Assessment of Cybercrime and Nigeria's National Security: A Study of Selected Ministerial Departments and Security Agencies in Nigeria

[1]OGAH, M. A. Ph.D and [2]ALIYU, T. S.

[1]Department of Political Science, Federal University, Lafia, Nasarawa State, Nigeria.
[2]Department of Political Science, Nasarawa State University, Keffi, Nasarawa State, Nigeria.
Email: musaogahari@gmail.com & aliyutala@gmail.com

Abstract

The contribution of internet to the development of the nation has been marred by the evolution of new waves of crime. The internet has also become an environment where the most lucrative and safest crime thrives, thereby posing threat to national security. This study assessed Cybercrime and Nigeria's National Security (2004-2019): A Study of Selected Ministerial Departments and Security Agencies in Nigeria. The differential association theory was adopted as a theoretical framework. This theory explains the social effect of crime and criminality. Quantitative and qualitative methods which relied on both secondary and primary sources of data were utilized. The study revealed that unemployment, growing poverty levels, unethical behaviors, peer group influence, corruption and weak security infrastructures account for the emergence of cybercrime in Nigeria. The study also found that, cyber insecurity has economic, financial, social, security and political impacts on the national security of Nigeria and Nigerians Based on the findings, the study strongly recommended that, government needs to consider massive employment generation as an issue of major focus in the national development and economic growth plan. To tackle poverty in the country, the government needs to formulate and implement programs that will directly benefit the poor, by restructuring sources of Nigeria's gross domestic product to significantly include variety of industries that are labour intensive, such as agriculture and industrialization. This will lead to the diversification of the country's sources of revenue, thereby reducing its overdependence on oil revenue.

Keywords: Cybercrime, Insecurity, National Security and Nigeria

Introduction

The increasing wave of global interconnectivity and technology has made the case for national security in virtually all countries to become a persistently disturbing one particularly in the wake of new forms of cyber security threats. According to a UN report in 2011, over 2.3 billion people, which are equivalent of one third of the world total population, had access to the internet. Surprisingly, from the above estimated figures, over

60% of those internet users came from developing countries (United Nations Office on Drug Crime, 2013).

Nigeria on its part launched the National Security Strategy and equally enacted the Cybercrime Act, 2015 as well as other policy initiatives. But in spite of this, cybercrimes have continued to increase within the Nigerian space (Bello, 2014). According to World Bank survey of 2011, out of the top ten countries in the world with a high level of cybercrime prevalence, Africa hosts four of these countries (Nigeria, Cameroon, Ghana and South Africa).

In another related study, the top five hotspots for cybercrime are; first, the Russian Federation followed by People's Republic of China, Brazil, Nigeria and Vietnam (Mitch, 2015). Also, the 2010 Internet Crime Complaint Center Report ranked Nigeria third in the hierarchy of nations with the highest prevalence of cybercrime (IC3 Report, 2010). Hence, Nigeria is considered one of the major hubs of cybercrime in the World. Cyber-terrorists, spies, hackers and fraudsters are increasingly motivated to target Information Communication Technology (ICT) infrastructure in Nigeria due to the increasing value of information held within it and the perceived lower risk of detection and arrest in conducting cybercrime as compared to more traditional crime.

Yedaly (2016) stated in a Symantec study of Nigeria cyber security that, overall national cyber security efforts in Nigeria are led by the National Security Adviser. Other major stakeholders include government institutions as well as private sector companies. The Government of Nigeria provides strategic direction in terms of overall cyber security policy. Nigeria has established policies for investigating cyber incidences including a number of cybercrime laws, a national cyber security strategy and various policies. The Nigerian government operates a CERT with national-level responsibilities, called the Nigerian Computer Emergency Response Team (ngCERT). The ngCERT is housed in the Office of the National Security Adviser and its primary mission is to manage the risks of cyber threats in the Nigeria's cyberspace and effectively coordinate incident response and mitigate strategies to proactively prevent cyber-attacks against Nigeria (Yedaly, 2016).

