rapidly revolutionising the world landscape to sustain the emerging vista of digital society that is continually impacting on all sectors of the economy which include but is not limited to socio-economic, political and cultural growth and advancement of societies and their people, especially through exploitation of smart technologies and provision of cloud technology-oriented services to all and sundry regardless of their locations and times of access. While communication far and wide has been made easy through utilisation of smart phones,

the Internet and other web technologies and tools; the common every day and routine activities have been transformed into online- based activities have been transformed into platforms such as e-government; e-business; e-banking; e-marketing; e- commerce; cyber talks and squatting; e-document; e-library; e-ticket; e- services; e- transaction; e-mail; e-money; e-learning; and e-voting; e-conference and lecture; e-political campaign; e-examination and interview; e-application and registration; and e-payment; etc. which can take place at the convenience of the stakeholders regardless of their locations.

Most fundamentally, the network technologies which include the Internet and other smart communication devices are systematically being employed in all public and private organisations, institutions, and systems to enhance performance, productivity, speed and flexibility of operations. The ICTs, when properly deployed and exploited, save both human and materials costs in managing systems and operations in the production sectors and provision of required services to meet the yearnings of stakeholders. Essentially, the EMBs have to deliberately queue in, as a matter of policy, to deploy and exploit the digital technologies in the management of electoral systems, operations and services in consonant with the dictates of the emerging 21st century digital society/age. The enviable by-products of the application of ICTs such as the electronic card readers and biometric data capture machine in the just concluded 2015 nation-wide general elections in Nigeria leaves much to be continually appreciated, desired, nurtured, promoted and sustained when compared to the hitherto masqueraded elections.

It is an established fact that electoral malpractices are endless depending on the prevailing political terrain and structure. One reliable option to effectively checkmate electoral malpractices to the barest minimum and enshrine confidence, fairness, integrity, and trust in the electoral system and ensure its sustainability is to employ Information and Communication Technologies (ICTs) in the management of electoral systems and processes. As veritable tools fundamental to effective operations and management of organisational activities, the application of ICTs in electoral management is found to greatly minimise to the barest minimum, electoral malpractices which include but not limited to:

- cases of multiple registration of voters and voting;
- distortion of voters' registration list;
- inflation of voters registration ;
- over registration and under-registration of voters;
- inclusion of fictitious names in the voters registration list;
- collusion with EMB operatives to favour some anointed candidates or parties at the pools;
- distortion and falsification of election results through systematised manufacturing and manipulation of the vote counts.

However, in an attempt to overcome the continuing rude shocks of electoral malpractices from favoured party and politicians by the helpless minority parties, it promotes collaboration, merger, and alliance of opposition parties to form a mega party to dislodge the incumbent government and the domineering political party. In a study conducted on electoral malpractices in Latin America, Eastern Europe, former Soviet Union, and Sub-Saharan Africa, Birch (2010) disaggregated electoral malpractices along three principal dimensions: manipulation of the rules governing election;

manipulation of vote choice-candidates electorate votes for; and manipulation of voting –electoral administration.

Considering the fore-goings, you do not to agree with me more that ICTs are required as a matter of policy to checkmate the wrongs consciously or unconsciously committed during voter's registration; voters' verification and accreditation; voting processes; vote counting and collation; and election results transfers/ postings to central collation centres to ensure accountability, transparency and fair play. Essentially, considering the critical and sensitive nature of electoral management , election processes and voting in the scheme of political advancement and survival of any nation, the need to apply ICTs in the management of electoral systems and processes should be seen as direct response to the obvious need for the EMB at the national and sectoral levels to continuously generate; acquire; identify; locate; store; process; retrieve; access; transfer; provide; deliver; and utilise all types of relevant political and election related information envisioned to facilitate achieving the mandate of the EMB and also to satisfy the need of the stakeholders at the national and sectoral polity and electoral systems on 24/7 operations regime at least costs and time of information access irrespective of the location. This will facilitate taking appropriate decisions and actions that will by and large positively impact on the political parties; politicians; the electorates; political systems and structures; the government; and the society at large.

