CYBER THREATS AND NATIONAL SECURITY IN NIGERIA: CHALLENGES AND OPTIONS

Captain (NN) Idowu Bobade Yusuf, ndc, FSS, MSS, psc, MNSE, M.Tech

INTRODUCTION

During the Cold War, the global security structure was static and bipolar, pitting the United States of America (USA) and its democratic allies against the Soviet Union and its communist allies (Kugler, R.L. 2009:321). The Cold War continued till the fall of Berlin Wall in 1990. Since then, the security paradigm has shifted significantly (Cleary and McConville, 2006:3). The challenges to global security increased and state entities were forced to take sides with the superpowers. Eventually, the end of the Cold War changed alliances and geopolitical dynamics of international relations, thus increasing regional insecurity. The changes, coupled with the proliferation of Information Technology (IT), made high technology and information system elements more readily available to many countries and organizations around the world. The advent of IT also paved way for other security challenges, particularly in cyberspace. The information revolution transformed not only the way society functions, but also the way war is conducted giving rise to a new type of conflict that takes place in cyberspace (Liaropoulos, 2011:para.1). Information warfare is now considered within the context of war in general (Erbschloe, 2001:1-3). Militaries and terrorist groups now have the capability to launch cyber attacks against military networks and critical infrastructures that depend on computer networks. This is a serious challenge for national security.

National security deals with safeguarding a nation's existence and defending its vital interests. The main objective of national security is existence (Tal, 2000:3). This means that physical survival constitutes an objective and primary value that all nations hold in common. Unlike the old generic notion of national security, which focused on countering imminent, catastrophic threats from a specific nation-state, this new concept is different. Today, cyber threat is one of the most serious economic and national security challenges that nations face. Cyber threats have become a national security priority in several western countries (Lemieux, 2011:1). In Europe, the cyber attacks in Estonia from April - May 2007 and Georgia (Eurasia) in August 2008 confirm that conflict spectrum has expanded and includes cyberspace as well (Blank, 2008:227-230). The cyber attacks in these places surely had negative consequences on the countries' national securities. In North America (particularly in the US), banks have spent millions of dollars responding to cyber attacks against American Financial Institutions. Officials from the affected banks are urging the US government to help mitigate the cyber attacks (Wall Street Journal, 2013 online).

In Africa, for more than a decade, Information and Communications Technology (ICT) has been attributed a key role in both economic growth and poverty reduction. Considerable improvements have been achieved in various parts of the continent with respect to certain aspects of ICT. These include the spread of mobile telephony and an increasing number of national ICT strategies and regional initiatives. Despite these achievements, cyber threats to national security in Africa have become a source of worry, as there is currently no continental coordination towards cyber security. Since the re-establishment of democracy in Nigeria (1999) and with series of appropriate policies in place, the ICT sector of the economy has seen tremendous improvements. Over the past 10 years however, unscrupulous computer users have perpetrated various crimes through the system.

CONCEPTUAL DIMENSIONS OF CYBER THREATS AND NATIONAL SECURITY

Concept of Cyber Threats

There are many definitions of cyber threats. According to Caitlin Hayden, Spokeswoman for the White House National Security Council, "Cyber Threats cover a wide range of malicious activities that can occur through cyberspace" (Verge, 2013). She wrote that "such threats include website defacement, espionage, theft of intellectual property, denial-of-service (DoS) attacks, and destructive malware". This Researcher examined the White House's definition and pondered on 'Threat' and 'Cyberspace' separately[1]. With the 3 definitions synthesized, this study defines 'Cyber Threats' as a series of malicious activities carried out by an actor, whether organisation or individual, with or without a specific political, social or personal goal, using web-based technology, against a global domain within the information environment framed by the use of electronics and electromagnetic spectrum via interdependent and interconnected networks. This definition covers cyber threats, cyber environment, actors and their motivation as well as possible consequences on national security. The formulated definition is therefore adopted as the working definition for this study.

Concept of National Security

National security is also difficult to define precisely, but almost every state acts in ways that reflect its view of what constitutes national security. Another issue in national security has been whether and where to place boundaries on the concept.

[1] Dungan et al (2007:10) define 'Threat' as "a malevolent actor, whether organization or individual, with a specific political, social, or personal goal and some level of capability and intention to oppose an established government, a private organization, or an accepted social norm". Kuehl (2009:28) views 'Cyberspace' as a "global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information communication technology".

Alberts and Papp (2000:10), state that: National security refers to the protection of a state, its territories, and its peoples from physical assault by an external force, as well as the protection of important state economic, political, military, social, cultural, and valuative interests from attacks emanating from foreign or domestic sources which may undermine, erode, or eliminate these interests, thereby threatening the survival of the state. Such protection may be pursued by military or nonmilitary means. This definition has a broad perspective incorporating both military and non-military such as human security aspects of national security. It also made provision for potential threats and valuating interests such as cyber threats. Therefore, the researcher agrees with the above definition and adopts it for the study.