Literatures in Nigeria have rarely considered the dangers of cybercrime, a new wave of crime which is damaging and drilling holes in the economy of the nation as much as it is leading to the erosion of confidence in genuine Nigerian commercial credibility, thereby impinging on Nigeria's national security. The contribution of internet to the development of the nation has been marred by the evolution of new waves of crime. The internet has also become an environment where the most lucrative and safest crime thrives. Cybercrime has become a global threat from Europe to America, Africa to Asia. Cybercrime has come as a surprise and a strange phenomenon that now lives with us in Nigeria. With each passing day, we witness more and more alarming cases of cybercrimes in Nigeria, with each new case more shocking than the one before. Cybercrimes have implication on safety of bank accounts and growth of small scale enterprises.

Literatures have often focused on various forms of crimes ranging from examination malpractices, falsification of admission, rape, robbery and stealing, sexual abuse, assault, cultism amongst others. A few literatures have considered the dangers of cybercrime as a new form of crime, which is denting and drilling holes in the economy of nations as much as it is leading to the erosion of confidence in genuine Nigerian commercial credibility therefore impinging on Nigeria's national security. Therefore, this study is carried out with the intension of identifying the remote causes of cyber insecurity, its effects on national security within the Nigerian space; it is also aimed at proffering solutions to such issues for the sake of national security and development.

Research Questions

Sequel to the foregoing background and the problem therein as discovered, the study is guided by the following questions:

i. What are the factors that have accounted for cyber insecurity in Nigeria?
ii. What are the effects of cybercrime on Nigeria's national security?
iii. What are the measures taken by Nigerian government against cybercrime?

Conceptual Clarification

Cybercrime

The meaning of Cyber insecurity otherwise referred to as cybercrime has evolved experientially and differs depending on the perception of both protectors and victims. To support the above, Yar (2005) argued that the lack of a consistent and statutory definition of the activities that may constitute cybercrime make it difficult to analyze it. In spite of this perception on the cybercrime definition, the Council of Europe has defined it as any criminal offence against or with help of computer network (United Nations Office on Drug Crime, 2013).

Sarrab, Aldabbas and Elbasir, (2013); Broadhurst (2006) and Douglas and Loader (2000) shared a similar view on cybercrime, defining it as computer-mediated activities which are illegal or considered illicit by certain parties and which can be conducted through global electronic networks. Other authors define cybercrime as unauthorized entry into a computer system with the motive to delete, modify or damage of computer data. These diverse definitions imply that cybercrime is a complex type of crime since it has various forms and motives.

Thus operationally, this study considers cybercrime to be crimes committed on the internet using a computer device as either a tool or a targeted victim. It encompasses all illegal activities perpetrated by one or more people referred to as scammers, hackers, internet fraudsters, cyber citizens or 419ners, using the internet through the medium of networked computers, telephones and other information and communications technology (ICT) equipment. Cybercrimes target laptops, tablets, mobile phones and entire networks.

National Security

National security has been defined from the prism of physical security and political security: physical security is associated with the military capacity of a state to manage physical threats, it involves the capacity of a state to mobilize military forces to protect its borders, successfully wade off aggression or threat to peace by non-state actors such as terrorist groups. National security has also been defined from the non-military threat perspective to include other threats to the human life such as natural phenomenon like climate change, environmental and health issues (Booth, 2007; Buzan, 1983).

Similarly, Prabhakaran (2008, p.521) as cited in Dan and Dauda (2010) defines national security as:

> The measurable state of the capability of a nation to overcome the multi-dimensional threats to the apparent well-being of its people and its survival as a nation-state at any given time, by balancing all instruments of state policy through governance, that can be indexed by computation, empirically or otherwise, and is extendable to global security by variables external to it.

National security is the ideal condition of a state, that is, the situation of being secured. Security means freedom from danger or anxiety. Security therefore is the state of being secure or means deployed to actualize it, it is not only about providing protection to the individual, physical environment, core values of a nation or other forms of national interest, but also the advancement of the quality of lives of the citizens of a country.

Theoretical Framework

This study is rooted in the theory of Differential Association. The theory of Differential Association was propounded by Edwin Sutherland in 1939. The central thesis of the Differential Association theory proposes that through interaction with others, individuals learn the values, attitudes, techniques and motives for criminal behaviour. According to Sutherland (1939), criminal behaviour is learned through interaction with other persons in a process of communication. This would mean an individual is influenced to participate in criminal behaviour through watching and interacting with other individuals who are engaging in the criminal behaviour.

