ASSESSMENT OF NATIONAL INTERNET SAFETY STRATEGY IN COMBATING CYBERCRIME IN NIGERIA

BY

DR HENRY I. OKON
DEPARTMENT OF EDUCATIONAL TECHNOLOGY AND LIBRARY SCIENCE
FACULTY OF EDUCATION
UNIVERSITY OF UYO, UYO
AKWA IBOM STATE

ABSTRACT

The study assessed the national internet safety strategy in combating cybercrime in Nigeria. One specific research objective was formulated to guide the study. The research design was an Expose-Facto research design. The population of the study comprised of all the personnel of the Nigerian police, NCC, ICPC, EFCC, NPF, NCWG, NCIC, CBN, in Nigeria. 350 respondents were randomly selected for the study, using simple random sampling technique. The research instrument tagged "NATIONAL INTERNET SAFETY STRATEGY AND CYBERCRIME QUESTIONNAIRE, (NISSCQ)" was used to collect data from the respondents. The test produced high average reliability coefficient of 0.92 which helped justify the use of the instrument. The findings from the data collection and analysis showed that strategy on national internet safety has significant impact on combating cybercrimes in Nigeria. Among others, it was recommended that there is a need for most Nigerians to pass into law a specific cybercrime law and that this law should classify cybercrimes as this would make it easier for law enforcement agents to investigate and prosecute cybercrimes within the borders of Nigeria.

KEYWORD: National internet safety, combat, cybercrimes, Nigeria.

Introduction

The development and improvement of the internet with new distinctive features and ability has widened the access to computer technology and created new opportunities for work and business activities. It has also poised threats to people using it either for business or leisure. Brenner (2007). The emergence of technology and electronic communication has brought far-reaching increase in the incidence of criminal activities. Crime and corruption represent a major concern for business executives not only in Nigeria but also in other parts of Africa. In Nigeria, for instance, the most serious impediments to economic activities and business are crime and corruption which averages 75% and 71% respectively (Fanawopo, 2004; Maitanmi, 2013). By definition, cyber crime may be referred to as any form of misconduct in cyber space. It is simply defined as the criminal use of the Internet. Cyber crime is believed to have started in the 1960's in the form of hacking. This was followed by privacy violations, telephone tapping, trespassing and distribution of illegal materials in the 1970s. The 1980s witnessed the introduction of viruses (Loader, 2000; Ali et al., 2014).

The fast pace of development of ICT from the 1990s till today has added to the list of criminal exploits in cyber space (Gercke, 2006). Today, the Internet is used for espionage and as a medium to commit terrorism and transnational crimes. With e-banking gaining ground in Nigeria and other parts of the world, customers and online buyers are facing great risk of unknowingly

passing on their information to fraudsters (Atili, 2011). Hackers get information on those who have made purchases through websites and then make fake cards, which they

use with less detection. Absence of a law specifically dealing with card-related crimes in Nigeria may be giving thieves a loophole to operate freely.

The internet creates unlimited profit oriented opportunities for commercial, social and other human activities. The advent and introduction of cybercrime has put the users of Internet to a higher risk. The global village currently records an increasing criminal behaviour. News of cybercriminal activities continue to fill the pages of the newspaper, it is central to world news and has become a global problem. There is hardly a place where computers and internet facilities are found that cases of crime are not recorded. New modes of operation are developing as the Global System for Mobile-telecommunication (GSM) is now used for browsing. A lot of young people are commonly among the perpetrators of these criminal activities. They spend hours browsing and sometimes stay awake all night to carry out their nefarious activities. This has therefore necessitated the need for a national internet safety strategy to help checkmate these crimes as cybercrimes are described as one of the fastest growing criminal activities on the planet. It covers a large range of illegalities including but not restricted to financial scams, computer hacking, downloading of pornographic images from the internet, virus attacks, stalking and creating websites that promote hatred. This study hereby seeks to address the national internet safety strategy in combating cybercrime in Nigeria.

