YAŞAR UNIVERSITY
GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

(MASTER THESIS)

NATIONAL CYBER SECURITY STRATEGY (NCSS): A MODEL FOR NIGERIA

Anas MU'AZU KADEMI

Thesis Advisor: Assoc. Prof. Dr. Ahmet KOLTUKSUZ

Department of Computer Engineering

BORNOVA İZMİR

JULY 2014

APPROVAL PAGE

This dissertation work entitled "National Cyber security Strategy: A model for Nigeria" and presented as a master thesis by me, has been evaluated in compliance with the relevant provisions of Yasar University Graduate Education and Training Regulations and Yasar University Institute of Science Education and Training Direction. The jury members below have decided for the defense of this thesis, and it has been declared by consensus/majority of votes that the candidate has succeeded in his/her thesis defense examination dated 17/7/2014.

Jury Members		Signature
Head:	Assoc. Prof. Dr. Ahmet KOLTUKSUZ	.....
Member:	Assoc. Prof. Dr. Murat KOMESLİ	.....
Member:	Asst. Prof. Kaan KURTEL	.....

ABSTRACT

The society's and individual's harnessing of the power of information and communication technology has inevitably become part of daily routine. The resulting ease, success and the productivity came with a price; breach of security. The prolific system interconnection, increasing linkage between infrastructures, and growing dependence on digital technologies further increased the varieties, volume and velocity of threats and risks. Coupled with that fact, information systems were engineered with less consideration on security but ultimate performance, interoperability and connectivity. The technical solutions are bypassed and themselves need to be sub-guarded. These and the increase of different actors group with advance persisted threats to individuals, organizations and a country as a whole makes it necessary for national government to take steps to adopt strategic measures, procedures and acquire tools to improve the way that technological and cyber-risks are managed: the National Cyber Security Strategy (NCSS).

It is a high-level top-down approach that articulates the nation's peculiar context, principles and achievable objectives. Strengthening security by collaboration, coordination and cooperation with proper deployment of legal, procedural, organizational and tactical measures. It will be hinted a necessity for all nation states to inaugurate the strategic dealing with cyber security as it is crucial for national security, economic prosperity and other national developmental goals. Nigeria is typically desperate for NCSS, a more comprehensive national-led approach toward cyber security to provide human and institutional capacity building, coordination and reshape the legislation policies to deter, detect, investigate and prosecute.

ACKNOWLEDGMENT

Acknowledging the support, protection and guidance of almighty Allah (S.W.T) shall be the first and foremost for his infinite mercy and assistance, who spare our lives this much.

However, this research would not have been successful without the support of a considerable number of people whom I hold in high esteem. I would like to express my deepest appreciation to my supervisor **Assoc. Prof. Dr. Ahmet Koltuksuz** who was abundantly helpful and offered invaluable assistance, support, guidance and encouragement. A special thanks to my able and kind tutors: Assist. Prof. Dr. Tuncay Ercan, Assist. Prof. Dr. Huseyin Hışıl, Assoc. Prof. Dr. Murat Komesli and Assoc. Prof. Dr. Kostadin Kratchanov. Furthermore I would also like to acknowledge with much appreciation the crucial role of Martin Grygar, who squeezed his valuable time to edit the work.

A warmth gratitude goes to my beloved family, Words cannot express how grateful I am. Your prayer for me was what sustained me thus far. I would also like to thank all of my friends who supported me in writing, and incented me to strive towards my goal.

It is indeed with great happiness to acknowledge the top-of-the-line financial support granted by the administration of ***Eng. Dr Rabiu Musa Kwankwaso*** to travel these miles and study overseas. I appreciate this noble opportunity.

Thank you all, May Almighty Allah reward you abundantly.