The theory of Differential Association asserts that, a person becomes delinquent because of an “excess” of definitions favourable to violation of law, over definitions unfavourable to violation of law. What this means is that, an individual will become a criminal because they are exposed to more persons that are favourable to criminal behaviour. That is when one is exposed to more criminal influences rather than more favourable legal influences.

However, Watson (2008) argues that national security is the ability to preserve a nation's physical integrity and territory; to maintain its economic relations with the rest of the world on reasonable terms; to preserve its nature, institution, and governance from disruption from outside; and to control its borders. In relation to Differential Association theory, criminal behaviour emerges when one is exposed to more social message favouring misconduct than pro positive social messages. This can be seen in environments with poor socio-economic conditions such as Nigeria, which may encourage negative views towards the law and authority. The internet and social media can provide such an environment to corrupt the minds of some users, who can as well be tutored online on the basis of hacking or phishing for fraudulent financial gains. A good example is the "yahoo yahoo boys" in Nigeria. A more recent example is that of Raymond Abass, known as Hushpuppi, found to have been engaging in cybercrime with 1,926,400 international victims (Dubai Police, www.guardian.ng). Most of these folks got the negative attributes from associating with other morally corrupt hackers/scammers online. All these constitute threats to the sovereignty of Nigeria and Nigeria's national security in general.

The theory is very relevant as it has successfully and empirically demonstrated that a nation needs to increase it definitions for crime by campaigning rigorously against cybercrime with the hope that the awareness being raised will form excess opinions as against the criminal minded persuasions that will sway the rational decisions of citizens to be law keepers instead of becoming law breakers by associating with their folks.

Methodology

The study area is Abuja, the Federal Capital Territory of Nigeria. The basis for choosing Abuja is that it houses most of the ministries and security agencies that constitute the targeted population of the study. The study adopted both primary and secondary methods. The instruments for data collection was questionnaires, interview and information from extant literature. Survey research design was chosen. The Population of the study was one thousand, three hundred and forty-one (1,341). The selected ministerial departments and security agencies in Nigeria for this study work are Department of Crime Investigation, Nigeria Police Force Headquarters with 260, Office of the Executive Secretary Technical Services, Nigerian Communication Commission (NCC) with 230, Department of Information and Overseas Communication, Ministry of Foreign Affairs with 210, Department of Cyber security, National Information Technology Development Agency (NITDA) with 280 and Professional Cyber Security Expert from Cyber Security Expert Association of Nigeria (CSEAN) with 361. Aside this population, nine (9) respondents who were senior staff of the selected ministerial departments and security agencies and were part of the sampled respondents, were purposively selected for interview to supplement and elaborate views gotten from questionnaire to assess thoughts, opinions and feelings about the cybercrime and Nigeria national security. The reason for this cross section was that the department in the institutions are not only key bodies when it comes to the topic of study, but that they can provide useful insight on the issues regarding Nigeria's continuous cyber insecurity.

The importance of sampling is to reduce the population under study to a manageable size and to meet up with the stipulated study period. In determining the sampling technique used, the study took into cognizance the technical nature of the investigation as it required the response of the population with adequate and relative knowledge on the subject matter. To achieve this, judgmental sampling techniques was employed. However, in selecting the sample size, the study adopted the determination formulas in social sciences as proposed by Yamane (1967) to arrive at 400 sample size. Out of four hundred (400) questionnaires distributed, three hundred and eight-five (385) were retrieved. Therefore, the following analysis was based on the 385 retrieved.

Results of the Findings

Factors Causing Cyber Insecurity in Nigeria

The findings of the study are presented in Table 1. The Table shows that 93.7% of the respondents agreed that unemployment is a causal factor of cybercrime in Nigeria; 3.7% were undecided whether unemployment is a causal factor of cybercrime in Nigeria while 2.5% disagreed that unemployment is a causal factor of cybercrime in Nigeria.