Conceptual framework

The Concept of National Internet Safety

National internet safety is the nation's readiness strategy to provide cohesive measures and strategic actions towards assuring security and protection of the country presence in cyberspace, safeguarding critical information infrastructure, building and nurturing trusted cyber-community (Macharia, 2014). The Strategy provides various initiatives for the focused areas and national mechanisms for developing and implementing legal and policy measures, national incident management, critical information infrastructure protection, cyber security assurance framework, manpower development, child online abuse and exploitation, national internet safety, public awareness, multi stakeholder partnership and global cooperation on cyber security (Howell and Lind, 2009; Ploch, 2010).

According to Stremlau and Osman (2015), the National internet safety comprises of short, medium and longterm mitigation strategies covering all national priorities, addressing the nation's cyber risk exposure. Specific key cyber threats worldwide inimical to National interests are identified such as; Cybercrime; Cyber-terrorism; Cyber conflict; Cyber espionage Child online abuse and exploitation. The Strategy aims are to set out a national roadmap with various coordinated mechanisms; harness implementation framework and actions that will guarantee attainment of the National vision, mission and goals on Cyber security as captured in the National Cyber Security Policy. Therefore, the Strategy is needed to achieve the following specific objectives:

1. A comprehensive cybercrime legislation and cyber-threat counter measures that are nationally adoptable, regionally and globally relevant in the context of securing the nation's cyberspace.
2. National mechanisms on capacity building, public awareness, skills empowerment is necessary to help strengthen our capability so as to respond promptly and effectively to cyber-attacks.

3. A trusted mechanism for engaging national multi-stakeholder and international partners towards collectively addressing cyber threats.

The strategy is further aligned with National Security Strategy and other relevant government documents most especially National ICT policy and National broadband plan. The Strategy defines the basis for a coordinated national and globally compatible

framework for action, cooperation and approach to protecting national critical information infrastructure against cyber threats (Greenwald, 2014).

The concept of Strategy

Strategy is a high-level plan to achieve one or more goals under conditions of uncertainty. In the sense of the "art of the general", which includes several subsets of skills including tactics, siege craft, logistics etc., the term came into use in the 6th century AD in East Roman terminology, and was translated into Western vernacular languages only in the 18th century. From then until the 20th century, the word "strategy" came to denote "a comprehensive way to try to pursue political ends, including the threat or actual use of force, in a dialectic of wills in a military conflict, in which both adversaries interact (Lawrence, 2013).

According to Lawrence (2013), strategy generally involves setting goals, determining actions to achieve the goals, and mobilizing resources to execute the actions. Strategy is important because the resources available to achieve goals are usually limited. Simandan (2018) asserts that a strategy describes how the ends (goals) will be achieved by the means (resources). Strategy can be intended or can emerge as a pattern of activity as the organization adapts to its environment or competes.

The UK National Cyber Security Strategy emphasizes the importance of partnerships among government, industry and academia to meet the primary objective of the strategy which is "making the UK one of the most secure places in the world to do business in cyber space". Cybercrime is broad and complex, and focuses on networks and data in both the public and private domain largely to steal money and intellectual property. Kshetri (2010) asserts that cybercrime if not properly checked will grow in frequency and superiority because adversaries can afford new technology and techniques, including cloud and mobile computing, big-data analytics and artificial intelligence. Nigerian partnership with other related agencies like ITU is one of the strategies which must be adopted to curb the menace of cybercrime.

ITU recognizes five essential factors that will assist any nation in the fight against Cyber insecurity. These are: Legal measures; Technical and procedural measures; Organizational structures; Capacity building; & International Cooperation.

The concept of cybercrime

In the words of Loader (2000), cybercrime implies those computers mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks. Maat (2004) and Bowker (2012) proposed a definition for cybercrime which encompasses all illegal activities where the computer, computer systems, information network or data is the target of the crime and those known illegal activities or crime that are actively committed through or with the aid of computer, computer systems, information network or data. It is significant to note that there is no consistent and statutory definition for cybercrime (Wada, Longe and Paul Danquah, 2012, Moore, 2005).

Ifukor (2006) and Laver (2005) stated that cyber crime includes all forms of crime committed through the use of the internet. They are referred to as internet fraud. This means using one or more components of the internet such as chart rooms and emails among others, to

present fraudulent solicitation to prospective victims or to defraud individuals or financial institutions (Choo, 2007).