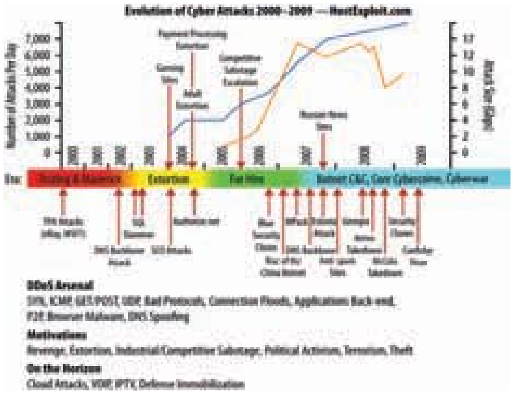
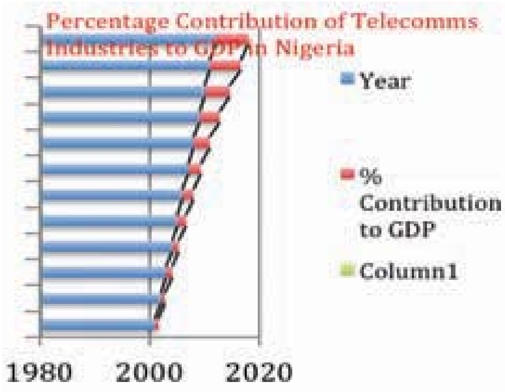
Relationship between Cyber Threats and National Security

National security considers the protection of the nation-state's economic, political, social and cultural tool as well as other interests against internal and external threats, including cyber threats. In Cyberspace, the threat agents can be criminals, hackers, terrorists, and nation-states. When national security measures are high, cyber threats and vulnerabilities will be reduced and conversely, when little security measures are put in place, the chance of success of cyber attackers will be high. It is evident that any threat to the cyberspace of any nation will have a negative impact on its national security. Thus, there is an indirect relationship between Cyber Threats and National Security. Copenhagen School's theory was used as the theoretical framework for the study because it deals with the emergence of new security issues like cyber threats.

AN APPRAISAL OF CYBER THREATS AND NATIONAL SECURITY IN NIGERIA

Cyber threats in Nigeria started in the 1980s as a traditional postal mail scam commonly known as 'advanced fee fraud' (AFF) or '419' (Waziri, 2005:2). However, the evolution of global cyber attacks became prominent from 2000–2009 as shown in Figure 1. Currently, Nigeria ranks tenth among top 10 Internet users in the world and third among the top 10 countries noted for Internet fraud (IC3 Annual Report, 2012 online). In October 2012, Symantec warned that Nigeria's cyber space would become easy target for cyber criminals. This is because despite real incidents of information security breaches, the Nigerian authorities have not appreciated the magnitude of cyber threats and how they can derail an economy (Adote, 2013 online). In Nigeria, the ICT sector contributed 5.83 percent to the country's GDP in 2012 making it the fourth highest contributor (Tribune, 2012 online).

Figure 1: Evolution of Global Cyber Attacks/Percentage Contribution of Telecomms Industries to GDP in Nigeria

	
Source: HostExploit.com, 2013	Source: Nigerian Communications Commission, 2013

Reports from Opera Mini show that 54 percent of Nigeria's Internet users access the Internet through mobile phones (Business Day, 2013 online), while other reports indicate an increase in cybercrime. As the world's dependence on the Internet grows, the disruptive capabilities of cyber attackers pose serious threats to national and international security. A Director of Central Bank of Nigeria (CBN), Mrs Olatokunboh Martins, recalled that a Symantec study had found the annual cost of cyber crimes to be about $150 billion with Nigeria responsible for 6.4 percent of online fraud in the US in 2011 (Oketola, 2012 online).

In 2012, secret agents of the United Parcel Service[2] (UPS) smashed a record scam with a face value of $2.1 billion in Lagos (Hassan, Lass and Makinde, 2012:626). In Nigeria, financial institutions are mostly the targets of cyber attacks because they carry valuable information related to people's identity, assets and financial status. To enhance national security, as the country prepares to enthrone a cashless economy, there is the need to put adequate measures in place to mitigate the cyber threats.

