THE INTERNATIONAL JOURNAL OF SCIENCE & TECHNOLEDGE

Cyber Security Threats and Challenges in Nigerian Elections

Mbing Isaac
Lecturer, Department of Computer Science, Kaduna Polytechnic, Kaduna, Nigeria
Akinjobi Joshua Adekunle
Lecturer, Department of Computer Science, College of Natural and Applied Sciences, Crawford University, Igbesa, Ogun State, Nigeria
Obasa Adekunle Isiaka
Lecturer, Department of Computer Science, Kaduna Polytechnic, Kaduna, Nigeria

Abstract:
Technological advances have changed every aspect of societal activity and behaviour in generally all aspects of our lives. With these advancements come vulnerability in preserving the integrity, security and confidence of communication activities. This paper discusses cyber security as it affects elections. As Nigeria joins the rest of the modern world in introducing electronic equipment in her election processes, Cyber security considerations must be at the fore front to avoid being at the mercy of sophisticated criminals who may take advantage of the low digital awareness of the teeming stakeholders to swing victory or expose information and data that hitherto must be for the consumption of few. Suggestions are made for the electoral commission managers' consumption

Keywords: *Cyber security, Cyber space, Critical Infrastructure, Electoral process*

1. Introduction

Thecopedia defines Cyber security as the body of technologies, processes and practices designed to protect networks, computers, programs and data from attacks, damage or unauthorized access. Cyber security therefore considers methods of information protection from theft, attacks and corruption.

Scholars have argued whether it should be Cyber security or Cyber Security. This paper will go along with Gartner, a World leading information Technology Research and Advisory company who opine that the use of the term 'Cyber security' in one world be adopted. It encompasses security practices related to the combination of offensive and defensive activities involving or relying upon information and operational technology environment and systems. Longe and Chiemeka (2008) opined that technological advancements have produced radical shifts in the ability to reproduce, distribute, control and publish information. The internet in particular has radically changed the economics and ease of reproduction of documents. This has been made possible and easier because the ability of the internet to transport text, sound, video and pictures in a very high speed and quantity.

1.1. Election as a National Security Concern

Wikipedia (the free encyclopedia) defines National Security as' a concept that a government along with its parliament should protect the state and its citizens against all kinds of national crisis through a variety of power projections'. The McMillan Dictionary (online) looks at it as 'protection of the safety of a country's secrets and its citizens'. However, Prabhakana (2008) opines that it is the measurable state of the capability of a nation to overcome the multidimensional threats to the apparent well-being of its people and the survival as a nation state at any given time by balancing all instruments of state policy through governance that can be indexed by computation, empirical or otherwise'.

Dasuki (2014) stated that the potency of threat of terrorism, militancy, oil theft, vandalism and sabotage of critical assets and infrastructure has now become unprecedented

Elections security in any society are closely link to national security and should therefore be given due consideration. Traditionally, in elections, authorities ensure that candidates, voters, electoral workers, observers, sensitive materials, results collation and transport, announcements of partial and final results are given physical security through deployment of security agents to the various locations of concern. Mismanaged elections may lead to ethnic conflicts, regional insecurity, protest or violent contestations argues Hounkpe et al (2010).

1.2. Elections as a Critical Infrastructure

In the national Cyber security policy (2014), part 7 identifies fifteen Nigeria national critical infrastructure including Information Technology. They are part of the assets, systems, and networks, whether physical or virtual, so vital to the country that their incapacitation or destruction or any other form of attack on them would have a debilitating effect on security, national economic security, national public health or safety, or any combination of them. No mention is made of Elections. It is however worthy to note that certain systems and assets of elections infrastructure meet the definition of critical infrastructure. Having in mind that Critical infrastructures are all these infrastructures which our society depends on in daily life, not only transport or energy or oil but many other sectors could be included in that list. Fair elections contribute to the stability of a country. They are targeted by cybercriminal in other to fraudulently rigged elections or as in recent times reveal electoral secrets to unauthorized persons. Physical and virtual assets or facilities, whether owned by private or

public entities which are essential to the provision of vital services to Nigerians for their social and economic well-being, and which if destroyed, will degrade or render unavailable, or will impact on the social or economic well-being of the nation or affect Nigeria's ability to conduct national defence and security should be classified as critical Infrastructure. The elections system in Nigeria should therefore be declared as critical infrastructure.

Designating the electoral process as critical infrastructure will have several advantages. Such a declaration would spur a coordinated overall approach in the management, development and mitigation of cybersecurity vulnerabilities in the electoral process, thereby helping to identify and stop threats. It will also ensure better encryption of voter systems since they will merit funding to engage in capacity-building

1.3. Cybercrime in Elections

With the advent of computers, the internet and various technological innovations, there arose monstrous criminal and anti-social activities perpetrated by several criminals on unsuspecting users on these huge technological resources. Criminal activities perpetrated on the internet range from fraud, theft, pervasive pornography, child pornography, paedophile rings, drug trafficking, extortion, hacking, copyright infringement, plagiarism, child grooming, cyber stalking, cyber warfare, cyber terrorism, to mention but a few. –

The "cyber" environment includes all forms of digital activities, regardless of whether they are conducted through networks and without borders. This extends the previous term "computer crime" to encompass crimes committed using the Internet, all digital crimes, and crimes involving tele-communications networks as argued by Guinier (2010).