The Concept of Strategy on National Internet Safety in Combating Cybercrimes in Nigeria

Nigeria like most other nations of the world has seen the urgency and the essence of cyber security and has gone through planning and policy stages and implementation of the Global Cyber Security Agenda and has taken concrete steps to secure its cyber space. In December 2014, Nigeria published its National Cyber Security Strategy which clearly mapped out Nigeria's National Cyber Security Vision and the strategies for achieving this vision. Furthermore, in May, 2015, the President of the Federal Republic of Nigeria signed into law the Nigeria Cybercrime (Prohibition, Prevention, etc.) Act. The Act provides an effective, unified and comprehensive legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment for cybercrimes in Nigeria (Odunfa, 2014). The Act also ensures the protection of critical national information infrastructure, and promotes Cyber Security and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights. The Nigeria National Computer Emergency Response Team (ngCERT) Operations Center was also officially commissioned in May, 2015 by the National Security Adviser (Osho and Onoja, 2015). During the Nigeria Internet Governance Forum (NIGF, 2013), it was estimated that over 95% of Nigerians on the internet are ignorant of personal security and safety responsibility online.

The MITRE Corporation in its 2014 publication suggested workable strategies for effective Cyber security operation centers regardless of their size, offered capabilities or type of constituency served. These strategies include the following:

1. Consolidate functions of incident monitoring, detection, response, coordination, and computer network defense tool engineering, operation, and maintenance under one organization: the CSOC.
2. Give the CSOC the authority to do its job through effective organizational placement and appropriate policies and procedures.
3. Focus on a few activities that the CSOC practices well and avoid the ones it cannot or should not do.
4. Favor staff quality over quantity, employing professionals who are passionate about their jobs, provide a balance of soft and hard skills, and pursue opportunities for growth.
5. Exercise great care in the placement of sensors and collection of data, maximizing signal and minimizing noise.
6. Be a sophisticated consumer and producer of cyber threat intelligence, by creating and trading in cyber threat reporting, incident tips and signatures with other CSOCs.

The preponderance of cybercrimes involving advance fee fraud (419), money laundering, phishing, to mention a few, has had severe negative consequences on Nigeria, including decreased Foreign Direct Investments in the country and tainting Nigeria's image. The menace of cybercrime and the magnitude and gravity of the situation led to the passing into law of the EFCC Act 2004. The EFCC Act also establishes the Economic and Financial Crimes Commission (the EFCC) to implement and execute the provisions of the act.

The EFCC Act mandates the Commission to collaborate with government bodies within and outside Nigeria to identify, determine the whereabouts and activities of persons suspected of being involved in economic and financial crimes. The power of the Commission to investigate all financial crimes including advance fee fraud, money laundering, counterfeiting, illegal charge

transfers, future market of negotiable instruments, computer credit card fraud, contract scam etc (Dasuki, 2011).

According to Steffani (2006), the rationale behind the establishment of the Nigerian Financial Intelligence Unit (NFIU) is to safeguard the Nigerian Financial system and contribute to the global fight against money laundering, terrorism financing and related crimes through the provision of credible financial intelligence. Considering that there are different FIU models, Recommendation of the Financial Action Task Force (FATF) do not prejudge a country's choice for a particular model and applies equally to all of them. The recommendation however emphasizes that countries should establish an FIU with
responsibility for acting as a national centre for receipt and analysis of suspicious transaction reports and other information relevant to money laundering, associated predicate offences and terrorist financing; and for the dissemination of the results of that analysis (Juwah, 2015).

The Unit has since then sought to develop standards and procedures for the receipt, analysis and dissemination of financial intelligence to law enforcement agencies, perform onsite and off-site examination of financial institutions, enhance compliance with the legal and regulatory regimes on Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) in Nigeria as well as respond to the global trends by collaborating with other FIUs worldwide.

