ISSN: 0973-5089 - January – June 2015. Vol. 9 (1): 120–143. DOI: 10.5281/zenodo.22390

National Cyber Security Policy and Strategy of Nigeria: A Qualitative Analysis

Oluwafemi Osho[1] **& Agada D. Onoja**[2]
Federal University of Technology, Minna, Nigeria

Abstract

With advancements in modernization came the infiltration of information and communication technologies across the world, Nigeria inclusive. Several benefits are obtainable from these but also prevalent are some associated risks. Communication exists massively in cyberspace and as such poses a myriad of threats to a nation. This can be addressed on a national spectrum by the implementation of cyber security policies and strategies. This research involves making a qualitative analysis of the current Nigerian National Cyber Security Policy and Strategy. The documents were analyzed in the light of selected harmonized strategy developmental frameworks and subsequently comparatively evaluated with similar documents of selected countries. After the analysis, the national documents were found to have met majority of the requirements in terms of content, but failed to address certain elements of concern to cyber security in the Nigerian environment.

Keywords: Cyber crime, Cyber space, Cyber security Policy, Cyber security Strategy.

Introduction

Characteristic of human existence is the persistent, yet insatiable urge for the discovery and continual improvement of easier methods of goal attainment and execution of tasks. Brought by this limitless urge, was the development of a myriad of modern techniques and procedures, all coined under the all-encompassing term broadly referred to as technology. Undeniably, technology has innovatively improved human living standards and provided multi-faceted solutions to complex problems facing human existence.

Technological advancements have resulted in the attainment of a variety of remarkable milestones, many of which are in the area of Information and Communication Technologies. Over the past few decades, further research and development has led to the discovery of innovative computer technologies, which have enjoyed widespread adoption in the world over. The massive infiltration of computerization in modern times has increasingly left the world heavily reliant on computer technologies and networks. This can be seen in several facets of human civilization including but not limited to banking, education, commerce, business, healthcare, socialization and communication, which have

[1] Department of Cyber Security Science, School of Information and Communication Technology, Federal University of Technology, Minna, Nigeria. Email: femi.osho@futminna.edu.ng
[2] Department of Cyber Security Science, School of Information and Communication Technology, Federal University of Technology, Minna, Nigeria.

metamorphosed from previously adopted conventional modes of operation to computerized techniques enjoying unprecedented acceptance levels.

The widespread adoption of these technologies has blazed like a wildfire and Nigeria as a nation is not left out of those favorably engulfed in its flames. The country has in the 21st century been one of the major consumers of information technologies in Africa, and can comparably match several other consumer countries in Europe and the Americas. A reflection of this can be seen in the high rate of foreign based information technology giants establishing branches, as well as the growing amount of indigenous technology firms in Nigeria.

Nonetheless, articulated to the widespread use of these technologies are several downsides; one of which is the commission of crime with the aid of these technologies. The coherent existence of crime and criminality with human existence has resulted in the adoption of ICTs in the commission of a variety of crimes, thanks to the interwoven nature of human existence, crime and technology. Computer crimes and cyber crimes, whose commissions have proven highly prevalent in modern times, are in actuality, not more than digitalized versions of their conventional equivalents, operational in cyberspace.

Odumesi (2014) adopted a working definition of cyber crime in Nigeria from the technological and sociological aspects, defining it as "a crime involving the abuse or misuse of digital resources in a cyber-environment on or through the internet, computer networks, computer systems and wireless communication systems." Blitz (2009) defined cyber crime as "abuses and misuses of computer systems or computers connected to the Internet, which result in direct and/or concomitant losses and also criminal activity that has been facilitated via the Internet." Loader and Thomas (2000, p. 2) had explained, "Cyber crime can be regarded as computer-mediated activities which are illegal or considered illicit by certain parties and which can be conducted through global electronic networks".

Conventional crimes can easier be curbed via physical measures involving detection, investigation, apprehension and prosecution, adopting traditional methods requiring the use of physical techniques however, when these crimes become digitalized, severe complications arise, making the solutions cumbersome or in some cases, infeasible to find. Digitalization of crimes have presented law enforcement agencies with mutations in conventional crime, resulting from the technicalities involved, advancements in crime commission methods, increased anonymity, reduced possibility of successful criminal profiling amongst others. Hence, traditional methods of solving crimes have become unhelpful with the computerization of these crimes.

Overwhelmed by the activities of cyber crime perpetrators, several countries, international organizations and initiatives have elevated issues of cyber security to the national level, reflecting its importance as a national security issue. Having a massive presence as an active participant in cyberspace, Nigeria is not left out as it has recorded a fair share of cyber crime incidents. Known for having a reputation of being a haven for the commission of computer-aided advanced fee fraud, widely referred to by the populace as "419" or "yahoo-yahoo" amongst other crimes, Nigeria's cyber crime statistics is high and climbing. Long-term commission of these crimes has left Nigerians and foreigners alike overly cautious to the extent where legitimate interactions of all forms originating in, or concerned with Nigeria and across cyberspace are now characterized with increasing disbelief.

Being an issue of national priority in Nigeria, cyber security is now elevated to the level of being handled by the Presidency through the Office of the National Security Adviser (ONSA). A reflection of these could be seen in the presentation of the National Cyber Security Policy and Strategy drafts by the above-mentioned office. What better results could these documents provide in terms of functionality and applicability to the Nigerian environment than those arrived at after a critical analysis of the developmental framework prior to its implementation.

Nigeria is interestingly at a defining moment in the establishment of a cyber-security policy and strategy framework. This is only an aspect of the numerous processes in their developmental stages concerning national security. In 2013, the President assented to the Nigerian Cyber Crime bill by the President. In June, 2014, the National Cyber Security Policy and Strategy drafts were officially presented at a symposium held in Lagos.

Characterized by an unrestricted borderless nature, the importance of security policy implementation through standardized and functional strategies in securing cyberspace cannot be overemphasized. This explains why the government of Nigeria has continued to solicit for the active support, participation and contributions of stakeholders from relevant sectors towards achieving increased national cyber security.