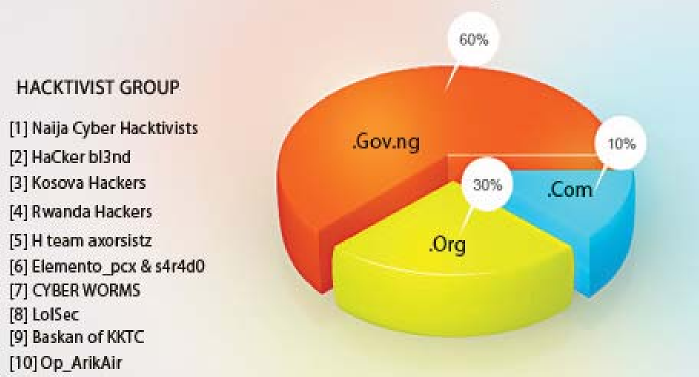
IMPACT OF CYBER THREATS ON NATIONAL SECURITY IN NIGERIA

Cyber attacks on the Federal Government of Nigeria (FGN) could be direct and indirect. Direct attacks on national security could undermine the government by damaging its credibility before its citizens. Adversaries could attack critical government functions or infrastructure to destroy the society directly. These attacks may extend to the military to ridicule and prevent it from performing its constitutional roles. Indirect attacks on government can manipulate

[2] Some of the instruments uncovered by UPS were Wal-Mart money orders, Bank of America cheques, US Postal Service cheques and American Express travellers' cheques.

government information to undermine people's trust in that government. Consequently, FGN must establish effective programmes and processes to counter the effects of both types of attacks. During the field survey for this study, 79.23 percent of respondents agreed that cybercrime is the most prevalent in Nigeria compared with cyber terror and cyber war. Cyber terrorism and cyber war pose little risk to national security of Nigeria for now. According to Centrex Ethical Lab, Figure 2 shows that the number of cases involved with the defacement of government websites in Nigeria has risen from 10 percent in 2010 to 60 percent in 2012 (Business Day, 2013 online). This is a huge increase.

Figure 2: Statistics of Defaced Nigerian Websites from 2010 – 2012



Source: techtelling.com-massive-cyberattacks-hits-internet-users, 2013

A field survey, using questionnaires, based on purposive sampling and non-probabilistic method was carried out during this study in Lagos, Abuja and Dhaka. A total number of 160 questionnaires were distributed through hard and soft copies. Since purposive sampling was used, only relevant respondents were considered necessary. Thereafter, 130 copies were received as in Table 1. The data are then analysed and interpreted to reach the findings.

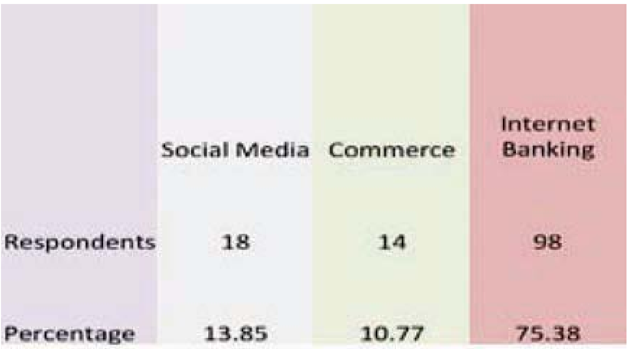
Table 1: Total Number of Questionnaires Distributed and Received

Place	Quest. Distr.	Quest. Rcve.	% Rcvd.
Lagos	70	53	75.71
Abuja	60	49	81.67
Dhaka	30	28	93.33
Total	160	130	81.25

Source: Author, 2013

The Researcher's survey (Table 2) establishes that the most targeted services in Nigeria in order of priority are Internet banking, social media and commerce with 75.38, 13.85 and 10.77 percent respectively. Although no one owns the Internet, 80 percent of it lies in the private sector (The UK Cyber Security Strategy, 2013:5 online). The investigation conducted by Ernest & Young (2013 online) revealed that the cost of cyber crimes to the Nigerian economy in 2012 was around $200 million. This shows that the private sector also plays a key role in cyber security of any nation-state. Thus, both direct and indirect cyber attacks on the FGN are issues of great concern. Cyber attacks on Nigeria's critical infrastructure and the military must be discouraged. DHQ could develop cyber security response plan to cater for cyber attacks in the Armed Forces of Nigeria (AFN).

Table 2: Most Targeted Service in Nigeria



	Social Media	Commerce	Internet Banking
Respondents	18	14	98
Percentage	13.85	10.77	75.38

Source: Author, 2013

CHALLENGES OF COMBATING CYBER THREATS IN ORDER TO ENHANCE NATIONAL SECURITY IN NIGERIA

The assessment of the issues in the fight against cyber threats in Nigeria raised some challenges. These challenges include lack of appropriate regulatory and legislative framework against cyber crimes, national cyber security strategy and national cyber awareness education. Others are inefficient collaboration and international cooperation in tackling cyber threats, and inadequate training of cyber forensic experts.