Powers/Mandate: - The NFIU largely draws its powers from the Money Laundering (Prohibition) Act 2011 as amended in 2012 and the Economic & Financial Crimes Commission (EFCC) establishment Act, 2002. The core mandate of every FIU as required by international standard is to serve as the national center for the receipt and analysis of: (a) suspicious transaction reports; and (b) other information relevant to money laundering, associated predicate offences and terrorist financing, and for the dissemination of the results of the analysis to law enforcement and anti-corruption agencies. Other Functions of the NFIU include the responsibility to receive currency transactions reports, suspicious transactions reports; currency declaration reports and other information relating to money laundering and terrorist financing activities from financial institutions and designated non-financial institutions (DNFIs); receive reports on cross-border movement of currency and monetary instruments; maintain a comprehensive financial intelligence database for information collection, analysis and exchange with counterpart FIUs in the jurisdiction and law enforcement agencies in Nigeria; advise the government and regulatory authorities on prevention and combating of economic and financial crimes; provide information relating to the commission of an offence by entities and subjects linked to another jurisdiction to foreign financial intelligence unit based on the membership of Egmont Group or on the basis of bilateral cooperation; promote public awareness and understanding of matters relating to economic and financial crimes, money laundering & financing of terrorist activities; liaise with compliance officers and ensure strong compliance culture by reporting entities. The NFIU has a reporting requirement which requires that it works closely with all the core regulators of financial, other financial institutions and designated non-financial businesses and professions, namely the Central Bank of Nigeria (CBN), National Insurance Commission (NAICOM), Securities & Exchange Commission (SEC), Special Control Unit against Money Laundering (SCUML), particularly in the receipt of the following reports:

7. Report of international transfer of funds and securities exceeding US$10,000.00 or naira equivalent as required by Section 2 (1) of the MLP.

8. The STRs mentioned under Section 6 (2) of the MLPA 2011 shall report exclusively to the NFIU to aid intelligence gathering and in line with Financial Action Task Force (FATF) 2012 Recommendations 20 and 29.
9. Declaration reports of more than USD$10,000 or its equivalent made to the Nigerian Customs pursuant to the Foreign Exchange Act, 1995 and Section 2 (3) of the MLP Act, 2011 as amended.

10. Currency Transaction Reports (CTRs) that should be submitted directly to the NFIU from the reporting entities as provided in Section 10 of the MLP Act 2011 as amended. vi. Application of freezing measures under Section 6 (5) (b) of the MLP Act 2011 as amended.

11. Mandatory Disclosures by financial institutions and any other individual (voluntarily) – related to single transaction, lodgment or transfer of funds in excess of ₦5, 000,000 or ₦1, 000,000 by an individual and ₦10, 000,000 or ₦5, 000,000 by a corporate entity as provided Section 10 (1) and (2), MLP Act.
12. Receive STRs on transactions that may relate to Terrorism or terrorist financing from reporting entities as provided under Section 14 of the Prevention of Terrorism Act 2011 as amended in 2013; The financial institutions shall also have regard to the Regulation on the freezing of terrorist assets issued in 2012 by the Attorney General of the Federation and United Nations Security Council Resolutions as issued from time to time.
13. Other statutory reports mandated by the regulators in their AML/CFT Regulations must also be complied with and the reports filed with the NFIU and the regulators.

Theory

Securitization Theory by Weaver (2004)

Weaver (2004) asserts that it is by labelling something a security issue that it becomes one. By stating that a particular referent object is threatened in its existence, a securitizing actor claims a right to extraordinary measures to ensure the referent object's survival. The issue is then moved out of the sphere of normal politics into the realm of emergency politics, where it can be dealt with swiftly and without the normal (democratic) rules and regulations of policy-making. For security this means that it no longer has any given (pre-existing) meaning but that it can be anything a securitizing actor says it is. Security is a social and inter-subjective construction. Buzan (1998) asserts that to prevent 'everything' from becoming a security issue, a successful securitization consists of three steps. These are: (1) identification of existential threats; (2) emergency action; and (3) effects on inter-unit relations by breaking free of rules (Buzan, 1998). This first step towards a successful securitization is called a securitizing move. A securitizing move is in theory an option opened to any unit because only once an actor has convinced an audience (inter-unit relations) of its legitimate need to go beyond otherwise binding rules and regulations (emergency mode) can we identify a case of securitization. In practice, securitization is thus far from being open to all units and their respective subjective threats. Rather, it is largely based on power and capability and therewith the means to socially and politically construct a threat. In this way the study of security remains wide, but with restrictions pertaining to 'who' can securitize it is neither unmanageable nor incoherent.

The application of this theory to the study is that the national internet security should be paramount and enforced as a strategy in the internet world to help combat cybercrime in the society. In other words, the security of people's internet transaction as well as the socio-

economic wellbeing of the people should be prioritized by the state. The scope of global security should be expanded to include threats in seven areas such as internet security which requires using national internet strategies to curb cybercrime.