This main objective of this study is to perform a critical scrutiny of the Nigerian Cyber Security Policy and Strategy drafts. To achieve this, we review timeline of cyber security policy and strategy development in Nigeria. Some selected National Cyber Security developmental frameworks, focused on the development of security policies and strategies in an open environment are examined. We then harmonize the examined frameworks, extracting peculiarities amongst them. Furthermore, the Nigerian National Cyber Security Policy and Strategy is evaluated in the light of these harmonized frameworks. And lastly, we present a comparative evaluation of the Nigerian Cyber Security Policy and Strategy with those of selected countries.

With Nigeria being at crossroads in cyber security policy formulation, this study would prove relevant in providing important information as deduced from an analysis of the National Cyber Security policy and strategy drafts, with regards to validating the standard of the documents. This information would prove helpful in the assessment of the drafts as compiled by ONSA and subsequently provide contributions and recommendations if need be, prior to eventual cyber security strategy implementation in Nigeria. It would also provide necessary information as to the viability of the policy and strategy framework with respect to the Nigerian environment.

Literature Review

Cyber Security Policy and Strategies

Prevalent in recent times are businesses, establishments, initiatives, organizations or nations as the case may be, creating and being governed by policies and strategies, applicable to all spheres of their operations and spanning their expected lifetime. These often times exist as documents, which serve as guidelines to be followed in all situations, whether favorable or unfavorable, expected or unforeseen. Policies and strategies act as developmental frameworks characteristically crafted by key policy makers and top executives of an organization and meant to be austerely adhered to, regardless of immediate or impending situations, having been developed for these purposes. The

success of any organizational initiative is dependent on the immediate goals set out to achieve as well as the methods prescribed and adopted with which to achieve such goals. These documents are more frequently intertwined in the goals, which they set to achieve and, hence, are often regarded as being one and the same.

According to the Office of the Nigerian National Security Adviser (2014), "National Cyber Security Strategy (NCSS) is the nation's readiness strategy to provide cohesive measures and strategic actions towards assuring security and protection of the country's presence in cyberspace, safeguarding critical information infrastructure, building and nurturing trusted cyber-community".

Essence of Cyber Security Policies and Strategies

It is imperative that amidst several existing government concerns, the issue of Cyber Security is one whose relevance should be given utmost attention. Currently, cyber security considerations are inevitably gaining global attention. Having such relevance, concerned policy makers, governments and stakeholders cannot help but cautiously craft guiding principles in the form of policies and strategies with which issues of cyber security are meant to be governed.

Jointly, a purposeful and operational cyber security policy and strategy would facilitate the attainment of a reduced possibility of successful cyber incidents on a national level. It would provide a country with the capacity to prevent such attacks and swiftly address them in the event of their occurrence. It also would represent international equality thereby fostering cooperation amongst countries in areas of security and development.

Focal Point of Cyber Security Policies and Strategies

In its entirety, cyber security policy and strategies attempt to provide a framework comprising a multiplicity of guiding principles and action plans aimed at addressing cyber security and its related incidents.

Office of the National Security Adviser (2014) shares similar views with Microsoft (Goodwin and Nicholas, 2013) by its presentation of the following components as major threats sought to be addressed by typical cyber security policies and strategies.

- *Cyber crime* – Cyber crime encompasses all forms of cyber assisted criminal activity in which its commission was partly or totally aided by cyber space and/or its components. Some frequently committed cyber-crimes include cyber stalking, cyber bullying, identity theft, computer-aided forgery, email scams, virus dissemination and malware attacks.
- *Cyber Terrorism* – Cyber terrorism is famous in recent times with the advancement in technology and involves the use of computing and cyber technologies in aiding or executing terroristic activities of any form.
- *Cyber Espionage* – This is synonymous to modern day spying. The existence of activities of spies on cyber space means the elimination of the need for physical presence of spies at the target location, easing its commission and complicating its detection.
- *Online Child Abuse and Exploitation* – Severely frowned at by the international community, online child exploitation is seen to be on the increase. It involves all

forms of activities, which take advantage of the timid nature of children by preys over the internet.

- *Hacktivism* – Regarded as a hybrid cyber activity, hacktivism is a use of computer technology in facilitating online protests, causing civil unrest or disobedience in cyber space by deliberate disruption of information flow.

National Cyber Security Strategy Lifecycle

The European Network and Information Security Agency (2012) in recognition of a national cyber security strategy as a living document, presented the following three approaches as being adoptable in its governance as regards lifecycle.

- *Linear approach*

Strategies functioning by this approach exist for but a while. In this approach, a national cyber security strategy is initially developed, then implemented, assessed and finally terminated or replaced.

- *Lifecycle approach*

This approach follows a similar initial pattern as that of the linear approach but differs at the point of assessment in which the results of the assessment phase are used in maintaining, reviewing and adjusting the existing strategy.

- *Hybrid Approach*

This approach attempts to govern cyber security strategies by continually performing improvements at various levels of the strategy lifecycle when the need arises with the intention of better strengthening its functions.

Cyber Security Policies and Strategies of various countries

Cyber security has in recent times steadily and undoubtedly gained a global stance when viewed on an international spectrum. This results from its potential contributive benefits if addressed appropriately and consequently, possible destructive corollaries if neglected on a national scale. Owing to this is the elevation of issues regarding cyber security as critical national concerns, having topmost priorities in several countries across the world. This had led to the sprouting of national cyber security strategies in the world over, as observed in several countries across all continents. These strategies are seen to have been analyzed in an attempt to deduce their strengths and weaknesses alike. Cutting across various national platforms, examinations into the analysis of some national cyber security strategies is included in this section.

The Data Security Council of India (2013) and Watanabe (2013) both acknowledged the presence of threats posing national security risks on India and France respectively. The DSCI analyzed the Indian strategy from a market driven versus regulatory approach, one that was broadly criticized for such reasons as shortfall in voluntary efforts by the private sector in guaranteeing national security requirements, but seen to be in adoption and encouraged by a multiplicity of countries including the United States. Watanabe (2013,) on the other hand, examined the Cyber Security Strategy of France from a military and national defense perspective, being reflective of its capabilities, responsibilities as well as prospects towards enhancing national cyber security. He emphasized that the French

national cyber security white paper serves as an adaptation means to recent evolutions in a strategic environment. By this analysis, the military roles and capabilities in enhancing cyber security as stipulated by the whitepaper were acknowledged, but faulted for France's lack of critical equipment and budgetary constraints in meeting these objectives.