Table 1: Perceived Causes of Cybercrime in Nigeria

Views	Agreed	Undecided	Disagreed	Total
Unemployment	372 (93.7%)	8 (3.7%)	5 (2.5%)	385 (100%)
Poverty	344 (86.5%)	13 (5.0%)	28 (8.5%)	385(100%)
Peer group influence	345 (86.2 %)	33 (10.2 %)	7 (3.5%)	385(100%)
Defective socialization	255 (66.2%)	84 (22.2%)	46 (11.5%)	385(100%)
Weak laws	287 (74.2%)	30 (9.5%)	68 (16.2%)	385(100%)
Corruption	348 (91.0%)	23 (5.7%)	14(3.2%)	385(100%)
Easy accessibility to internet	302 (75.5%)	13 (7.5%)	70 (17.0%)	385(100%)

Source: Field Survey (2019)

The study findings reveal that 86.5% of the respondents were of the view that poverty is a major cause of cybercrime in Nigeria; 5.0% were undecided on whether poverty is a major cause of cybercrime in Nigeria while 8.5% disagreed that poverty is a major cause of cybercrime in Nigeria.

86.2% of the respondents argued that peer group influence is the cause of cybercrime in Nigeria; 10.2% were undecided whether peer group influence is a major cause of cybercrime in Nigeria while 3.5% disagreed that peer group influence is the cause of cybercrime in Nigeria.

66.2% of the respondents agreed that defective socialization is a cause of cybercrime in Nigeria; 22.2% were undecided whether defective socialization is a cause of cybercrime in Nigeria while 11.5% disagreed that defective socialization is a cause of cybercrime in Nigeria.

74.2% of the respondents agreed that weak laws are responsible for cybercrime in Nigeria; 9.5% were undecided whether weak laws are responsible for cybercrime in Nigeria while 16.2% disagreed that weak laws are responsible for cybercrime in Nigeria.

91.0% of the respondents agreed that corruption is the cause of cybercrime in Nigeria: 5.7% were undecided whether corruption is the cause of cybercrime in Nigeria while 3.2% disagreed that corruption is the cause of cybercrime in Nigeria.

Lastly, 75.5% of the respondents agreed that easy accessibility to internet is the factor responsible for cybercrime in Nigeria; 7.5% were undecided whether accessibility to internet is the factor responsible for cybercrime in Nigeria while 17.0% disagreed that easy accessibility to internet is the factor responsible for cybercrime in Nigeria.

Question one: Causes of cybercrime in Nigeria?

In a separate reaction, a Cyber criminal who answered unanimously in this interview (2019) stated that unemployment and poverty are the major factors responsible for the emergence of cybercrime in Nigeria. Most Nigeria youths who engaged in cybercrimes are graduates, unemployed and poor. This is a function of corruption in Nigeria. In order for them to sustain themselves, they became compelled to engage in cybercrime in deceptive manners. Besides, we don't see it as crime. We are taking back what the government stole and fail to provide us with. (Unanimous Software Pirate, interviewed 10th July, 2019).

Jonik Ephraim in this Interview (2019) stated that although there is variation in the causes of cybercrimes but the study consider inadequate legislation, high financial benefits, relative ease/low costs of executing cybercrime, low probability of being caught and prosecuted due to weak laws and weak law enforcement mechanisms. Also, I believe the level of stigmatization of cyber criminals unlike other crimes has not been enough to deter them from committing the crime (Jonik Ephraim, Cybercafé operator, Interviewed 16th June, 2019).

Effects of Cybercrime on Nigeria's National Security

The results in Table 2 reveal that 92% of the respondents were of the view that cybercrime all tarnish the country's reputation internationally. On the other hand, 90% of the respondents, believed that lack of trust and confidence is definitely hindering profitable transactions. 85.5% of respondents argued that Denial of innocent Nigerians of opportunity abroad is another impact. Whereas Inimical to Progress/development had 68.7% impact, loss of employment had 57.7% impact, Loss of Life had 57.5%, Loss of Revenue had 55.3% impact on the National security of the Nigerian state.