METHOD

Research Design

An Expost-Facto design was used for this study. It is very obvious that in this type of design the researcher cannot manipulate the effect on the dependent variable but just obtain the effect already existing in the natural course of events.

Area of the Study

The research area for this study was Nigeria. Nigeria is one of the countries in Africa called the giant of Africa. Nigeria has been home to a number of kingdoms and tribal states over the millennia. The modern state originated from British colonial rule beginning in the 19th century, and took its present territorial shape with the merging of the Southern Nigeria Protectorate and Northern Nigeria Protectorate in 1914. The British set up administrative and legal structures whilst practicing indirect rule through traditional chiefdoms. Nigeria became a formally independent federation in 1960. It experienced a civil war from 1967 to 1970. It thereafter alternated between democratically elected civilian governments and military dictatorships until it achieved a stable democracy in 1999, with the 2011 presidential election considered the first to be reasonably free and fair.

Population of the Study

The population of this study comprised all the personnel of the Nigerian police, NCC, ICPC, EFCC, NPF, NCWG, NCIC, CBN, in Nigeria.

Sample and Sampling Techniques

350 respondents were randomly selected for the study, using simple random sampling technique. The research instrument was used to collect data from the respondents.

Instrumentation

The main instrument used in this study was questionnaire titled "NATIONAL INTERNET SAFETY STRATEGY AND CYBERCRIME QUESTIONNAIRE" (NISSCQ). The questionnaire was made up two sections, sections A and section B. Section A was used to collect information on personal data of the respondents while section B of the questionnaire was made to measure the main variables of the research. The obtained data were coded statistically before the statistical analysis of the data.

Validation of the Instrument

The researcher ensured that the instrument passed through face and content validation by the experts in test and measurement in Nasarawa State University.

Reliability of the Instrument:

Pearson Product Moment Correlation was used to determine the reliability coefficient of the instruments. Using the test-retest method, the instruments were administered twice to twenty (20) staff of those organisation (NCC, ICPC, EFCC, NPF, NCWG, NCIC, CBN) in other states with two weeks' interval between each administration. The reliability coefficient for the questionnaire and business studies achievement test ranged of 0.92, which showed that the instruments were highly reliable.

Administration of Instrument

The instruments were administered personally by the researcher to the respondents and this took a period of one week.

Model Specification:

Research question (using percentage analysis)

$$\% = \frac{\mathbf{CF}}{\mathbf{TF}} \; X \frac{\mathbf{100}}{\mathbf{1}}$$

Where CF is the Cell Frequency
TF is the total frequency
100 is a constant value

Hypotheses (using Chi-Square Analysis)

The Null hypothesis states that Strategy on national internet safety has no significant impact on combating cybercrimes in Nigeria.

$$X^2 = \frac{(O-E)^2}{E}$$

Where O = The Observed frequency of people's perception of the extent of the impact of Strategy of national internet safety on combating cybercrimes in Nigeria.
E = the Expected Frequency of people's perception of the extent of the impact of Strategy of national internet safety on combating cybercrimes in Nigeria.
2 = Constant index Number

Method of Data Analysis

Data collected were processed using the Statistical Package for Social Science (SPSS). The research questions were answered using (mean) descriptive statistics; while the hypothesis was tested using the goodness of fit chi-square analysis at 0.05.

Results and Discussion

Research Question

To what extent does strategy on national internet safety help in combating cybercrimes in Nigeria? Table 1 was used to answer the research question.

Table 1:

Descriptive analysis of the extent to which strategy on national internet safety help in combating cybercrimes in Nigeria

Extent of Strategy	Freq	%
Very Great Extent	134	38.29
Great Extent	104	29.71
Average	54	15.43
Low Extent	39	11.14
Very Low Extent	19	5.43
TOTAL	**350**	**100%**

Source: Field Survey

The result in Table 1 shows to what extent the strategy on national internet safety help in combating cybercrimes in Nigeria. From the result, it was observed that 134 (38.29%) of the respondents affirmed a very great extent of strategy on national internet safety which helps in combating cybercrimes in Nigeria while 19(5.43%) of the respondents affirmed very low extent that the strategy on national internet safety help in combating cybercrimes in Nigeria.