Also, explained was the whitepaper pointing out France's key position in security and defense but this was criticized as operations of the European Union's Common Security and Defense Policy (CSDP) has in recent times, been observed to lack political will.

Şentürk, Cil, and Seref (2012) and Nitta (2013) in close correlation with Watanabe (2013) admitted the important global role played by the United States in enhancing cyber security. In their analysis of the Turkish cyber security strategy, Şentürk, Cil, and Seref (2012) submitted that the United States national cyber security strategy is seen to be the most examined amongst others, indicating the country's lofty cyber security global relevance. In explaining the importance of cyber space, they reiterated a statement by the UK Cabinet Office in 2009, which highlighted the country's understanding of the security of her national cyber space, in the 21st century, as indispensable for national prosperity and safety.

Though viewed also from a military perspective, their analysis differed from that of Watanabe (2013). It prescribed methods to be adopted by a national cyber security strategy being approached by a target country with a Deter-Disarm-Defend triangle, comprising of defensive military procedures. They however recommended a review of the Turkish national cyber security strategy to allow for the incorporation of more offensive strategies, in the face of the defensive ones presently in place.

Nitta (2013) in her analysis of the Japanese cyber security strategy attempted to point out some areas of weakness and recommend measures for improvement. She acknowledged Japan's move towards increased international collaboration, but encouraged national independence in cyber security. Suggested recommendations included the need to hasten human resource training in essential cyber security areas for increased technical collaboration with other countries, better situational awareness, regardless of high-quality cyber security structure presently in place.

Regardless of the limitless possible variants in which National Cyber Security policies and strategies might come, they generally attain convergence by a common aim – intensifying efforts to strive towards achieving optimum security in cyberspace. However, distinctions lie in the focal points by which this aim is intended to be sought.

Canada

The Canadian Cyber Security Strategy addresses national security in cyberspace from the distinct perspective of the protection of critical national infrastructure. This can be observed from the three strengthening pillars of the strategy which are securing government systems, partnering to secure all vital cyber systems outside the federal Government, and helping Canadians stay secure online. These were majorly aimed at addressing three categories of threats including state sponsored military activities and cyber espionage, internet use by terrorists, and cyber crime (Government of Canada, 2010).

United Kingdom

United Kingdom, on the other hand, in its Cyber Security Strategy of 2011, focused on the derivation of enormous social and economic value from a secure, vibrant and resilient cyberspace. It was hoped that the core values would increase prosperity and improve the United Kingdom national security. Four objectives were stated in the Strategy. These include: tackling cyber crime to make UK one of the most secure parts of the world to conduct business relating to cyberspace; increased resilience to cyber attacks and being better positioned to protect national interests in cyber space; shaping a safe cyberspace that supports an open society; and building essential knowledge, capability and skills to cater for all its cyber security objectives. It can be deduced that the UKs' strategy is aimed at better positioning the nation amongst its pairs (Cabinet Office, 2011).

Japan

Japan in its 2010 National Cyber Security Strategy, primarily focused on protecting the nations' Information System by adopting defensive measures against large-scale cyber-attacks, which have in recent times increasingly gained popularity. Several carefully crafted action plans were prescribed for implementation in the attainment of optimum delivery of security of national Information Systems (Information Security Policy Council, 2010).

Kenya

Crafted in 2014, the Kenyan national Cyber security Strategy clearly acknowledges the nations' position as being in its infancy in terms of cyber security. It therefore centers its strategy on protecting Kenyan National cyberspace interactions against unavoidable threats it must encounter in the course of the developmental phases of the nation's cyber security stance (Government of Kenya, 2014).

France

France, by its National Cyber Security Strategy reflected the large-scale adoption of modern cyber technologies by its citizens. It therefore focused its strategy on strengthening and protecting National Information Infrastructures and sovereignty related information as well as becoming a world power in cyber defense. France collectively viewed cyber security in its strategy, from a defensive perspective (French Network and Information Security Agency, 2011).

The Netherlands

The National Cyber Security Strategy of Netherlands aims at adjusting the national cyber security posture from awareness to capability. Having gained deeper insight into cyber threats, Netherlands by its strategy aspires to adopt a new approach to issues of cyber security by intensifying actions to address cyber threats rather than increasing awareness on the existence of these threats (National Coordinator for Security and Counterterrorism, 2014).

Methodology

The goal of this study is to perform a critical analysis of the Nigerian National Cyber Security Policy and Strategy drafts of 2014. The research entails the execution of several procedures in an attempt to systematically perform a comprehensive scrutiny of the drafts and subsequently present useful and unbiased information regarding its viability.

The method of analysis involved an initial review of some related works in the research area, constituting works involving the review of national cyber security policies and strategies of Japan, France, India and Turkey. In addition, policies and strategies of Canada, United Kingdom, Japan, France, Netherlands and Kenya were reviewed.

An in-depth analysis of some selected national strategy developmental frameworks was performed, after-which the frameworks were harmonized, adopting a 60% minimum occurrence criterion for the extraction of common peculiarities found essential to be contained in a typical national cyber security strategy. Afterwards, the Nigerian national cyber security strategy was evaluated in the light of the harmonized frameworks, using the extracted peculiarities as a basis to measure its competence.

A comparative analysis of the Nigerian national cyber security policy and strategy with those of selected countries was thereafter performed.

Basis for Case Study selection

Being a highly determining national document, prior to its analysis, it was necessary to perform similar but less critical examination of related documents already functional in six countries – Canada, France, Netherlands, United Kingdom, Japan and Kenya. These countries were chosen as they span across four continents – Africa, Asia, Europe and North America. Three of which were chosen from Europe, as it presently has the highest number of countries with functional Cyber Security Policies and Strategies. The continent is also home to the highest number of organizations concerned with the crafting of developmental frameworks for the creation or review of such documents.

In the course of this research, three categories of documents – the national cyber security policies and strategies of selected countries, selected developmental frameworks, and the Nigerian national Cyber Security Policy and Strategy – were analyzed to different intensities.