It has been observed by Mohammed (2014) that conceptually, ICT is seen as the use of computer based information and communication systems to acquire, generate process, store and transmit data. He added that, while ICTs are generically considered as technologies used for collecting, storing, editing and passing on or communicating information in different forms, some authors and contributors to the debate consider ICTs to include telecommunication technologies such as satellite; radio and television; telephony and digital technologies such as information networks; computer hardware and software; digital networks; and Internet. He concluded that generally, ICTs can be conceived as automated and virtual products (including software applications) and services that facilitate information generation, identification, location, storage, retrieval, dissemination, access and utilisation. He submitted that some of the early ICTs include: television, radio, telephone, and still camera and slide projectors. Whereas, the contemporary ICTs include: television cabled news networks, digitised radio and television sets; computers; digital camera and projectors; satellite and wireless systems such as smart phones; tablets; Internet; Local , Area and wide networks; and e-information resources. Fundamentally, the concept of ICT can be tallied with that of technology which can simply be conceived as an instrument; equipment; device; infrastructure; and tool used to support, facilitate and sustain effective and efficient performance of a system, an operation; a duty; a task; and a function as well as provision of a varied service.

The effective deployment and exploitation of the ICT technologies at various levels and platforms has facilitated organisations' institutions' and indeed the individuals' efforts to continuously generate, acquire, identify, locate, store, process, retrieve and access variety of data and information envisioned to be relevant and strategic to meeting their immediate and future needs and expectations; and also package, transfer, provide, deliver and utilise them accordingly by the relevant stakeholders far and wide without recourse to location and on 24/7 regime. It has been observed that governmental and non-governmental institutions, organisations and agencies are steadily embracing the digital technologies and networks in their schemes of operations and services to cope with the challenges of the information age.

Cybersecurity and Electoral System

It is an established fact that the effective deployment, utilisation and sustenance of network technologies, particularly the Internet and other facets of Cloud- based or rather, online-based systems, products and services is systematically being hampered by variety of encumbrances such as socio- political, economic and ethical issues and considerations; blackmail and extortion; political, philosophical and ideological cynicism and differences; terrorism; hacktivism; criminality; and other forms of malicious online delinquencies aimed at attacking the smooth operations of the network systems and services to satisfy their ulterior desires. These forms of online sophisticated and stealthy network security threats, breaches and risks call for the deployment of effective and efficient cyber security systems, frameworks and cultures by public and private organisations, institutions and agencies as well as the individuals to checkmate the cyber hoodlums.

By and large, cyber insecurity has no boundary as it is aimed at attacking all categories of people, institutions, organisations, agencies, individuals, systems and devices on both off-line and online. It is a common knowledge that information divulged online, even on private websites and chats is susceptible to hacking; spamming; tracking; interception; intimidation; and blackmail by the fifth columnists, spies and other people of the under-world. The concomitant effects of WikiLeaks on the USA's and its allies' government privacy; the Harley Burton saga in USA; the interference of the USA satellites and other sensitive security networks between 2007 and 2008 and by the North Korea in 2014/2015; the hacking of the Predators by the Iraqi militants; the interference of the official website of the Federal Republic of Nigeria (www.nigeria.gov.ng) by the Irish Gay hacker in2013 to protest the anti-gay bill passed by the Nigerian Senate, etc. are on records and require no further debate.

Basically, whether it is for defensive or offensive purposes, cyber-attacks are made to inflict some desired effects on the cyber operations of the target by way of either to destroy or neutralise the functions. Fundamentally, it can be argued that the rigmaroles of cyber insecurity and indeed cyber security can be viewed from the perspectives of:

- type and nature of network system deployed and being utilised;
- category and capacity of systems users;
- type and efficacy of the systems management structure;
- type and effectiveness of systems management and use policies;
- type, costs and efficacy of the security platform, systems and devices deployed;
- type of data and information being processed, packaged, accessed, transferred and secured;
- type and structure of database;
- costs and type of systems maintenance and sustenance protocols and policies;
- costs and type of capacity building programmes for systems managers and users;
- type and parameter of legal and ethical issues and considerations; and
- type and levels of services access and provision.

Attacks on Cyber networks and indeed on other digital network platforms which the EMBs and other managers of public and private institutions, agencies, organisation and systems need to be worrisome about and should strategise to effectively combat their menace can be in different dimensions and formats which include but not limited to:

- wilful misdirection of electronic messages;
- unlawful interception and bugging of inter and intra communication and messages among the stakeholders;
- computer related frauds and forgery;
- interception of electronic messages, mails and money transfers;
- unlawful access to computer systems and digital databases;
- deliberate arson and theft of strategic electronic infrastructure and devices;
- forgery of electronic signature and codes;
- fraudulent modification and configuration of computer systems, networks, databases and systems interfaces;
- unauthorised issuance of electronic transactions;
- phishing, spamming and spread of computer viruses;
- utilisation of fraudulent devices and attached websites and e-mails;
- deliberate collusion to obstruct and refuse the release of information officially ordered for or needed; and
- Systematic collusion with charlatans to dysfunction strategic systems, operations and services; etc.