Lack of Appropriate Regulatory and Legislative Framework Against Cybercrime

Cyberspace is one of the most complex legal frontlines today, not only in Nigeria but also in the entire globe. Criminals use the Internet to perpetrate various crimes ranging from economic fraud, identity theft, money laundering and defamation. The costs associated with cyber attacks are substantial due to lost revenues and inconveniences caused by network inoperability as well as in terms of lives affected by identity theft. According to Symantec research, the value of global cybercrime outweighs the hard drug market with a yearly activity of $288 billion (Financial Intelligence, 2012 online). The cybercrime activities dominant in Nigeria include espionage, Internet hacking, scam, extortion, fraud, impersonation, free ware, Internet hoax, spyware, viruses and worms. Currently, there is no legislation against cybercrime in the country. It is treated like any other crime[3] (Meyer, 2012:15). The dangers posed by cyber criminals, who are not properly punished when apprehended, are on the increase. There is therefore the challenge of appropriate regulatory and legislative framework.

Lack of National Cyber Security Strategy

The absence of appropriate cyber strategy has continued to increase concerns over e-commerce, online safety and financial transactions. A number of services, particularly Internet banking and similar transaction have become targets of cyber criminals with varying degrees of success. As the country integrates electronic payment system into its financial institution; a step that is expected to accelerate e-commerce growth, the negative impact of cybercrime on businesses continues to create fear in the minds of Internet users. Many foreign investors are not comfortable transacting online businesses with Nigerians. These observations bring to fore the challenge created due to lack of national cyber security strategy in Nigeria.

Lack of National Cyber Awareness Education

The increased use of social media and unsupervised child access to the Internet is leading to greater child exploitation according to the Child Exploitation and Online Protection Agency (The UK Cyber Security Strategy, 2013:27). The Agency has reported receiving 1,300 reports of child exploitation on average each month, 263 percent more than 2 years ago (The UK Cyber Security Strategy, 2013:27). The various financial institutions are also not doing enough to sensitize their clients on how to avoid pitfalls in Internet transactions. Since cyber attackers exploit ignorance and lack of awareness in people, the federal, state and local governments have to work together to mitigate such menace. A basic level of awareness for business and home users will go a long way in such enlightenment campaign (South Africa Cyber Threat Barometer, 2012/3; Ahmed, 2013, pers. Comm. 30 August). In Nigeria, the awareness education is low and this is a great challenge that must be addressed.

Inefficient Collaboration and International Cooperation in Tackling Cyber Threats

In Nigeria, there is minimal collaboration of law enforcement agencies. Implementation of cyber initiatives is slow and not yielding desired results. The security outfits expected to work as a team and find a lasting solution to the cyber attacks are pre-occupied with

[3] In 2004, former President of Nigeria, Olusegun Obasanjo (2004), formed a 15-member cybercrime committee made up of representatives from the government and private sectors. The Committee, known as the Nigerian Cybercrime Working Group (NCWG), was to find a solution to the Nigerian Internet-based fraud and cybercrime. The NCWG in addition to accomplishing some of its mandates drafted the Nigerian Computer Security and Protection (NCSP) Bill (Whyte, 2011). The ONSA is currently reviewing the Harmonized Cybersecurity Bill of 2011. The final draft would go to the legislatures for passage into law.

internal strife and inter-agency rivalry. Instead of uniting for a common front to fight cyber warriors, the organisations are busy strategizing to be the lead agency in Nigerian Cybercrime Working Group (NCWG). A number of international organizations have taken steps in pushing toward cyber law in both developing and developed economies[4] (Farhad 2013, pers. Comm., 6 June). The ITU is identified as a leader in this domain; it launched the Global Security Agenda in November 2007, and formed a High-Level Experts Group to look into the issues and develop proposals for long-term strategies to promote cyber security (Shalhoub and Al Qasimi, 2010:18). Nigeria has to key in to this vision and expedite action in carrying out more initiatives both at the national and international levels in order to tackle the challenge. The establishment of Cyber Incident Response Team (CIRT) is relevant in this regard.

Inadequate Training of Cyber Forensic Experts

In many critical sectors of the economy, skilled IT security professionals are lacking and there is insufficient technical training. According to Owolabi (2012:53), only about 37.5 percent of Nigeria's security agencies have ICT policies and where such policies exist, they are not harmonized to achieve synergy. The level of ICT infrastructure in the security agencies is below 40 percent and the level of ICT skills is about 22 percent (Owolabi, 2012:53). Daramola (2013, pers. Comm., 30 August) confirmed that Office of the National Security Adviser (ONSA) and EFCC now have trained cyber forensic experts but they are inadequate. Additionally, digital forensics and investigative skills are in need. In order to sustain the gains made by the NCWG, the FGN in April 2007 established the Directorate of Cyber Security (DCS), in the ONSA with the mandate to spearhead the fight against cyber threats in the country (Aliyu, 2010 cited in Whyte, 2011:27). Ilori[5] (2013, pers. Comm., 30 August) affirmed that no Nigerian university offers Cybersecurity as a major course. Emuekpere[6] (2013, pers. Comm., 15 August) also avowed that cyber security is not even taught in military institutions including the Defence Intelligence School (DIS), Abuja. Only better-equipped and well-trained staff can effectively fight cyber criminals. Inadequate training will lead to a compromise in national security. There is therefore the challenge of inadequate training of cyber forensic experts in Nigeria.