Cyber risks are therefore of two distinct types:

i) Cybercrimes: extraction of money, credit card data, cause disruption of communication, intercept mails and other sensitive information
ii) Cyber war use of advanced persistence threats to carry on sabotage, espionage against another nation or state in order to cause disruption or extract data.

Because the cyber space is unregulated, inexpensive, cyber criminals have found it a fertile ground. Some of the common cyber crimes include:

i) Virus: it is an infiltration theft, modification and/or corruption of information and files from a targeted computer system.
ii) Worms: exploit weaknesses in operating systems in order to damage networks.
iii) Spyware and malware: take control of one's computer and/or collect personal information without one's knowledge
iv) Trojan: create a backdoor on one's computer by which information can be stolen and damage caused.
v) Phishing: is an attempt to acquire user information by posing as a legitimate entity.
vi) Pharming: is an attack to re-direct a website's traffic to a different, fake website where user information is compromised.
vii) Drive-by: is an opportunistic attack against specific weaknesses of one's system
viii) Man-in-the middle: is an attack where a middle man impersonates each end-point and manipulates the victims.
ix) Spamming: involves mass amounts of email being sent in order to promote and advertise products and websites. Spammers are also devising advanced techniques to avoid spam filters, such as permutation of the emails contents and use of imagery that cannot be detected by spam filters.
x) Vote flipping: is a nastier attack that requires an attacker to access the computers inside voting systems.
xi) Cyber harassment: is electronically and intentionally carried out by threatening acts against individuals. Such acts include cyberstalking

There are many more such attacks as criminal daily research on new methods as technology constantly improves. All of these attacks can be deployed in an election system.

1.4. Cyber-attacks Statistics

Let's briefly look at the increase in these attacks in order to appreciate the risks at our door steps. The following figure will give us a slight idea of the problem

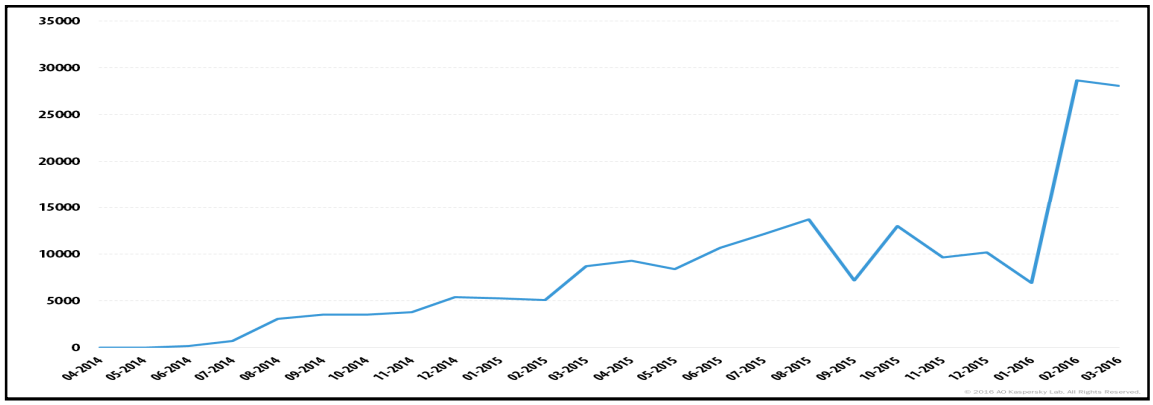

Figure 1: Source:https://i2.wp.com/kasperskycontenthub.com/securelist/files/2016/11/mw2C583&ssl=1

It is obvious that the trend is increasing `

1.5. State of Cyber Security and Protection in Nigeria

Within and outside the shores of Nigeria, the ugly situation of cybercrimes is causing embarrassment for citizens at both social and business gatherings. These cybercrimes and other internet abuses have been described as hindrance to development in Nigeria opined Ekeke (2012) Meanwhile, some efforts are ongoing to tackle the menace of cybercrime in the country. At the then first National Cyber Security Forum in Lagos, the National Security Adviser, Col. Sambo Dasuki (rtd) opined that "the abnormal trend of cybercrime is denting Nigeria's image, and that the cyber terrorists have succeeded in changing the way Nigerians see and relate with one another." According to him, "Realizing the importance of cyber space, the Federal Government of Nigeria has designated cyber security as a national security priority with the office of the National Security Adviser (ONSA) stepping up efforts towards meeting the challenge by working in close collaboration with all stakeholders to ensure a safer and more secure cyberspace." Akingbolu, (2014)