Technology Acceptance, Adoption and Utilisation

From both theoretical and practical perspectives, Mohammed (2015) submitted that the extent of technology acceptance, adoption and application (to the management of the EMBs and other public and private digital systems, operations and services)can greatly be affected by the consequences of the implications of the impact of the psychology of and theories of management and practices particularly, as it relates to behaviourism (human- characteristics and attitudes), cognitivism (brain-based- human memory and perceptions) and constructivism (management- administrator's and operator's own construct of fulfilment, achievement, experience and perspectives). In like manner, he is of the view that, technology adoption, acceptability and application to systems management, functions, operations and services can significantly be affected positively or otherwise by variety of factors such as:

- the peculiar predispositions of the management, administrator and operator;
- the prevailing circumstances surrounding the systems environments;
- the stakeholders' perceived usefulness, relevance, availability, adequacy and appropriateness of the technology being adopted and adapted; and
- the type and functionality of the technologies in use.

By and large, he added that, the application and/or non-application of technologies to the management of systems, operations and services can be influenced by:

- the operator's and user's characteristics, skills and experiences in using the technology;
- the type of technologies available, adaptable and useable;
- the type and feature of the systems environments;

- the users' perceived usefulness and relevance of the technology in actualising the mission, goals and aspiration of the project in one hand, and achieving their individual and collective objectives and aspirations on the other hand;
- the context of the vision, mission and objectives of the project;
- the level of access and ease of use of the technology by the stakeholders;
- the perceived attitudes, experiences and opinions of others on the usefulness, relevance and ease of use of the technologies to achieve the desired target;
- the stakeholders' technology fluency, literacy and competence;
- the perceived levels of the stakeholders' skills, potentials, motivation, capacity, ability, willingness and readiness to effective utilise the technologies;
- the perceived implications of the cognitive outcome of applying the technology; and
- the methodology adopted to effectively queue in the stakeholders to accept, adopt and utilise the technologies to achieve the vision, mission, goals and objectives in focus.

Challenges to Technology Acceptance, Adoption and Utilisation.

There is no doubt in the fact that the ICTs particularly the Internet and other network technologies and tools have effectively impacted on the management, functions, operations and services of public and private establishments and systems from all dimensions and perspectives. However, Mohammed (2015) observed that effective adoption and exploitation of the state-of-the-art ICTs especially in developing countries are systematically being affected by variety of challenges which include:

- costs of computer hard ware and software acquisitions;
- costs of systems upgrades;
- systems malfunction and costs of maintenance;
- heavy online access traffic jam especially on popular networks and websites;
- information overload on thematic topical issues and search;
- lack of sustained sources of electric power supply;
- the administrators', operators' and users' phobia for technology applications, especially the computers;
- physical challenges to ICT systems usage especially when charging them;
- preponderance of unsolicited advertisements on the Internet sites;
- costs of Internet and related computer networks connectivity;
- dwindling budgetary allocations, access and utilisation;
- Internet/online information search difficulties and frustrations;
- administrators', operators' and users' bankruptcy in information and computer literacy/ fluency;
- inadequate and sometimes absence of technical support from systems suppliers due to non-renewal of systems maintenance agreement contract or deliberate collusion to sabotage the smooth operations of the systems;
- lack of adequate genuine spare parts;
- inadequate expert technicians;
- human errors and inequities;
- inadequacy of time to effectively access and utilise the ICT tools and services due to the users' personal pressing commitments and engagements;

- environmental and other natural disasters;
- non-compliance with the terms of contractual agreements between the service providers and customers/ consumers;
- oversubscription of inadequately available computer systems and bandwidth due to over populated students' enrolments; and
- inadequate time for practical teaching, learning and familiarisation with the technologies' potentials.

Cyber Security Management Expectations

Generally, it is expedient that cybersecurity adoption, management and sustenance are conceived from holistic perspectives and framework covering managerial considerations such areas:

- the management and leadership of the organisation especially as it relates commitment, diligence and readiness to manage risks and continually invest in the systems;
- human considerations and factors related to the extent of the integration of the right stakeholders into the security management scheme particularly through training and re-training to acquire the requisite security education, knowledge, skills and culture to enhance effective utilisation of the systems;
- system continuity and information risk management approaches that shall ensure robust comprehensive and effective risk management of security-related information within and outside the establishment continually;
- control measures adoption and implementation to checkmate identified cyber security risks and minimisation of impacts on security compromise on the technology and operations; and
- regularity in legal compliance with relevant national and international regulatory certification standards and benchmarks.