TABLE OF CONTENTS

Pages

APPROVAL PAGE....iv
ABSTRACT....v
ACKNOWLEDGMENT....vi
INDEX OF FIGURES....ix
INDEX OF TABLES....ix
ABBREVIATION....x
CHAPTER 1. INTRODUCTION 1
1.1 Background.... 3
1.1.1 National security....7
1.1.2 ICT and the internet....7
1.1.3 Cyber security....10
1.2 Terms and the diverging perception....11
1.3 Research focus....12
1.4 The objectives and the overall aim....12
1.5 Research methods....13
CHAPTER 2. NATIONAL CYBER SECURITY STRATEGY (NCSS) 14
2.1 Evolvement.... 15
2.2 Scope of the strategies....19
2.3 NCSS and other strategies....19
2.4 Terms used.... 20
2.5 Setting the context....26
2.5.1 What factors Influence NCSS ?....27
2.5.2 Approaches and processes....28
2.5.3 Strategic Ends....29
2.5.4 Three level of activities and stakeholders....29
2.6 Cyber-attacks....30
2.7 Trends in NCSS....32
2.8 What is lacking in NCSS ?....33
2.9 Examples from Different Countries....34

CHAPTER 3. THE MAKING OF A NATIONAL CYBER SECURITY STRATEGY 36

3.1 What makes up NCSS..... 37

3.3 NCSS life cycle and what to expect at each step..... 39

3.3.1 Development Phase..... 40

3.3.2 Implementation phase..... 47

3.3.3 Evaluation and adjustment..... 54

3.4 Algorithm for defining NCSS..... 58

3.5 A generic Algorithm to create cyber security strategy..... 60

CHAPTER 4. A MODEL NCSS FOR NIGERIA 63

4.1 Introduction..... 63

4.1.1 What has been done so far?..... 64

4.2 The Strategic context..... 67

4.2.1 What has induced a lack of cyber security in Nigeria?..... 69

4.2.2 The Imperatives for Nigeria..... 70

4.3 Scope..... 70

4.4 NCSS relation to other documents..... 73

4.5 National Vision..... 74

4.6 Framework conditions..... 74

4.7 Strategic aim and objectives..... 75

4.8 Strategic measures..... 76

4.8.1 Legal measures..... 77

4.8.2 Organizational structure..... 79

4.8.3 Technical and procedural measures..... 87

4.9 Means..... 90

4.10 Implementation hints..... 91

4.11 Glossary of definitions..... 92

CHAPTER 5. CONCLUSION AND RECOMMENDATIONS 94

5.1 Conclusion..... 94

5.2 Recommendations..... 95

BIBLIOGRAPHY 96

INDEX OF FIGURES

Figure page

Figure 3.1 NCSS composition.....38
Figure 3.2 Elaboration Steps Flow chart.....44
Figure 3.3 Implementation flowchart.....53
Figure 3.4 An evaluation and adjustment flow chart.....57
Figure 3.5 Overall NCSS life cycle.....62
Figure 4.1 Proposed governing structure.....82
Figure 4.2 'whole of government' and 'whole of nation' response.....84
Figure 4.3 A way to a secure use of cyberspace.....87
Figure 4.4 The effective cyber security tackling in Nigeria.....90

INDEX OF TABLES

Table page

Table 2.1 :Cyberspace and cyber security definitions at international level.....23
Table 2.2: Cyberspace perceived nations.....24
Table 2.3: Cyber security perceived nations.....23
Table 2.4: Major cyber-attacks from 2006 to 2013.....31
Table 2.5: A summary of nations' NCSS.....34

ABBREVIATION

APT	Advance Persistent Threat
ARPANET	Advance Research Project Agency Network
BYOD	Bring Your Own Devise
CCPU	Computer Crime Prosecution Unit
CERT	Computer Emergency Respond Team
C-I-A	Confidentiality- Integrity-Availability
CSIR	Computer Systems Incident Response
DDoS	Distributed Denial of Service
DFC	Directorate for Cyber security
EFCC	Economic and Financial Crime Commission
ENIAC	Electronic Numerical Integrator and Computer
ENISA	European Union Agency for Network and Information Security
FIRST	Forum for Incident Response and Security Teams
GPEN	Global Prosecutors E-Crime Network
ICS	Industrial Control Systems
IMPACT	International Multilateral Partnership against Cyber Threats
ISPs	Internet Service providers
ITU	International Telecommunication Union
IXPN	Internet Access Point of Nigeria
NCI	National Cyber security Initiatives
NCS	National Cyber Security
NCSS	National Cyber Security Strategy
NCWG	Nigerian Cybercrime Working Group
NSS	National Security Strategy
RACI	Responsible, Accountable, Consult, Inform
VoIP	Voice over Internet Protocol

CHAPTER 1. INTRODUCTION

In today's world, the information revolution era of reshuffling of bits to carry out information operations of negative or positive influence is attracting the attention of policymakers. Information is now the core element of power, driven by the rapid advancement in technology that gives rise to a virtual, complex and globally common environment; "Cyberspace". Conflict, crimes and more human hostile activities are being reported more frequently than ever. In fact, it seems to becoming the next battlefield, as speculated by some scholars.