1.6. Challenges of Elections Cyber crimes

The various targets in any election could be summarized thus:

i) Information stored by campaign managers (donors and their donations, various emails, opposition researches and vulnerability studies),
ii) Campaign strategies information
iii) Using specific information to influence public opinion for/or against a candidate. Criminals here may pharm of phish in a prominent personality system or website.
iv) Poking among voter's registration data. During registration of voters, hackers take advantage of lukewarm interest of participants to gather sufficient voters' data.
v) Compromising users' accounts can also impact negatively on a campaign the use of social media accounts to disseminate false information to the media networks and online services can impact negatively or positively on the supporters.
vi) Results compilation that are being sent to the collection centre database can be taped on the network and results compromised.
vii) The role of in-house sophisticated programmers who can rewrite codes for window manager components of the operating systems to rig elections. Some of these programming can be written to start execution only on voting dates. That may be the reason why change of voting dates may become a herculean task

All the above and many more are attacks that can be planned and carried out on elections to swing votes, expose candidates or parties, leak vital and confidential information that may be damaging to whoever is concerned.

2. Conclusion

In fighting cybercrimes, the significance of cyber legislation cannot be overemphasized in our contemporary Nigerian society as it concerns elections. There is no doubt that prevention of cybercrimes and enforcement of cyber security is a necessity in Nigeria requiring holistic attention of all stakeholders.

Cyber ethics education will go a long way in addressing the menace in the country. Cyber ethics education for prevention of cybercrimes should be emphasized.

Attempts have been made above to point out cyber security risks and vulnerable areas. Attacks in cyber security elections may not be visible immediately. It is however pertinent to note that before, during or after elections, sensitive hacked information may be released with serious damaging effects on the actors. We also will not forget the integrity of the election which may be difficult to prove otherwise in a court of law. It is time to take pro-active measures before the nation be confronted with election cyber security issues.

2.1. Suggestion to Challenges

i. There should first of all be wide cyber security awareness trainings among youth, students in post-secondary institutions and also among election workers both permanent and temporary.
ii. Involve also service providers in the management of cyber security.
iii. Ensure the development of a national cyber security technology framework to specify cyber security standards, awareness education.
iv. Harmonize local laws with international best practices
v. Increase security personnel professionalism in cybercrime detection, reporting and prosecution
vi. Involve cyber security experts in the formulation of relevant policies.
vii. Leverage on the right set of technology and practices before embarking on aggressive computerization of elections
viii. In addition to the existing ones, more Rural Information Technology Centres should be established.
ix. There is need to protect the election system from cyber interference by checking the use of voting machines connected by wireless networks while encouraging the deployment of machines that produce auditable paper trails.
x. Government officials and non-governmental organizations that support elections should adopt measures to protect election systems from online threats, deter cyber interference with such systems, and reassure citizens that their right to vote is defended. Achieving these objectives requires local, national, and international actions to strengthen cyber security in election systems and to elevate election integrity in cyber security policies, human rights activities, and election assistance and monitoring
xi. Acceptance tests for the electronic equipments that will be used should be performed at the national, state or local government levels upon equipment delivery by the manufacturer and the well-trained ICT personnel of the electoral body to confirm that the equipment delivered meet the specifications demanded.
xii. The election personnel to conduct voting with the voting equipment should be ready and tested prior to the start of an election to ensure that they understand and master the voting system functions properly, and confirm that voting equipment has been properly integrated, and equipment status reports produced.
xiii. Election officials also should perform verification at the polling place and any central locations used for vote counting to ensure that all voting systems and voting equipment function properly before, during, and after an election.

3. References

i. Akingbolu, R. (2014) Nigeria: combating cybercrime through constructive engagement. Accessed July 9, 2014 from *http://allafrica.com/stories/201407101214.h tml.*
ii. Daniel GUINIER (2010) Prospective Analysis on Trends in Cybercrime from 2011 to 2020 McAfee Labs
iii. Dasuki S. (2013). Protecting our critical national assets. Retrieved 14th August, 2015 from http://weekend.peoplesdailyng.com/index.php/opinion/opinion/885-protecting-our-critical-nationalassets
iv. Ehimen O. R, Bola A (2010). Cybercrime in Nigeria. Bus. Intell. J. 3(1):26
v. Ekeke, E.C. (2012) Internet abuses as hindrance to development in Nigeria: a Christian ethical approach. International Journal of Asian Social Science, 2 (7), 1123 – 1131Gatner ' gatner Copyright & Guide Policy Section. www.gatner.com/
vi. Hounkpe,Mathew &Gueye,Alioune Badara (2010) 'The Role of Security Forces in the Electoral Process: The case of six West African Countries' AbujaFriedrich-Ebert-Stiflung.
vii. Longe O.B, Chiemeka, S.C (2008) Cybercrime and Criminality in Nigeria: What roles are Internet acHcess points playing ? Eur Journal of Social Science 135-139
viii. Odumesi JO (2006). Combating the menace of cybercrime: The Nigerian Approach (Project), Department of Sociology, University of Abuja, Nigeria p.45.
ix. Palen, Prabhakaran (2008) 'national security Imperatives and Challenges' New delhi, tata McGraw, p52
wikipedia.org/wiki/Baron_Verulam
http://www.finedictionary.com/baron%20verulam.html
https://www.supportthevoter.gov/ (link is external)
https://www.nased.org/