Table 2: Effects of Cybercrime on Nigeria's National Security

Views	**Yes**	**No**	**Total**
Tarnishing the country's reputation	348 (92.0%)	37 (8.0%%)	385 (100%)
Lack of trust and confidence, hinders profitable transaction	350 (90.0%)	35 (10.0%)	385(100%)
Denial of innocent Nigerians opportunities abroad	342 (85.5 %)	43 (14.5 %)	385(100%)
Inimical to the progress & development of the country	265 (68.7%)	120 (31.3%)	385(100%)
Loss of employment	221 (57.7%)	164 (42.3%)	385(100%)
Loss of lives	230 (57.5%)	155 (42.5%)	385(100%)
Loss of revenue	211 (55.3%)	174 (44.7%)	385(100%)

Source: Field Survey (2019)

Question 2: What Other Negative National Security Impacts do Cybercrime holds for Nigeria?

In-depth interviews revealed other negative cybercrime impacts on Nigeria. According to Vincent Olagunju and Eze Chibuzo Johnson in this interview (2019), the issue of Cybercrime creates a bad image for Nigeria and this has also earned Nigeria her present ranking by the Transparency International as one of the most corrupt nations on earth.

Similarly, cyber insecurity will naturally repel foreigners or foreign assistance due to the fact that since most of the attacks are carried out remotely and electronically- attacking a foreigner's data base, according to the interviewees, will be worse than physical attacks. There has been publicity of cybercrime cases particularly the yahoo-yahoo case and the fraudulent mails coming from Nigerian Servers to foreigners, when discovered it is not particularly attracting foreigners to Nigerians.

Government Measures Against Cybercrimes

From Table 3, 50% of the respondents considered current control measures as effective, 3% argued that they are very effective. The other 36% considered the measures as less effective, 7% said they are not effective, whereas, 4% remained undecided.

Table 3: Measures used by Government against cybercrime in Nigeria

Responses	**Percentage**
Very Effective	3%
Effective	50%
Less Effective	36%
Not Effective	7%
Undecided	4%
Total	100%

Source: Field Work, 2019.

The statistics seem to be at tangent with the findings on the prevalence rate, with the prevalence rate pointing to inadequacies on the current preventive measures. Interestingly though, most of the interviewees indicated that the current control measures are not very effective and they admitted that it will be difficult to outwit the cyber criminals.

Question 3: What are best approach to address the cybercrime issue in Nigeria?

Adejube Olayinka reacted to this question that we need to have the right legislative environment to allow police and the courts bring criminals to justice whether in the cyber or physical world. Presently, Nigeria is obviously struggling with basic policing as criminals are moving freely online and worsening the levels of cyber-attacks. We need to have dedicated units or cyber commands so as to speak to our police and military in order to ensure our officers and men understand the threat and then prepare to respond. Other initiatives that can work, according to Olayinka revolve around education, mobilization and sensitization, establishment of programs and IT forums for Nigerian youths, Cyber Ethics and Cyber Legislations/Laws.

Similarly, Aminu Lawal and Abdul-Hakeem Ajijola in separate interviews (2019) had asserted that more effective management of risks associated with cybercrime requires collaboration among government, the private sector and civil society organizations. He noted that Ministries, Departments, Agencies as well as private bodies must start taking steps to fight cybercrime within them and government on its side must take steps to review the Evidence Act so that electronic evidence could be accepted in court.

Nigeria became the fifth country in Africa and the first in West Africa to enact a cybercrime law but other grey areas like the evidence act must be addressed as well. Although, the inauguration of the Cybercrime Advisory Council is pivotal and will provide the platform and opportunity for all stakeholders to collaborate and exchange ideas on an issue that affects all sectors in the economy. However, experts in public and private sectors should bring in their experiences to discharge their responsibility to ensure a more secure cyberspace in the country (Aminu Lawwal, Abdul-Hakeem Ajijola, Department of Cyber security, National Information Technology Development Agency (NITDA) interviewed 13 and 15 July, 2019).

Basically, topmost issues that should be addressed by the program should include: Social Engineering averting, detection of phishing scams, Email hygiene, internet usage best practices and password hygiene. In the same way, there is need for continuous monitoring. Organizational best practices conducting continuous monitoring on all critical systems - standards such as NIST identify a three-tiered impact system (low, moderate and high Impact) to use when implementing monitoring policies. Continuous monitoring does not imply true, real-time 24 x 7, nonstop monitoring and reporting. Instead, it means implementing monitoring and oversight processes that provide a clear understanding of security state at any given point in time (Bolanle Omotosho, Cyber security specialist/ consultant, 2019).