[4] Farhad, a former Director Signal Intelligence Bureau, Directorate General of Forces Intelligence, Dhaka-Bangladesh, made this assertion during a personal interview on 6 June 2013.

[5] Mr Soji Ilori is a Lecturer at Obafemi Awolowo University, Ile-Ife, Nigeria. The Telephone interview was conducted on 30 August 2013 about 1330 hours Nigerian Local Time.

[6] Commodore MA Emuekpere is the current Commandant of Defence Intelligence School, Abuja. The Telephone interview was conducted on 15 August 2013 about 1100 hours Nigerian Local Time.

STRATEGIES TO OVERCOME THE CHALLENGES OF CYBER THREATS IN ORDER TO ENHANCE NATIONAL SECURITY IN NIGERIA

Options of Cyber Strategies for Nigeria

Cyber threats pose serious danger to critical infrastructures, finance, government and telecommunications sectors as well as to individuals and by implication to the national security. Accordingly, nation-states have formulated or reviewed their national cyber security strategies. Examples of such countries include: the UK, India and the SA. The Cyber Security Policy Framework for South Africa is highlighted since the Researcher considers it as the best option for Nigeria:

The Cyber Security Policy Framework for South Africa

The SA Cabinet approved the National Cyber Security Policy Framework in March 2012. The framework outlines policy positions that are intended to address national security threats in terms of cyberspace, combat cyber warfare, cybercrime and other cyber ills (South Africa Cyber Threat Barometer, 2012/3:5). Other outlines include developing, reviewing and updating existing substantive and procedural laws to ensure alignment; and to build confidence and trust in the secure use of ICTs. The policy framework[7] will witness the establishment of relevant cyber institutions and identify specific areas of responsibility by a number of government departments. The State Security Agency is tasked with the overall responsibility and accountability for coordination, development and implementation of cyber security measures in the country, as an integral part of its mandate. Since SA has the largest economy in Africa and the Security Policy Framework is robust, Nigeria could learn from it.

Strategies to Mitigate Cyber Threats in Nigeria

The strategies to overcome the challenges of cyber threats in Nigeria include the provision of cybersecurity legal framework, formulation of a national cyber security strategy and the implementation of national cyber awareness programme. Others are increased collaboration/international cooperation and the establishment of cyber training centres. These strategies are discussed in subsequent paragraphs.

Provision of Cyber Security Legal Framework. Cyber crime cannot be completely eliminated, but can be minimized. One way to do this is to provide cybersecurity legal framework. The Nigerian legislature could enact strict laws regarding cyber criminals and punish them accordingly. Such laws if enacted could detect and deter cyber attacks and

[7] The policy is made up of 6 strategic objectives. These include facilitating the establishment of relevant structures in support of cyber security, ensuring the reduction of cyber security threats and vulnerabilities and fostering cooperation and coordination between government and private sector. Other objectives include promoting and strengthening international cooperation and building capacity on cyber security as well as to promote compliance with appropriate technical and operational cyber security.

promote cyber technology to advance the country's economic and national security interests. Nigeria has no cyber legislation for now, and has not amended its existing laws to reflect the new reality of cybercrime. As a way out, the FGN could task the Ministry of Justice (MOJ) in conjunction with the NASS to review existing laws to cater for cybercrime. The FGN could also prevail on the ONSA to complete the review of the Harmonized Cybersecurity Bill 2011 and create the final draft that would go to the legislature for passage into law latest by September 2014. This will give legal backings to law enforcement agents when prosecuting cyber criminals and enhance national security in Nigeria.

Formulation of a National Cyber Security Strategy. Cyber security in Nigeria is of utmost importance if the country is to minimize economic and financial crimes through cyberspace. A critical constituent of such defence is the formulation of a national cyber security strategy. Thus, Nigeria could articulate such strategy with the objective of tackling cybercrime and protecting national interests in cyberspace. Such strategy could centre on addressing the modus operandi of common attacks and prescribe ways to tackle future incidents. The ONSA could draft the national cyber security strategy by March 2015 in conjunction with the NCWG. The relevant portions of the SA Cyber Security Policy Framework could be adopted. The ONSA could coordinate national response to major cyber incidents and improve on the existing cyber security model. Additionally, the Defence Headquarters (DHQ) could develop a cyber security response plan to cater for any cyber attacks in the military latest by December 2014.