The analysis of the documents of the selected countries, Nigeria excluded, was done with the intent of deriving the generic characteristics, contents and structure of such documents. In other words, these analyses served as case studies in this research. They were performed in an attempt to gain an overview of what such documents should and should not be.

Critical to this study was the in-depth analysis of some developmental frameworks adoptable in the review or creation of a standardized and reputable cyber security strategy. They included:

- The ITU National Cyber Security Strategy Guide (Wamala, 2011)
- Cyber Security Policy Making at a Turning Point (Organization for Economic Cooperation and Development, 2012),
- National Cyber Security Strategies (European Network and Information Security Agency, 2012),
- Microsoft's Developing a National Strategy for Cyber Security (Goodwin and Nicholas, 2013), and

- Commonwealth Approach for developing National Cyber Security Strategies (Commonwealth Telecommunications Organization, 2014).

The choice of framework selection was based on the compatibility of the frameworks in one form or the other with the Nigerian environment. The national strategy framework developed by Microsoft was chosen to be used in this research, owing to the fact that the company has a global representation, an African and specifically a Nigerian presence. Being a high consumer of Microsoft technologies in both software and hardware, and having been deemed fit for the establishment of a Microsoft branch, a strategy framework developed by Microsoft is irrefutably acquiescent to the Nigerian environment.

Similarly, the National Cyber Security Guide developed by the International Telecommunications Union (ITU) was chosen for use in this analysis for several reasons. First, because of the equity in global considerations across multiple countries by ITU; second was the high-level acceptance of the standards set by ITU exhibited by Nigeria and several other countries; and the all-inclusive international approach adopted by the organization in addressing global challenges facing information technologies.

The adoption of the Commonwealth approach for developing national cyber security strategies clearly resulted from Nigeria's position as a Commonwealth member state, as well as the active role played by the country and benefits derived from its membership to the organization.

The framework crafted by the Organization for Economic Cooperation and Development (OECD), was used in this research because of the organizations motive to globally address challenges facing modernization, independent of the country in question.

The choice of frameworks was rooted in their applicability and relevance to Nigeria, being developed by organizations to which the Nigerian Information and Communications Technology sector is in conformance with.

Examined Frameworks for Developing National Cyber Security Strategies

Useful in the development and scrutiny of National Cyber Security Strategies and/or Policies are Strategy Developmental frameworks. Seasoned professionals who collectively create a pool of knowledge and skills essential in selecting only the finest-grained requirements to be contained in a National Cyber Security Strategy design these frameworks. Frameworks adopted in this research include the following.

1. Commonwealth Approach for developing National Cyber Security Strategies

Birthed by the first Commonwealth Information and Communications Technology Ministers' Forum held in 2014, which resulted in some agreed upon cyber-governance principles, was the development of a framework useful in the development of National Cyber Security Strategies by the Commonwealth Telecommunication Organization (CTO). The framework is aimed at being available for adoption by member states who intend to embark on the development of such standardized document with the Commonwealth as a basis.

2. *International Telecommunication Union (ITU) National Cyber Security Strategy Guide*

In 2011, upon recognition of the importance of a cyber security strategy and extent of possible adverse effects of its inefficiency, the International Telecommunication Union (ITU) developed the ITU National Cyber Security Strategy Guide. This document is independent of international barriers and is prescribed for adoption by all interested countries, in combination with high national values for use as a basis of their individual strategies. The guide targets individuals who are responsible for elaborating national cyber security strategies across different societal sectors.

3. *Organization for Economic Cooperation and Development (OECD) Cyber Security Policy making at a Turning Point*

Consisting of 34 member states, the Organization for Economic Cooperation and Development serves as a platform through which governments of several countries jointly address a variety of common challenges posed by globalization and concerning both member and non-member states.

To this regard was the analysis of the New Generation of Cyber Security Strategies of several countries, to deduce common trends, obviously mandatory as being contained in any modern National Cyber Security Strategy.

4. *Developing a National Strategy for Cyber Security: Foundations for Security, Growth, and Innovation by Microsoft*

Upon realization and in response to the uprising of cyber incidences, Microsoft, an ICT giant, deemed it necessary to contribute to the cyber security sector by the development of a framework for developing a National Strategy for Cyber Security, aimed at being adopted by nations in the world over. Microsoft began by extensively explaining the concept of cyber security, meaning, aim and functions of a well-developed National Strategy for Cyber Security.

5. *European Network and Information Security Agency (ENISA) Guidebook on National Cyber Security Strategies*

Global recognition of the criticality of information and communication infrastructures as well as the challenges posed by securing these infrastructures has continually being a bother. Prompted by this, was the performance of an intense study on existing National Cyber Security Strategies in their individual environmental contexts by the European Network and Information Security Agency, (ENISA) in 2012, resulting in the development of a guidebook aimed at identifying recurrent and notably essential components of a typical National Cyber Security Strategy. Aimed at being a cyber security governance tool, it is recommended for use by both EU and non-EU member states for improved resilience and added security on a national spectrum in cyber space.

I. Comparison between Cyber Security Developmental Frameworks

An individual examination of the selected National Cyber Security Strategy developmental frameworks and subsequent comparison of their prescribed contents resulted in the tabular representation illustrated in table 1 below.

Table 1 Comparison of Cyber Security Developmental Frameworks based on content

Framework / Content	Commonwealth Approach for Developing National Cyber Security Strategies (Commonwealth)	The ITU National Cyber Security Strategy Guide (ITU)	Developing a National Strategy for Cyber Security (Microsoft)	Cyber Security Policy Making at a Turning Point (OECD)	National Cyber Security Strategies (ENISA)
Criterion – Developmental Phases					
Strategy Development					
1. Backed by Strong Leadership	✓	X	✓	✓	X
2. Multi-Stakeholder approach	✓	✓	✓	✓	✓
3. Definition of Cyber Security vocabulary	✓	X	✓	✓	✓
4. Inform and educate key players	✓	✓	✓	✓	✓
Strategy Delivery					
1. Continuous Progress Report	✓	✓	X	X	X
2. Overseeing by dedicated agency	✓	✓	✓	✓	X
Strategy Review					
1. Continuous monitoring and validation	✓	✓	✓	X	✓
2. Periodic Review	✓	✓	✓	✓	✓
3. Align Review to national planning cycles	✓	X	X	X	X
Criterion – Constituent Sections					
Introduction and Background Section					
1. Current National Cyber Security State	✓	✓	✓	✓	✓
2. Presentation of Cyber Security challenges	✓	✓	✓	✓	✓
3. Strategy development justification	✓	✓	✓	✓	✓