Cyberspace integrates almost every aspect of human endeavor, making individual, organizations, cooperatives and governments more prosperous and booming. At the same time it makes these entities much more pregnable, with devastating ramifications. Attacks are more targeted, resourced and sophisticated. In general the challenges are complex and tactical approaches to the security proves inefficient. Hence, a political zeal to meet these challenges is obviously required. Nation states by their very position of strength embark on strategic approaches, publicizing and announcing national cyber security strategy documents. Yet many states have yet to produce a strategic scheme, though, there are about 69 countries that have cyber security and/or cyber warfare plans or some specific plans for information and political operations.[1] Moreover, as few as thirty-five states produced or announced a national cyber security strategy document, only 3 from Africa (Kenya, Uganda and South Africa).[2] Nigeria does not produce any, despite how well it is known for cyber crimes (Scam, fraud etc.).

---

[1] J. Lewis and K. Timlin, "Cyber security and Cyber warfare: Preliminary Assessment of National Doctrine and Organization", Center for Strategic and International Studies, Washington, DC, 2011

[2] http://ccdcoe.org/328.html National strategies and policies. NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia. Accessed 27/12/13 20:03.

The effort to control, regulate and enhance security of information and telecommunication infrastructure as composed of cyberspace has transformed from tactical to strategic, individual to governmental and organizational to nation-states. Hence, to arrive at a significant comprehensive solution, national cyber security strategy is being developed as a high-level top-down approach.

As of the current state of many strategies, the main goals of cyber security are to protect critical infrastructures, enhance economic well-being and national security. With these in mind, it turns out that the ultimate objective is to mitigate cyber risks and threats. Unfortunately, most if not all strategies lack a concrete mechanism to address cyberspace as a global virtual space, rather more confined within a state's interest.

To set up or to elaborate a National Cyber Security Strategy (NCSS), the policymakers need to pay attention to the balance between openness (freedom) and security, defensive and offensive operations, system modernization and critical infrastructure protection, perceptions and definitions to key elements and the need to have a common standards and harmony.

As a basis of global security of infrastructures and services, tight and suitable technical and legal measures have to be in place. These, in conjunction with diplomatic means, deterrence mechanisms and policies would effectively face and respond to cyber security. With strategic problems, rising politically motivated cyber incidents and the ubiquity and sophistications in threats, it is apparent that no single country or international organization would come up with an all and sundry solution. An approach that combines expertise, resources and capabilities of national governance, international organizations and local communities is needed. National cyber security strategy, through the relevant central focal point would serve as the means for coordination.

As the trends shows, adversaries have had more enabling capabilities to carry out an attack which is aided by anonymity, rule and regulations that ends at

state borders and high infrastructure connectivity with insufficient security. These pave a way for continuously much more unknown vulnerabilities, undetected intrusions and hence attacks increase in velocity, volume and variety. The future that we all seek is that in which vulnerabilities are reduced, confidentiality enhanced, impact of attack reduced and are responded to in a timely fashion.

1.1 Background

The reliance on information and communication technologies make it indispensable for reliable and sustainable communications network infrastructure and services, to this effort there are measures taken to address these issues. Technical measures, operational (institutional) measures and the most recent the strategic measures are couple with legal support, the central concept of which is coordination of activities, capacity building (awareness) and international cooperation.