Hypothesis

The Null hypothesis states that Strategy on national internet safety has no significant impact on combating cybercrimes in Nigeria. To test the hypothesis, chi-Square analysis was performed on the data (see table 2)

Table 2:
Chi-square analysis of Strategy on national internet safety has no significant impact on combating cybercrimes in Nigeria

National Internet Safety	Observed Freq	Expected Freq	X^2
VERY GREAT EXTENT	134	70	
GREAT EXTENT	104	70	
AVERAGE	54	70	129.57*
LOW EXTENT	39	70	
VERY LOW EXTENT	19	70	
TOTAL	**350**	**350**	

***Significant at 0.05 level; df = 4; Critical = 9.49**

Table 1 shows the calculated X^2-value as (129.57). This value was tested for significance by comparing it with the critical X^2-value (9.49) at 0.05 levels with 3 degree of freedom. The calculated X^2-value (129.57) was greater than the critical X^2-value (9.49). Hence, the result was significant. The result therefore means that the Strategy on national internet safety has no significant impact on combating cybercrimes in Nigeria. The significance of the result caused the null hypothesis to be rejected while the alternative one was accepted.

Discussion of Findings

The results of the data analyses in tables 1 and 2 were significant due to the fact that the calculated X2-value (129.57) was greater than the critical X2-value (9.49) at 0.05 level with 4 degree of freedom. The result implies that the Strategy on national internet safety helps in combating cybercrimes in Nigeria. The significance of the result caused the null hypotheses to be rejected while the alternative one was accepted.

Conclusion

In conclusion, this study assessed the national internet safety strategy in combating cybercrime in Nigeria. Concepts were reviewed as follows; concept of national internet safety, concept of strategy, concept of cybercrime and the concept of strategy on national internet safety in combating cybercrimes in Nigeria. Securitization theory was employed and based on the findings of the research work, it was concluded that strategy on national internet safety has no significant impact in combating cybercrimes in Nigeria. Based on the findings of the research work, it was also concluded that strategy on national internet safety will help in combating cybercrimes in Nigeria and that the controls of operational cyber security of the energy utilities are not applied in compatibility with the risks predicted, regularly tested, monitored and revised. It was hereby recommended that there is the need for the Nigerian government to pass into law a specific cybercrime law. This law should classify cybercrimes as this would make it easier for law enforcement agents to investigate and prosecute cybercrimes within the borders of Nigeria.

REFERENCES

Aina, L. O. (2002). *Research in Information Sciences:* An African Perspective. Ibadan: Stirling-Horden. pp.1-31.

Ali, A.Y. Pocock, K. & Hu, Q. (2014), The effect of board of directors' IT awareness on CIO compensation and firm performance. *Journal on Decision Sciences*, 45(3), 401-436.

Aluko, M. (2004). 17 ways of stopping financial corruption in Nigeria. *www.comcast.net*. April 5, 2010.

Atili, A. (2011) Want! law for tackling cyber crime. *The Nations Newspaper,* pp.41

Bowker, R. (2012) Developments in the global law enforcement of cyber-crime. Policing: *An International Journal of Police Strategies and* Management, 29 (3), 408-433

Brenner, S. (2007). Law in an Era of Smart Technology, Oxford: *Oxford University Press* p.374.

Buzan, F. (1998) *"The Law of Crimes in Nigeria"* (2nd edition) Ahmadu Bello University, Zaria.

Choo, T. (2007) Commonwealth Approach for Developing National Cybersecurity Strategies. Retrieved August 20, 2014 from www.cto.int/priority-areas/cybersecurity/national-cybersecurity-strategies.

Cybercrime Act, (2015) "*The Text Book of Criminal Law*," 2nd ed. Stevens & Sons, London.

Dasuki, E. A. (2011) Why EFCC is losing war on web scam. *Vanguard Newspaper,* pp.34

Fanawopo, S. (2004). FG *moves to enforce cyber crime laws*

Gercke, M. (2006), The slow wake of a global approach against cybercrime. *Computer Law Review International*, 2(2), 141.

Greenwald, S. E. (2014) Combating Cybercrime in Nigeria. *The Electronic Library.* 26(5), 716-725.