Guiding Principles Section					
1. Root Strategy in National Values	✓	✓	✓	✓	X
2. Privacy Respect and Civil Liberties protection	✓	✓	✓	✓	✓
3. Risk-based approach	✓	✓	✓	✓	✓
Vision and Strategic Goals Section					
1. Promote economic development	✓	✓	X	✓	✓
2. Provide National leadership	✓	✓	X	✓	✓
3. Tackle Cyber crime	✓	✓	✓	✓	✓
4. Strengthen Critical Infrastructure	✓	✓	✓	✓	✓
5. Raise and Maintain Awareness	✓	✓	✓	✓	✓
6. Achieve Shared Responsibility	✓	✓	X	✓	✓
7. Develop national and international partnerships	✓	✓	✓	✓	✓
Risk Management Section					
1. Describe risk management method	✓	✓	✓	✓	✓
2. Describe threats and vulnerabilities	✓	✓	✓	✓	✓
3. Categorize risks	✓	✓	✓	✓	✓
4. Avoid creation of national standards to avoid deviation from ICT supply chain	✓	X	✓	✓	X
5. SMART (Specific, Measurable, Achievable, Relevant and Time-based) objectives	✓	X	✓	✓	✓

Strategy Implementation Section					
1. Governance and Management structure	✓	✓	X	✓	✓
2. Legal and Regulatory framework	✓	✓	✓	✓	X
3. Capacity Development	✓	✓	✓	✓	✓
4. Awareness	✓	✓	✓	✓	✓
5. Incident Response	✓	✓	✓	✓	✓
6. Stakeholder Collaboration	✓	✓	✓	✓	✓
7. Research and Development	✓	✓	✓	✓	✓
8. Monitoring and Evaluation	✓	✓	X	X	✓
Criterion – New Themes					
1. Development of Industrial Policies on Cyber crime.	✓	X	X	X	X
2. Addressing major business players	✓	X	✓	✓	✓
3. Fostering cooperation with ISPs	X	✓	X	✓	✓
4. Identifying economic drivers and incentives	✓	✓	X	✓	✓
5. Developing digital identity frameworks	✓	✓	X	X	✓
6. Protection of children online	✓	✓	✓	✓	X
7. Conducting Cyber Security Exercises	✓	✓	✓	✓	✓
8. Developing a military cyber-defense capability	✓	✓	X	✓	X
Non-Governmental Stakeholder Considerations					
1. Trade and Innovation concerns	X	X	X	✓	X
2. Role of International Standards	✓	✓	✓	✓	✓
3. Flexibly policy options	✓	✓	✓	✓	✓

II. Comparative Evaluation between the Nigerian National Cyber Security Policy and Strategy, and those of selected countries.

Table 2. Comparison between National Cyber Security Strategies

Content \ Country	Nigeria	Canada	Netherlands	Kenya	France	Japan	United Kingdom
Criterion – Developmental Phases							
Strategy Development							
1. Backed by Strong Leadership	✓	✓	✓	✓	✓	✓	✓
2. Multi-Stakeholder approach	✓	X	✓	✓	✓	X	X
3. Definition of Cyber Security vocabulary	✓	X	X	✓	✓	✓	X
4. Inform and educate key players	✓	✓	✓	✓	✓	✓	✓
Strategy Delivery							
1. Continuous Progress Report	✓	✓	✓	✓	✓	✓	✓
2. Overseeing by dedicated agency	✓	✓	✓	✓	✓	✓	✓
Strategy Review							
1. Continuous monitoring and validation	✓	✓	✓	✓	✓	✓	✓
2. Periodic Review	✓	✓	✓	✓	✓	✓	✓
Criterion – Constituent Sections							
Introduction and Background Section							
1. Current National Cyber Security State	X	✓	✓	✓	✓	✓	✓
2. Presentation of Cyber Security challenges	✓	✓	✓	✓	✓	✓	✓
3. Strategy development justification	✓	✓	✓	✓	✓	✓	✓

Guiding Principles Section							
1. Privacy Respect and Civil Liberties protection	✓	✓	✓	✓	✓	✓	✓
2. Risk-based approach	✓	✓	✓	✓	✓	✓	✓
Vision and Strategic Goals Section							
1. Promote economic development	✓	✓	✓	✓	✓	✓	✓
2. Provide National leadership	✓	✓	✓	✓	✓	✓	✓
3. Tackle Cyber crime	✓	✓	✓	✓	✓	✓	✓
4. Strengthen Critical Infrastructure	✓	✓	✓	✓	✓	✓	✓
5. Raise and Maintain Awareness	✓	✓	✓	✓	✓	✓	✓
6. Achieve Shared Responsibility	✓	✓	✓	✓	✓	✓	✓
7. Defend the value of human rights	✓	✓	✓	✓	✓	X	✓
8. Develop national and international partnerships	✓	✓	✓	✓	✓	✓	✓
Risk Management Section							
1. Describe risk management method	✓	✓	✓	X	X	✓	✓
2. Describe threats and vulnerabilities	✓	✓	✓	✓	✓	✓	✓
3. Categorize risks	✓	✓	✓	✓	✓	✓	✓
4. Avoid creation of national standards to avoid deviation from ICT supply chain	✓	✓	✓	✓	X	X	✓
5. SMART objectives	✓	✓	✓	✓	✓	✓	✓
Strategy Implementation Section							
1. Governance and Management structure	✓	✓	✓	✓	✓	✓	✓
2. Legal and Regulatory framework	✓	✓	X	X	X	X	✓
3. Capacity Development	✓	✓	✓	✓	✓	✓	✓