Security issues in cyberspace evolve from a technical primer to strategic[3]. There is high need to let everyone know and believe that some reasons contribute to why we should all care about cyber security. Some evidence is concrete for all to see, others needs it to be pointed out. Internet and telecommunication systems modernize every aspect of our lives, the ease of use and the cost effectiveness with fruitful outcomes that make individuals and groups embrace these new technologies. About 40% of the world population are online and the number of mobile-cellular subscription is about 6.8 billion[4], which is almost the entire world population and these figures are annually increasing. Unfortunately, most of these users, especially new users are not well aware of the risks involved and the crimes being perpetrated, not to mention of how to safely use the systems with the basic security precautions in mind.

---

[3] Kenneth G "Strategic cyber security", NATO cooperative cyber Defense Center of excellence Tallinn, Estonia. 2011.

[4] ITU, The World in 2013. ICT Fact and Figures, (Geneva: ITU, 2013).

Furthermore, besides the hardware improvement; advancement in the programming and coding boost applications development and services; both standalone, web-based and other cyber-related. These make the tools for attack inexpensive (with a few Dollars or even free of charge from the underground market); easy (less skills and professional knowledge); and effective (devastating consequences). Even a boy that is 12 years old has the ability to hack in-to major government websites. The more the dependence on E-services (cyberspace in general) the higher the risk of being compromised. According to the report "2012 Norton cybercrime report" by Symantec, there are 556 million victims of cyber-crimes (scams, frauds, theft, hacking, malware and viruses attacks etc.) per year in 24 countries; this figure is more than the entire population of the EU[5]. Countries ranked as the advanced members of the information societies are often the victims, they bear most of the damage and costs from malicious programs and host the majority of botnets. Increasing applications and services makes the cyber environment more cluttered, compounding the way in which targets are being pursued.

Moreover, critical infrastructures that are being modernized (based in cyberspace) are becoming much more susceptible to cyber-attack. Government systems and industrial control systems are being explored for their weaknesses. In the 2012 fiscal year, 172 unique vulnerabilities affecting industrial controls systems (ICS) were traced [6]. Between October 2012 to December 2013 a total of 200 incidents were recorded in the US. Well resourced adversaries are using multiple possibilities and attack vectors to pursue their objectives. The Morris Worm in 1988 was one of the first worms that affected cyber-infrastructure and stopped about 10 percent of computers connected to the internet.[7] Since then, every new advent of

---

[5] Norton cybercrime report, Symantec, 2012.

[6] ICS-CERT monitor, US. http://www.us-cert.gov/control_systems/pdf/ICS-CERT_Monthly_Monitor_Oct-Dec2012.pdf .

[7] http://www.washingtonpost.com/wp-srv/special/investigative/zeroday/cyber-history-timeline/ accessed on 23/12/2013 time 21:50.

malicious codes come with more powerful exploits and stealthier technologies; recent attacks like Stuxnet and Flame malware prove it.

In addition, there has been quite an increasing number of individuals and/or groups with varieties of motivations threatening Cyberspace. Before the year 2000, attackers were mainly hackers/crackers, script kiddies and criminals whose sole motives were curiosity, breaking new defenses and some financial gain. Following the ubiquity of information technology and cyber enabled services and infrastructures, many actors are actively evolving threat to cyberspace: Hacktivists, criminal groups, foreign governments, botnets operators and companies (industrial espionage) with their respective motives are more destructive, financially damaging and disruptive.

In addition to the above policy, there are considerations that highlight reasons for cyber security and, additional challenges that necessitate strategic security in cyberspace to be explored. Many users of information and telecommunication technology are not aware of the basic security precautions and do not appreciate the ease now which their systems could be compromised e.g. the presence of malware (root kits, backdoors and others) or be part of botnets. The threat that may even extend to malware such as cryptolocker with the victims being held to a form of ransom. Malwares target individuals but can combine to form a serious threat to a national security.

Moreover, international legislations to tackle cyber insecurity are so meagre, even if present they are not comprehensive enough to face the dynamic nature of the cyber environment, as regulations may be outdated or few states have signed various laws from treaties, though, there are also some customary laws like those of the International Court of Justice.

Categorically, what is being done so far to address cyber security issues could be described to either as tactical or strategic? In many cases the solutions adopted are purely technical, and the drawback is that they address a particular problem in a

particular context, which could be evaded and bypassed, so technical solutions themselves need to be protected and managed in a secured manner[8]. Cyber threats ought to be tackled in a dynamic and continuous managerial process, involving preventive measures and consequence management in both legal, organizational, technical and human perspectives.