Question 4: Measures put in place by the Nigerian government to address cyber security issues?

According to Onajite Regha, some of the most popular measures came inform of the initiative to develop the Cybercrime Act 2015. The Act is made up of 59 Sections, 8 Parts; and 2 Schedules. The very 1st Schedule lists the Cybercrime Advisory Council, while the 2nd Schedule lists the businesses to be levied for the purpose of the Cyber Security Fund under S.44(2)(a) GSM service providers and all telecom companies; Internet service providers, banks and other financial institutions, insurance companies and Nigerian Stock Exchange. Secondly is the initiative of drawing up the Nigeria Criminal Code Act 1990 to fight cyber-attacks. The act declares as a crime any type of stealing of funds in whatever form, and makes it punishable under the Act. Although cybercrime is not explicitly mentioned in the Act, it is a type of stealing punishable under the criminal code. The most distinguished stipulation of the Act is Chapter 38, which deals with obtaining Property by false pretenses- dishonesty. The specific provisions relating to cybercrime is section 419, while section 418 gave a definition of what constitutes an offence under the Act.

Similarly, Collins Onuegbu in another interview (2019) relieved that the Corrupt Practices and Other Related Offences Act (ICPC ACT) also came as a virulent tool that could be explored in the battle against cyber insecurity. The mandate on ICPC was established under the ICPC Act with specific task to enforce anti-corruption laws, Cap C31 of the Corrupt Practices and Other Related Offences Act, Laws of the Federation of Nigeria 2004 established the Independent Corrupt Practices Commission (ICPC), which is one of the major anti-corruption agencies in Nigeria. The Act in general forbids the various perceived acts of corrupt practices arising from communications or transactions involving public/government officers and the public or private individuals. Also other legal instruments that were equally vital in the government's initiative to stamp out cybercrime included; part 2 and Part IV of the Economic and Financial Crimes Commission Act 2004 (EFCC ACT) as amended likewise listed offences that in many ways surrounded on the fight against cybercrime but like the ICPC act it did not deal with cyber challenge directly.

Discussion of Findings

i. The study discovered that, unemployment, growing poverty levels, unethical behaviours, peer group influence, corruption and weak security infrastructures account for the emergence of cybercrime in Nigeria.

ii. Cyber insecurity has economic, financial, social, security and political impacts on the national security of Nigeria and Nigerians. Such effects include: loss of intellectual property, direct financial loss from cybercrime, loss of sensitive business information (such as negotiating strategies), stock market manipulation, service disruptions, reputational damage to hacked companies, reduced trust online, military security problems and internet stalking, harassment as well as bad national image.

iii. There appears to be existing government measures against cybercrimes. However, the study found that, beside the 2015 Cyber security Act, every other laws plays just a supporting role and therefore not sufficient since there had no direct bearing with dealing with the issue of the cyber insecurity. There have always been multiple suggestions to improve cyber security in Nigeria but the government appears to favour short term measures that guarantee temporal solutions.

Conclusion

The study attempted to establish the nexus between cybercrime and national security in Nigeria from the critical information/data security perspective. While one can blame human and material losses in Nigeria to other forms of crimes, the stark reality is that, cybercriminals in Nigeria are perpetuating cyber acts that are not only imposing dangerous international and psychological consequences on law abiding Nigerians residing abroad, but also affecting the wellbeing and safety of the generality of Nigerians wherever they may reside.

As noted earlier, cybercrime has negative impact on the economy as well as the image of the country. With the increase in use and dependence on technologies, there is a high risk posed by cybercriminals. Thus, there is need for a holistic approach to combat this crime in all ramifications. A careful appraisal of the nature, causes, already taken measures and impacts of cybercrime, one will understand that there will always be new and unexpected challenges. To stay ahead of cyber criminals and cyber terrorists, anti-cybercrime approaches must be based on partnership and collaboration by both individuals and government. There is much we can do to ensure a safe, secure and trust worth computing environment. It is crucial not only to our national sense of wellbeing, but also, to Nigeria's national security. The perpetrators of cybercrime are not far- fetched, they are our brothers, friends, colleagues, distant relatives and neighbours who can be tamed under appropriate circumstances with the right strategies.