4. Awareness	✓	✓	✓	✓	✓	✓	✓
5. Incident Response	✓	✓	✓	✓	✓	✓	✓
6. Stakeholder Collaboration	✓	✓	✓	✓	✓	✓	✓
7. Research and Development	✓	✓	✓	✓	✓	✓	✓
8. Monitoring and Evaluation	X	✓	✓	X	✓	✓	✓
Criterion – New Themes							
1. Fostering cooperation with ISPs	X	✓	✓	X	X	✓	✓
2. Identifying economic drivers and incentives	✓	✓	✓	✓	✓	✓	✓
3. Developing digital identity frameworks	X	✓	X	✓	✓	X	X
4. Protection of children online	✓	✓	X	✓	X	✓	✓
5. Conducting Cyber Security Exercises	✓	✓	✓	✓	X	✓	✓
6. Developing a military cyber-defense capability	X	✓	✓	X	✓	X	X
Non-Governmental Stakeholder Considerations							
1. Role of International Standards	✓	✓	✓	✓	✓	✓	✓
2. Flexible policy options	✓	✓	✓	✓	✓	✓	✓

Findings and Discussion

Evaluation of the Nigerian National Cyber Security Policy and Strategy

The evaluation of the Nigerian National Cyber Security Policy and Strategy is based on a 60 percent minimum content occurrence across the examined strategy developmental frameworks. In other words, contents observed to have a minimum occurrence of 60 percent across all examined frameworks are identified, and subsequently selected as mandatory contents that any standard National Cyber Security Policy and Strategy should address.

Developmental Timeline

With plans in place for an increased broadband service delivery and infiltration of ICT technologies, a subsequent increase in cyberspace interactions is inevitable. Sadly, these interactions are characteristically accompanied by an inexhaustible list of threats, which if not addressed, will not only mar the intended plans, but also self-destruct the entire

nation. To this regard was the move by the Presidency, through the Office of the National Security Adviser (ONSA), to put together a Nigerian National Cyber Security Policy and Strategy draft, which is the first of its kind.

Evaluation of the Nigerian National Cyber Security Policy and Strategy in the light of harmonized Developmental Frameworks

The evaluation was conducted using the contents recommended by standardized developmental frameworks as a basis. Presented in this analysis are contents of the Nigerian National Cyber Security Policy and Strategy, observed to be in accordance with the harmonized developmental frameworks, shown in the context with which they were stated.

- **Strategy Development**

i. ***Backed by Strong Leadership***

This is reflected in the national cyber security strategy by stating that coordination of strategy implementation will be undertaken by the Office of the National Security Adviser, which is directly answerable to the Presidency. By implication, the strategy is being supported by the highest level of national leadership.

ii. ***Multi-Stakeholder approach***

This can be observed in the policy objective of creating multi-stakeholder partnerships and leadership advisory measures useful in gathering intelligence, information sharing and coordinated response. The strategy clearly adopts a multi-stakeholder approach by its numerous moves demanding contributions as well as assigning active roles to such cyber security stakeholders as academia, technical community and law enforcement in securing cyber space and its associated interactions.

iii. ***Definition of cyber security vocabulary***

Contained in Appendix 2, are concise explanations of professional cyber security terms used throughout the policy and strategy drafts. This reduces the technicality and improves understanding of the national policy and strategy if examined by persons not conversant with the field of cyber security and its associated terminologies.

iv. ***Inform and educate key players***

The strategy intends to use the National Internet Security Initiative to train and educate key players in the cyber security industry amongst others, in raising awareness on national internet safety. Targeted amongst these key players are members of the judiciary, law enforcement and the business community.

- **Strategy Delivery**

i. ***Continuous progress report***

Demanded by the strategy is an annual preparedness report, which demands the provision of details as regards the extent to which the strategy implementation has gone. It thereby provides an understanding of critical infrastructure protection and overall cyber security state of Nigeria.

ii. ***Overseeing by dedicated agency***

The Nigerian National Cyber Security Policy and Strategy was developed and presented by the Office of the National Security Adviser, which is directly answerable to the Presidency. It was tasked with the responsibility of creating and managing all matters concerning the national policy and strategy.

- **Strategy Review**

i. ***Continuous Monitoring and validation***

The Nigerian National Cyber Security Strategy intends to adopt a continuous monitoring approach aimed at being up to date with current threat and risk trends facing cyberspace. The strategy intends to monitor the strategy implementation, noting areas that demand increased attention and subsequently update the strategy in future reviews.

ii. ***Periodic Review***

It is recommended that in a bid to retain its functionality, the Critical Information Protection strategy be reviewed after a five year interval.

- **Introduction and Background Section**

i. ***Current National Cyber Security State***

Stated in terms of recent advancements in Information and Communication technologies, as measured by the exponential increase in mobile network and internet penetration was the national cyber security posture. However, this does not present a clear explanation of state of cyber security in Nigeria. As an introduction to a National Cyber Security Strategy, it is imperative that such issues as immediate and apparent threats as well as possibly successful attacks against the nation or its citizenry be clearly included in this portion of the strategy, to provide substantial information on the actual state of cyber security in the nation.

ii. ***Presentation of Cyber Security challenges***

The presence of security challenges posed by increased internet penetration and interactions in cyberspace was acknowledged and served as a justification for the development of the strategy.

iii. ***Strategy development justification***

The strategy intends to address identified threats, recognizing them as being capable of destroying the integrity of a nation, disrupting operations of critical information infrastructure and destabilizing national security.

- **Guiding Principles Section**

i. ***Root Strategy in National Values***

The national cyber security policy offers chances for the creation of a secure network environment providing some benefits, one of which is the promotion of national values.

ii. ***Privacy Respect and Civil Liberties protection***

Respect for citizen privacy and the protection of civil rights intended to be achieved by the policy implementation and is contained in the data protection and privacy section

of the legal framework initiative, where the legislative is tasked with the responsibility of developing and enacting initiatives concerned with data protection and citizen privacy.

iii. ***Risk-based approach***

A risk-based approach is intended to be adopted by the policy as a basis for performing assurance and monitoring of the cyber security strategy. By this, the strategy intends to identify risks posed by cyberspace and strike a balance between retaining the openness of the internet, mitigating and accepting some risks.