Implementation of National Cyber Awareness Programme. Fighting cyber crime in Nigeria requires a holistic approach by all stakeholders. This therefore underscores the need to create a security awareness culture involving the public, ISPs, cybercafés, government, security agencies and Internet users. The government could create awareness education about the problems, risks and solutions. The FG could introduce cyber education into our universities and other institutions of higher learning as very few, if any, currently undertake such courses in its academic curriculum. The Nigerian media, both electronic and print, could be encouraged to sensitize the populace on the effects and impact of cybercrime on the society. The FGN could organize workshops across the country to increase the awareness of the populace. Such workshops and seminars could commence by January 2014 and aim at the teeming youths, amongst whom cybercrime is prevalent.

Increased Collaboration/International Cooperation. Keeping the Nigerian cyberspace safe for smooth conduct of electronic transaction will require continued collaboration across government, private sector and stakeholder communities. In Nigeria, a holistic model driven by the government and private sectors including law enforcement agencies is needed. The FGN could develop and implement information sharing arrangements and protocols with other security organisations. The government could partner at the national level with the private sector, individuals and non-governmental organisations. Such partnership could serve a national need in support of government efforts. Since cybercrime is borderless, combined efforts with other countries would be important in tackling the menace. Thus, in addition to being a member of International Multilateral Partnership Against Cyber Threats (IMPACT), Nigeria could assent to the Budapest Convention and take part in other multilateral cybercrime initiatives such as Commonwealth Internet Governance Forum (CIGF) and Forum for Incident Response and Security Teams (FIRST). The FGN could consider the establishment of CIRT in the country.

Establishment of Cyber Training Centres. Cybercrime is a serious menace in Nigeria. To adequately counter cyber threats, expertise and specialist skills are required. To achieve these, there is an urgent need to train security agents. Such training must be practical, flexible and credible. The FGN could establish 3 cyber-training centres in Lagos, Abuja and Port Harcourt to address the growing cyber challenges. The government could direct the Ministry of Education to include Cybersecurity in the curriculum of Nigerian tertiary institutions. The relevant sectors of the economy could also be encouraged to train their personnel in cyber security. Training in forensics could be made mandatory for organisations that constitute the NCWG.

RECOMMENDATIONS

To mitigate the impact of cyber threats in order to enhance national security in Nigeria, it is recommended that:

a. The ONSA should expedite action on the current review of the Harmonized Cybersecurity Bill 2011 and create the final draft that would go to the legislature for passage into law to give legal backings to law enforcement agents when prosecuting cyber criminals latest by September 2014.

b. The ONSA in conjunction with the NCWG should draft a national cyber security strategy by March 2015.

c. The ONSA should organize frequent cyber security workshops and seminars across the country to educate the masses about malicious activities in cyberspace with effect from June 2014.

d. The FGN should assent to the Budapest Convention on Cybercrime and establish CIRT in Nigeria by June 2015.

e. The FGN should establish cyber training centres and introduce Cybersecurity as a course workload into Nigerian tertiary institutions with emphasis on research and development by September 2017.

f. The DHQ should formulate a cyber security response plan for the AFN by December 2014 to mitigate cyber-related attacks within the Services.

CONCLUSION

This study set out to examine the impact of cyber threats on national security in Nigeria with a view to suggesting appropriate strategies to effectively combat the menace. An appraisal of cyber threats and national security was undertaken and challenges of combating cyber threats in order to enhance national security in Nigeria were identified. The cyber strategy framework of the RSA was examined before proposing the strategies to overcome the identified challenges. The study established an indirect relationship between cyber threats and national security.

The work revealed that in Nigeria, Internet fraud has not abated due to the booming economy and revolution in the IT sector. Thus, if no adequate measure is put in place, Nigeria's move to enthrone a cashless economy may be jeopardized. It was established that cyber crime is the most prominent of all the cyber threats and cyber criminals mostly target Internet banking compared with social media and commerce. It was proven that there is no appropriate legal framework to address cybercrime in the country. Unless this challenge is tackled, cyber incidents will continue to rise. The study noticed that since financial transactions have become the targets of cyber fraudsters, national cyber security strategy is an issue to be taken seriously.

The identified challenges of combating cyber threats in Nigeria include lack of cyber security legal framework, national cyber security strategy, and national cyber awareness education. Other challenges are inefficient collaboration and international cooperation in tackling cyber threats, and inadequate training of cyber forensic experts. In other to mitigate these challenges, strategies were suggested. The researcher opines that ONSA needs to create the final draft of the Harmonized Cybersecurity Bill 2011 for onward transmission to the NASS for legislation. The formulation of a national cyber security strategy centering on methods of attacks and curbing future incidents is paramount. The ONSA could organize cyber seminars/workshops while the DHQ develops cyber security response plan to cater for cyber attacks in the AFN. Nigeria could accede to the Budapest Convention to demonstrate further commitment to tackle cyber threats in Nigeria. The establishment of CIRT in Nigeria would be a step in the right direction. The FGN could establish cyber training centres and introduce Cybersecurity as a course workload into the nation's tertiary institutions. These strategies could be implemented in short, medium and long-term plans.