Howell, H. & Lind, U. (2009) Customs arrest suspected hacker. The *Vanguard Newspaper*, pp,53

Ifukor, M. O (2006). Cybercrime: a *challenge to information and communication technology* (ICT). Communicate: *Journal of Library and Information Science.* 8(2) 38-49

Juwah, P. (2015) "Fighting Cybercrime in Africa." *Computer Science and Engineering* 2 (6): 98–100.

Kshetri, R. (2010) "Africa: *A New Safe Harbor for Cybercriminals*?" Trend Micro Incorporated Research Paper. www.trendmicro.co.uk/media/misc/africa-new-safe-harbor-for-cybercriminals-en.pdf.

Laver, N. (2005) "Somalia: Media Law in the Absence of a State." *International Journal of Media and Cultural Politics* 8 (2,3): 159–74.

Lawrence, D. (2013). Strategy. Oxford University Press. ISBN 978-0-19-932515-3.

Loader, B. (2000). Cybercrime: law enforcement, security and surveillance in the information age. *Routledge, London*, *J. Soc. Policy* 30(1):300.

Maat, S. (2004). Cybercrime: A Comparative Law Analysis (Doctoral thesis), University of South Africa, Pretoria, South Africa p.239.

Macharia, J. (2014). "Africa Needs a Cybersecurity Law but AU's Proposal Is Flawed, Advocates Say." http://techpresident.com/news/wegov/24712/ *africa-union-cybersecurity-law-flawed*.

Maitanmi, O. S. (2013), Impact of Cyber Crimes on Nigerian Economy, *The International Journal of Engineering and Science* (IJES, vol. vol 2(4), 4551.

Mintzberg, D., Henry, K., Quinn, F. & James, B. (1996). The Strategy Process: Concepts, Contexts, Cases. Prentice Hall. ISBN 978-0-132-340304.

Moore, H. (2005) Examining factors that influence a Youth's potential to become a Victim of Online Harassment, *International Journal of Cyber criminology* Vol 4 Iss 1and2, p 685–698 Online available from <http://www.cybercrimejournal.com/ mooreetal2010ijcc.

NIGF, (2013) Cyber-crimes and the boundaries of domestic legal responses: Case for an Inclusionary Framework for Africa. *Journal of Information, Law and Technology* (JILT), 1, 1-18.

Odunfa, A. (2014), Nigeria: *Report on Cyber Threat Calls for Quick Passage of Bill*. Available from: http://www.allafrica.com/ stories/201405080279.Html.

Osho, W. & Onoja, R. (2015) Identification systems: A risk assessment framework. Australian Insitute of Criminology, Australian Government. Canberra: *Trends and Issues in Crime and Criminal Justice.*

Ploch, L. (2010) "Countering Terrorism in East Africa: The U.S. Response." *CRS Report for Congress, Congressional Research Service*.

Simandan, D. (2017) Competition, contingency, and destabilization in urban assemblages and actor-networks. Urban Geography, pp.1-12. *https://doi.org/ 10.1080/02723638.2017. 1382307*

Simandan, D. (2018) Iterative lagged asymmetric responses in strategic management and long-range planning. Time & Society, Online First, *https://doi.org/10.1177/ 0961463X17752652*.

Steffani, M. (2006) Cyber Security Analysis of Turkey. *International Journal of Information Security Science*, 1(4), 112-125.

Stremlau, G. & Osman, W. (2015) The Privacy Privilege: Law Enforcement, Technology and the Constitution, 7 *journal of technology law &p olicy*

Teseema, D., & Socters, T. P. (2006) Cronan & Jones TW (1998) Modeling IT Ethics: A Study in Situational Ethics.MIS Quarterly 22(1): 31-60.

Wada, T. Longe D. A. & Paul, S. Danquah. O. R. (2012) Action speaks louder than words – understanding cyber criminal behavior using criminological theories. *Journal of internet banking and commerce, April 2012, vol.17, no.1*.

Waziri F (2009). Antigraft campaign: The war, the worries. The Punch, 1st March 2009, p.1.

Weaver, C. (1998) *"Principles of Cybercrime*" (2nd edition), Cambridge University Press, United Kingdom.

Weaver, c. (2004) *"Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement"* https://www.fas.org/sgp/crs/.../R4257.pdf