- **Vision and Strategic Goals Section**

i. ***Promote economic development***

The policy and strategy are partly intended to be tools for economic development. This was stated while explaining the importance of cyber space to the government, stating Nigeria's recognition of cyberspace as the fifth domain, which drives critical national tasks such as economic development, social interactions, medical, government and national security operations.

ii. ***Provide National Leadership***

A stated objective of the national cyber security policy is to establish amongst others, a national leadership advisory mechanism, useful in intelligence gathering, information sharing and coordinated response. The implementation of the national cyber security policy, would serve as a leading pathway for the attainment of a secure cyberspace for citizen interaction.

iii. ***Tackle Cyber crime***

Contained in the policy is an objective to develop a framework aimed at enhancing collaboration between necessary agencies in combating cyber crime. Several mentions were made of initiatives involving law enforcement and the judiciary on the roles, which they are expected to play in fighting cyber crime.

iv. ***Strengthen Critical Infrastructure***

The strategy on the protection and resilience of critical information infrastructure suggests that several activities should be initiated across the government, business community and stakeholders in ensuring the protection of critical information infrastructures.

v. ***Raise and Maintain Awareness***

The principle of national awareness, capacity building and advocacy was contained as a guiding principle in the national cyber security policy. These efforts were sought to span across several sectors, including private institutions, law enforcement and individual citizens.

vi. ***Achieve Shared Responsibility***

Acknowledged by the strategy on protection and resilience of critical information infrastructures is the fact that the responsibility of critical infrastructure protection should be shared across the government and infrastructure owners and operators.

vii. ***Develop national and international partnerships***

The importance of partnership on a national scale in incident response and cyber crime prevention, as well as on an international scale in online child protection, addressing cyber threats and best practices was contained in the strategy.

- **Risk Management Section**

i. ***Describe risk management method***

In description of the adopted risk management method, the policy identifies several sectors, which are prone to risk, and recommends that the private sector, being the major owners and operators of cyberspace, collaborates with the government in identifying and protecting critical infrastructure, to manage the risks posed on these identified critical information infrastructures.

ii. ***Describe threats and vulnerabilities***

The strategy explains that the cyber threat landscape is fuelled by both state actors – targeted at government infrastructures - and non-state actors including unorganized criminals, terrorists and extremists. These two categories pose major threats on national cyber security. Vulnerabilities are described in the strategy and are said to range from technical faults to human negligence.

iii. ***Categorize risks***

In explaining national cyber risk exposure, the strategy gives an overview of the cyber threat landscape and its impacts. It then classifies cyber threats into five major categories namely Cyber crime, Cyber espionage, Cyber conflict, Cyber terrorism and Online Child Abuse and Exploitation.

iv. ***Avoid creation of national standards to avoid deviation from ICT supply chain***

Recommendations of international standards to be adopted are contained in the strategy on assurance and monitoring where an initiative recommends international standards and frameworks, some of which were specified to ease ICT standardization.

v. ***SMART (Specific, Measurable, Achievable, Relevant and Time-based) objectives***

The objectives of the strategy meet the SMART requirements by clearly being specific in its intended goals, which address relevant security issues and would be monitored and measured for further review set at a five-year interval.

- **Strategy Implementation Section**

i. ***Governance and Management structure***

The strategy implementation will be governed by the Office of the National Security Adviser in joint collaboration with pertinent government agencies in the achievement of strategic cyber security goals. This office was responsible for the creation of the Nigerian National Cyber Security Policy and Strategy and would subsequently be responsible for the policy and strategy management.

ii. ***Legal and Regulatory framework***

Provision is made in the strategy for the development and promotion of such legal framework initiatives as overhauling the judiciary to accommodate new cyber crime legislations. The federal government is responsible for taking legal and regulatory actions aimed at improving its laws to fight cyber crime.

iii. ***Capacity Development***

The strategy provides for capacity development as needed in cyber security incident management. It recommends the development of national capability in the judiciary and law enforcement in cyber crime prosecution as well as the understanding and handling of electronic evidence. It also recommends development across various cyber security sub sectors such as research and development.

iv. ***Incident Response***

The strategy on incident management, as contained in the National Cyber Security Strategy caters for deterring and responding to cyber threats. It provides for the creation of a Nigerian Computer Emergency Readiness Team, which will speedily respond to security incidents.

v. ***Stakeholder Collaboration***

Largely encouraged in the National Cyber Security Strategy is the adoption of a multi-stakeholder approach through collaborations and partnerships between various cyber security stakeholders and the government. This owes its relevance to the important contributory roles and responsibilities attributed to these stakeholders.

i. Research and Development

Emphasis was placed in the Nigerian National Cyber Security Policy, on promoting development in cyber security innovations, to meet the ever-evolving threat situation by collaborations between the government and academia on cyber security research and development.

ii. Monitoring and Evaluation

It is important that various stakeholders have increased confidence and trust in the National Cyber Security Strategy to be a tool for providing increased security. This will be achieved as contained in the strategy, by continuous monitoring and review of the cyber security program management and implementation, which subsequently, would unceasingly provide better security measures across cyberspace.

- **New Themes - General Considerations**

i. ***Fostering cooperation with ISPs***

Being the operators of the tunnels through which all cyber space interactions are passed through, it is important that a national cyber security strategy promotes cooperation between Internet Service Providers and the government, as this would ease access to network traffic and cyberspace activity monitoring amongst others thereby, ensuring higher safety of citizens on the internet. The Nigerian strategy should therefore contain initiatives to foster such cooperation.

ii. ***Identifying economic drivers and incentives***

The identification of economic determinants on which the national economic posture depends is essential by a National Cyber Security Strategy. These are contained in the Nigerian strategy and presented as sectors to which sector specific plans are made regarding national cyber security. Some examples include the financial services sector and the commercial facilities sector.

iii. ***Developing digital identity frameworks***

The existence of a cyberspace digital user identification framework would be of immense use in the fight against cyber crime on a national spectrum. A national cyber security strategy should contain measures to be put in place to ensure that this becomes a reality. With a functional digital identity framework in place, all cyberspace interactions can be monitored and attributed to specific users, thereby promoting a more secure cyberspace, capable of identifying users on the platform. Unfortunately, the Nigerian National Cyber Security Policy and Strategy does not contain this.

iv. ***Protection of children online***

The strategy dedicates an entire chapter to the protection of children against online abuse and exploitation. It recognizes the dangers posed by cyberspace interactions on children and actions to be taken for protection of children.

v. ***Conducting Cyber Security Exercises***

The national incident management strategy provides for the conduct of simulated cyber security exercises by the Nigerian Computer Emergency Readiness Team to enable stakeholders to better understand their roles during possible crisis.

vi. ***Developing a military cyber-defense capability***

Upon harmonization of the cyber security developmental frameworks and extraction of essential components of a National Cyber Security Policy and Strategy, it was observed that further development of the military for the provision of cyber defense is critical to national security.