Recommendations

Based on the findings, this study has come out with the following recommendations:

i. That government needs to consider massive employment generation as an issue of major focus in the national development and economic growth plan. To tackle poverty in the country, the government needs to formulate and implement programs that will directly benefit the poor, by restructuring sources of Nigeria's gross domestic product to significantly include variety of industries that are labour intensive, such as agriculture and industrialization. This will lead to the diversification of the country's sources of revenue, thereby reducing its overdependence on oil revenue.

ii. There is the need for the right legislative environment to allow police and the courts bring criminals to justice whether in cyber or physical world. Presently, Nigeria is obviously struggling with basic policing as criminals are moving freely online and worsening the levels of cyber attacks. Nigeria needs to have dedicated units or cyber commands so to speak in our police and military in order to ensure our officers and men understand the threat and then prepare to respond. Other initiatives that could work revolve around education, establishment of programs & IT forums for Nigerian youths, Cyber Ethics and Cyber Legislations/Laws. Sensitization should be carried out also to bring to the fore the far-reaching consequences of these malicious actions. These will help in eliminating cybercrime thereby overcoming its effects on Nigeria's national security.

iii. The laws in existence should be implemented vigorously. More focus should be placed on enhancing forensic analysis so that prosecution is swift and accurate.

References

Bello, F. (2014). Public Policy Implication on National Security: available at http://www.nialsnigeria.org/journals/fatima.bellolaw.pdf,

Booth, K. (2007). *Theory of World Security,* Cambridge: Cambridge University Press.

Broadhurst, R. (2006). Developments in the Global Law Enforcement of Cybercrime

Policing: *An International Journal of Police Strategies and Management.* pp. 408-433.

Buzan, B. (1983). The National Security Problem in International Relations. *Copenhagen School of Security Studies: International Journal,* 40(4);756-758 available at en.m.wikipedia.org

Dan, E.S. & Dauda, S.G. (2010). Trans-Border Economic Crime, Illegal Oil Bunkering and Economic Reforms in Nigeria, *Policy Brief Series*, No. 15, Octber 2010.

Douglas, T. & Loader, B. D. (2000). *Cybercrime: Security and Surveillance in the Information Age,* UK: Routledge. Dubai Police, www.guardian.ng

International Crime Complaint Center (IC3). (2010). 2010 Internet Crime Report: New York. Available at www.ic3.gov

Mitch, G. (2015). Army to Establish Unified Cyber Corps: The Times of Israel.

Sarrab, M., Aldabbas, H. & Elbasir, M. (2013). *Challenges of Computer Crime*

Investigation in North Africa's Countries. The International Arab Conference on Information Technology (AaCIT'2013).

Sutherland, E. (1939). Principles of Criminology. Fourth edition: Chicago. Alta Mira Press.

UNCTAD. (2015). Information economy report 2015: Unlocking the potential of e-commerce for developing countries. New York and Geneva: United Nations Publication.

United Nations Office on Drug Crime (2011). Comprehensive study on Cybercrime: United Nations Publication.

Wada, F., and Odulaja, G. O. (2012). Assessing Cyber Crime and its Impact on E-Banking in Nigeria Using Social Theories. *African Journal of Computing & ICT,* 5; 69-82.

World Bank (2011). Global Cyber Security Program: World Bank Group. Washington DC.

Available at http://countrysurveys.worldbank.com

Yedaly, M., Yankey, A. K., Wright, B. & Nahorney, B. (2016). *Cybercrime and Cyber*

security trends in Africa. Published November, 2016. Symantec Corporation World Headquarters350 Ellis Street Mountain View, CA 94043 USA+1 (650) 527 8000 1 (800) 721 3934.

Yamane, T. (1967). *Statistics: An Introductory Analysis*, 2nd edition, New York: Harper and Row

Yar, M. (2005). The Novelty of Cybercrime: An Assessment in Light of Routine Activity

Theory. *European Journal of Criminology*, 2(4); 407-427.