Fundamentally, cyber security model should be holistic in structure and outlook to accommodate the relevant sectors of an establishment. Ideally, holistic cyber security model should address critical issues related to:

- minimisation of risks of security attacks on the establishment by outside cyber hoodlums and also limit the impact of any successful attack;
- availability of relevant information on cybercrime trends and incidences to facilitate decision-making;
- a clear understanding of the roles of the stakeholders during and after cyber-attacks and suspected attempts ;
- stakeholders' confidence and assurance of the deployment of effective cyber security systems and plans by the establishment to boost its reputation, readiness, capacity, ability and competence;
- confidence in the establishment's assured increased knowledge and competence in cyber security; and
- upliftment of the establishment to attain the requisite cyber security benchmark and minimum standards.

The Way Forward

It has been observed that effective cybersecurity assurance in any establishment is a by-product the type of security technologies and gadgets put in place in one hand, and the extent of the attitude, behaviour, commitment, readiness, ability and capacity of the management, staff and users of the systems and services on the hand to faithfully implement and sustain security assurance endeavours. It should however be noted that:

- ✈ it is a mirage to attain 100% security in most cases as the continuous efforts to counter security risks and threats are also continually being subverted by the people of the underworld;
- ✈ Investing and re-investing heavily on the-state –of –the art security devices per se may not be the only solution as effective cyber security also dependents more on the humans in addition to technology;
- ✈ aiming to have better security infrastructure to outsmart the hackers may depend on the primary goals of the security policy;
- ✈ Cyber security compliance should go beyond effective monitoring to include ability to learn what should be done;
- ✈ recruiting best professionals to defend cybercrimes should be backed by attitude.

Food For Thought

The need to continually have a free, fair, credible and acceptable electoral process and results under secured and liberal democratic platform where all and sundry can exercise their right to vote and be voted for especially using the state-of-the-art technologies should be the vision, mission and goals of EMBs in the 21st digital age. In order to meet up to the exigencies of the contemporary world, the EMBs have to continually keep some basic questions in focus to effectively guide the management, processes and operations of electoral system. Such questions should determine:

- ✍ whether the EMB indeed has anything about it that is prone to malicious attack;
- ✍ to what extent the EMB security measures put in place are confidently effective and efficient;
- ✍ to what extent security is seen as an effective enabler to further and future successes of the EMB;
- ✍ which viable options should be adopted to cost-justify further human and material investments and re-investments for enhanced security;
- ✍ to what extent the impact of presumable successful cyber-attack is comprehended;
- ✍ to what extent is the model of the security architecture and hierarchy deployed and managed are relevant and effective; and
- ✍ to what extent legal obligations and contractual agreements on systems security are regularly adhered to and sustained;
- ✍ the security profile and the extent of the security risks of the EMB and in relation to other institutions and agencies it associates with;
- ✍ the coverage of cyber security budget and extent of access and utilisation; and
- ✍ the levels and extent of the EMB's attitude, behaviour, culture, support and commitment to technologies applications to electoral system management and security.

As a way forward, there is the need for the EMB to have provision for:

-.

- periodic risk and vulnerability assessment;
- Security improvement plans;
- insider threat analysis, threat trends, training service, recovery planning, security audit;
- security management services including network and device management, incident response strategies;
- System teats and evaluation; and

cyber security standards for the security of infrastructure, device, services, protocols, tools and techniques to ensure robust, reliable and dependable system security.

References

Birch, D (2010). Patterns of Electoral Malpractice- Working Paper No. 4. Project on Malpractice in New and Semi-Democracies. University of Essex.

Diamond, L. (2002). Free and Fair? The Administration of the and conduct of the 1983 Nigerian Elections. In: A.A. Akinsanya, G.J. Idang (Eds) Nigerian Government and Politics: 1979-1983. Calabar: Wusen Publishers, p.353.

Krouse, R.W. (1982). Two Concepts of Democratic Representation: James and John Stuart Mill. Journal of Politics, 44(2), p.529.

Mohammed, Z. (2014).Promotion and Utilisation of Indigenous ICT Products and Services for National Development. A paper presented at the e-Nigeria 2014 Annual Information Technology Summit organised by the National Information Technology Agency (NITDA) in collaboration with relevant stakeholders from private and public sectors, and the non-governmental Organisations Held at The Congress Hall, Transcorp Hilton Hotel, Abuja Between 18th and 20th November. pp 2-3.

Mohammed, Z. (2015). Exploring the Potentials of Web Technologies in Education, Training, Teaching, Learning and Research in Educational Institutions in Nigeria. A Lead Paper presented At the Workshop on Web Technology Fluency for Teaching and Research Held at the MTN Connect Library, Kashim Ibrahim Library, Ahmadu Bello University, Zaria Between 12th and 14TH May, pp.5-6.