With the incessant terrorist activities in Nigeria currently, it would be expected that the Nigerian National Cyber Security Strategy would intensify efforts towards the development of military capability capable of addressing cyber terrorism in the event of these conventional terrorists shifting their activities against the country to cyberspace. The effect of a cyber-war could be devastating on Nigeria, if the National Cyber Security Strategy does not put military cyber warfare capabilities in place.

- **Non-Governmental Stakeholder Considerations**

i. ***Role of International Standards***

The strategy encourages the adoption of, and acknowledges the roles played by international standards in information security governance and control. It encourages the adoption of internationally recognized information and communication technologies, to remain within the global cyber security supply chain.

ii. ***Flexible policy options***

The strategy contains considerations that allow for improvements and contributions in line with changes in the information systems environment. It recommends that upon discovery, new methods can be adopted to address new threats. By this, the national cyber security policy incorporates measures that reduce its rigidity, making it capable of adjusting to changing needs and requirements.

Conclusion

In the course of the analysis of the Nigerian National Cyber Security Policy and Strategy, the results of the comparative analysis with similar documents of selected countries was reflective of the fact that the documents are reasonably comprehensive in terms of content. The evaluation based on the harmonized frameworks also showed that the required contents expected to be typically contained in such documents are largely present.

Sadly however, certain aspects which appear to be critical to the Nigerian scenario such as an explanation of the current national cyber security state, partnership with internet service providers, establishment of digital identity frameworks, and the development of a military cyber defense capability were seen to either be utterly absent or only barely implied.

Observed from the findings of this research, are certain areas of concern regarding the Nigerian National Cyber Security Policy and Strategy, for which the following recommendations are put forward for consideration in future reviews.

1. The provision of comprehensive details of the current state of Nigerian cyber security should be contained in the policy and strategy, to provide immediate information to national industry stakeholders.
2. The national policy and strategy should be better localized, to adequately address national issues regarding cyber security.
3. Attention should be paid to the development of a digital identity framework, as the policy and strategy documents are aimed at reducing threats and increasing security, which can be flawed without a proper form of citizen identification in cyberspace.
4. Partnerships between the government and Internet Service Providers should be encouraged to better enhance national cyber security monitoring.
5. The development of a cyber defense military capability with the ability to provide cyber counterterrorism in the event of a cyber war should seriously be looked into and included in the documents.

References

Cabinet Office (2011). *The UK Cyber Security Strategy*. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

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

Data Security Council of India (2013). *Analysis of National Cyber Security Policy (NCSP – 2013)*. Retrieved September 25, 2014 from http://dsci.in/search/node/1474.

European Network and Information Security Agency (2012). *National Cyber Security Strategies - Practical Guide on Development and Execution*. Retrieved August 20, 2014from www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncss/national-cyber-security-strategies-an-implementation-guide.

French Network and Information Security Agency (2011). *Information Systems Defense and Security – France's Strategy*. Retrieved September 13, 2014 from http://www.enisa.europa.eu/media/news-items/french-cyber security-strategy-2011

Goodwin, C. F., Nicholas, J. P. (2013). *Developing a National Strategy for Cybersecurity*. Retrieved August 17, 2014from www.microsoft.com/security/cybersecurity/resources.aspx.

Government of Canada (2010). *Canada's Cyber Security Strategy*. Retrieved August 21, 2014 from www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-sctr-strtgy/index-eng.aspx

Government of Kenya (2014). *Cybersecurity Strategy*. Retrieved September 13, 2014 from http://www.icta.go.ke/wp-content/uploads/2014/03/GOK-national-cybersecurity-strategy.pdf.

Information Security Policy Council (2010). *Information Security Strategy for Protecting the Nation*. Retrieved September 13, 2014 from www.nisc.go.jp/eng/pdf/New_Strategy_English.pdf.

Loader, B. D. and Thomas, D. (2000). Introduction. In B. D. Loader and D. Thomas (Eds.), *Cyber crime: Law enforcement, surveillance and security in the information age* (pp. 1 – 14). New York, USA: Routledge.

National Coordinator for Security and Counterterrorism (2014). *National Cyber Security Strategy 2*. Retrieved September 13, 2014 from http://www.enisa.europa.eu/media/news-items/dutch-cyber security-strategy-2011.

Nitta, Y. (2013). *Japan's Approach towards International Strategy on Cyber Security Cooperation*. Retrieved September 13, 2014 from http://lsgs.georgetown.edu/sites/lsgs/files/Japan_edited%20v2.pdf_for_printout.pdf

Odumesi, J. O. (2014). Combating the Menace of Cyber crime. *International Journal of Computer Science and Mobile Computing*, *3*(6), 980 – 991.

Office of the National Security Adviser (2014). *National Cybersecurity Policy*. Retrieved August 6, 2014 from http://www.cybersecuritynigeria.org.ng/ncsf/index.php/downloadable-docs.

Organization for Economic Cooperation and Development (2012). *Cybersecurity Policy Making At A Turning Point*. Retrieved September 13, 2014 from www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf.

Şentürk, H., Çil, Z.C., Şeref, S. (2012). Cyber Security Analysis of Turkey. *International Journal of Information Security Science, 1*(4), 112-125.

Wamala, F. (2011).The ITU National Cybersecurity Strategy Guide. Retrieved from http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf.

Watanabe, L. (2013). *France's New Strategy: The 2013 White Paper* [White paper]. Retrieved September 13, 2014 from http://www.css.ethz.ch/publications/pdfs/CSS-Analysis-139-EN.pdf.