BIBLIOGRAPHY

Books

1. Alberts, D.S. & Papp, D.S. 2000, 'National Security in the Information Age: Setting the Stage', in *Volume II of Information Age Anthology: National Security Implications of the Information Age,* eds D.S. Alberts & D.S. Papp, CCRP, Washington D.C., Pp. 1- 55.

2. Cleary, L.R. & McConville T. 2006, 'Commonalities and Constraints in Defence Governance and Management', in *Managing Defence in a Democracy,* eds L.R. Cleary & T. McConville, Routledge, London, Pp. 3-16.

3. Erbschloe, M. 2001, *Information Warfare: How To Survive Cyber Attacks,* Mc Graw-Hill, New York.

4. Imoisili, I.C. (ed), 1996, *Social Research Methods for Nigerian Students,* Malthouse Press Limited, Lagos.

5. Khuel, D.T. 2009, 'From Cyberspace to Cyberpower: Defining the Problem', in *Cyberpower and National Security,* eds F.D. Kramer, S.H. Starr & L.K. Wentz, National Defence University Press, Washington, D.C, Pp. 24-42.

6. Kugler, R.L. 2009, 'Deterrence of Cyber Attacks' in *Cyberpower and National Security,* eds F.D. Kramer, S.H. Starr & L.K. Wentz, National Defence University Press, Washington, D.C, Pp. 309-340.

7. Mustafa, A. 2010, *Research Methodology,* A.I.T.B.S. Publishers, Delhi.

8. Tal, I. (translated by Martin Kett) 2000, *National Security: The Israeli Experience,* Praeger Publishers, Westport.

9. Waziri, F.M, 2005, *Advance Fee Fraud, National Security and the Law,* Bookbuilders, Ibadan.

Periodicals/Journals

10. Blank, S. 2008 'Web War I: Is Europe's First Information War: A New Kind of War?', *Comparative Strategy*, Vol. 27, No.3, Pp. 227-247.

11. Hassan, A,B. Lass F.D. & Makinde, J. 2012, 'Cybercrime in Nigeria: Causes, Effects and the Way Out', *ARPN Journal of Science and Technology,* Vol. 2, No.7, Pp. 626-630.

12. The UK Cyber Security Strategy: Landscape Review, 12 February 2013.

13. The South African Cyber Threat Barometer: A Strategic Public-Private Partnership Initiative to Combat Cybercrime in South Africa, 2012/3.

Official Publications

14. Duggan, D.P. Thomas, S.R. Veitch, C.K.K. & Woodard, L. 2007, *Categorizing Threat: Building and Using A Generic Threat Matrix.* Sandia National Laboratories. Albuquerque, New Mexico.

15. Nigerian Communications Commission 2010, Nigeria Telephone Subscriber Data 1999–2009.

16. Obasanjo, O. 2004, Address delivered by His Excellency at the Inauguration of the Nigerian Cybercrime Working Group, Abuja on 10 March.

Unpublished Materials

17. Aliyu, M. 2011, Assistant Director, Directorate of Cyber Security, Office of the National Security Adviser, Abuja, quoted in Whyte, EG, 'Cyber Threats and National Security in Nigeria: Challenges and Prospects', A Research Project submitted at the National Defence College, Abuja, NDC Course 19, June 2011.

18. Owolabi, A.R. 2012, 'Information and Communications Technology and Terrorism: Challenges and Prospects', A Research Project submitted at the National Defence College, Nigeria, NDC Course 20, June, 2012.

19. Whyte, E.G. 2011 'Cyber Threats and National Security in Nigeria: Challenges and Prospects', A Research Project submitted at the National Defence College, Abuja, NDC Course 19, June, 2011.

Unstructured Interview

20. Ahmed, S.T.U. Deputy Inspector General of Police, Bangladesh Police, Dhaka, personal interview on 30 August 2013.

21. Daramola, I.O. Director Legal Intercept, Office of the National Security Adviser, Presidency, Abuja, telephone interview on 30 August 2013.

22. Emuekpere, M.A. Commandant Defence Intelligence School, Abuja, telephone interview on 15 August 2013.

23. Farhad, S.M. Former Director Signal Intelligence Bureau, Directorate General of Forces Intelligence, Dhaka, personal interview on 6 June 2013.

24. Soji, I. Lecturer, Obafemi Awolowo University, Ile-Ife, Nigeria, telephone interview on 30 August 2013.

Internet/Electronic Media

25. Adote, R. 2013, 'Can Cyber Attacks pose a Threat to National Security', *Guardian Online*, accessed on 22 April 2013 from <http://www.ngrguardiannews.com/index.php?option=com_ content& view= article &id=113905:can-cyber-attacks-pose-a-threat--to-national- security&catid=55: compulife&Item=391>

26. BusinessDay, 2013, 'Internet users to submit personal details to ISPs', accessed on 26 May 2013 from http://businessdaynigeria.com/internet-users-submit-personal-details-isps.

27. Ernest & Young, 2013, quoted in BusinessDay, "Cyberattacks on Government Websites to Rise", accessed on 29 June 2013 from http://businessdaynigeria.com/cyberattacks-government

28. Financial Intelligence, 2012, 'Cashless Nigeria….An Eye On Cybercrime' Online, 19 December 2012, accessed 19 May 2013 from <www.myfinancialintelligence.com/telecoms-and-it/cashless-nigeria-eye-cybercrime /2012-12-12-19>

29. Lemieux, F. 2011, 'Investigating Cyber Security Threats: Exploring National Security and Law Enforcement Perspectives', *Cyber Security Policy and Research Institute Journal,* accessed on 28 March 2013 from http://www.cspri.seas.gwu.edu/Seminar-Abstracts- and-Papers/2011-Investigating- Cyber-Security-Threats-Lemieux.pdf.

30. Liaropoulos, A. 2011, 'Cyber Security and the Law of War: The Legal and Ethical Aspects of Cyber-Conflict, *Greek Politics Specialist Group*. Accessed in 2013 from http://www.academia.edu/612371/Cyber-Security_and_the_Law_of_War_The_ Legal_and_Ethical_Aspects_of_Cyber-Conflict_Greek_Politics_Specialist_Group_Working_Paper_no.7_April_2011

31. Oketola, D. 2012, 'Protecting Information Assets Amid Increasing Risks' *Punch*, 17 September, accessed on 12 June 2013 from <http:www.punchng.com/business/technology/protecting- information-assets-amid- increasing-risks/>

32. Oketola, D. 2012, 'Targeted Cyber attacks, An Increasing Economic Threat', *Punch*, 23 January, accessed on 12 June 2013 from <http:www.punchng.com/business/technology/targeted-cyber-attacks-an-increasing- economic-threat/

33. Oxford Dictionaries, online edition, accessed on 16 April 2013 from http://oxforddictionaries.com/us/definition/american_english/cybersecurity

34. Wall Street Journal, 16 January 2013, accessed on 5 April 2013 from <http://online.wsj.com/article/SB1000.html>

Authour

Captain (NN) Idowu Bobade Yusuf is a Course Member of NDC 2013, Bangladesh. He was born in Lagos, Nigeria, on 05 January 1964. He joined the Nigerian Navy on 08 July 1985 as a member of 6th Regular Course, Nigerian Naval College, Onne, Port-Harcourt, Nigeria. He graduated as the Best-all-round Cadet, winning the President Sword of Honour in 1987. He was commissioned as a Sub Lieutenant on 08 July 1989. He is also a graduate of the famous German Naval Academy, Flensburg, Germany. In addition, he did the Sub-Lieutenant Technical Course and obtained the German Bridge Watch-Keeping Certificate between January 1988 and December 1990. The officer has attended courses at various military institutions abroad including HMS DRYAD, UK *and US Army Intelligence School of Excellence, Fort Huachuka, Arizona. He attended the Communication School at Nigerian Navy Ship (NNS) QUORRA, Lagos, where he specialized as a Communications Officer. He attended both Junior and Senior Staff Courses at the prestigious Armed Forces Command and Staff College, Jaji, Nigeria. He graduated from Obafemi Awolowo University, Ile-Ife, Nigeria with Bachelor of Science degree in Electronic and Electrical Engineering and Master of Technology, Electronic and Telecommunication Engineering. He has held many appointments in the Nigerian Armed Forces. He was an instructor at the Communication School, NNS QUORRA and Nigerian Navy Intelligence School, Lagos. He served at the Armed Forces Simulation Centre, Jaji-Kaduna and Defence Intelligence Agency, Abuja. He was the Executive Officer, NNS AGU and he commanded the only Presidential Yacht, MV AMARYA, both ships stationed in NNS BEECROFT, Lagos. Captain Yusuf served at the Headquarters of the Nigerian Navy Logistics Command, Oghara and commanded the Nigerian Navy Intelligence School, Apapa, Lagos. He has sailed to over 10 countries mostly in Europe and Africa and visited many other countries. Before coming for NDC in Bangladesh, he was the Command Communications Officer at the Headquarters Naval Training Command, Lagos. Captain Yusuf is married to Mrs Adetola Yusuf, a housewife and a businesswoman. They are blessed with 3 children; Bukayo, Philip and Deborah. His hobbies include reading, teaching, and sightseeing. Others are playing volleyball, chess and badminton. He is also a very good listener.*