Besides the issues being resolved there are some outstanding aspects that need to be addressed. A clear distinction between cyber defensive and cyber offensive capabilities. Some states have incorporated cyber-attack and cyber warfare into their doctrine and military organizations. There is a thin line between offensive and defensive actions, so a nation's strategic documents have to specify explicitly what they really mean by incorporating cyber commands. The obligation for a state is to apply offensive cyber capabilities and the application of existing laws and norms and amendment of the relevant legislation on the use of offensive capabilities and force in Cyberspace. Hence a clear landscape and international law is needed. Also, with respect to capacity building, there is lack of comprehensive courses in our institutions and career path for cyber security. The availability of cyber security and information assurance classes is very scarce in the public educational system[9]. Mainly information operation is attributed to military and because there is no guarantee of financial success (no career path).

The argument that 'Can a cyber-attack pose a serious threat to a national security?' Seems unjustifiable to some and vivid to others. This may be due to the fact that yet there is no serious attack launched at the nerve center of any nation and that the attacks are mainly on elements of the private sectors. Tied all together, the likelihood of a cyber war has not yet visibly materialized. But, from all indications, cyberspace will be the next share of conflict, even with the consideration that most

[8] Cyber security guide for developing countries.

[9] Edwin Leigh Armistead "The Development of IO/IW Curriculums in the United States: A Review of Current Efforts and a Case Study From Norwich University" 2012 ICIW paper.

critical infrastructures are operated by private entities. Most countries are now including and updating military plan to encompass cyber dimension and capabilities, information operations and electronic warfare.

1.1.1 National security

National security can be dated before the advent of cyber security strategy, it is the quest for securing national assets, economy and societal values that influence and span in to national cyber security strategy development. The term "National security" has been in use since post-World War II as an academic concept[10], literally known from the United States, which initially aimed at military reference, now becoming much more broader, including non-military, economic and other dimensions. National cyber security is derived from two terms: 'National security' and 'cyber security' and the direct connection is a recent phenomenon, largely due to the shift from countering a specific threat to a strategic way of dealing and mitigating multiple threats and risk based management.

Almost all national cyber securities strategy articulate cyber security as the top issue in national security, and this move has proven to be the approach to comprehensive national security. For a State to have National security, it must have military security, economic security, political security, environmental security, infrastructural security and most importantly to our discussion in today's information era, is information assurance and security in the cyber environment. It is worth the efforts, due to the fact that cyber security is a complement to economic security, infrastructural security and the above mentioned element of security.

1.1.2 ICT and the internet

Data, considered as a raw fact that is being processed to get information, is the primary target in security issues. But data in its discrete forms is not that much useful in the real sense because it does not directly identify a pattern, a trend or a

[10] http://en.wikipedia.org/wiki/National_security accessed 29/12/2013 15:30.

system, but information does. Information is derived from data. Perceived information subsequently becomes knowledge and knowledge together with considerable experience provide wisdom that guide our way to the present information and communication technology society. Human beings advances because they share and communicate knowledge and wisdom which is the foundation of the development in sciences and technology. In the same context, cyberspace also advances due to the sharing and telecommunication of information and services fuelled and guided by interconnectivity and interoperability of the infrastructures.

From the dawn of ICT, national security was the key consideration in the first developments in electronic computing, which played profound roles during World War II. For example, the Bombe and Colossus were cryptographic devices; while ENIAC was designed to compute ballistic trajectories. In essence, during the pre-internet period before the 1960s, governments tried to solve war problems using computing devices. Then, it can be said that there were no computer crimes compared to the subsequent periods, largely because the systems were not so interconnected and nor abundant. After the World War II, the alumni of code breaking efforts join research institutes as computers and electronic devices began to have influences outside the military domain and research networks also broke a new ground. To further give an idea of the role played by national security, one of first networks, ARPANET project was funded by US Department of Defense. What was the real motivation for that?

The internet first came in to being after many breakthroughs, influenced by the need to promote advanced research and education networking. At this time application computers were built and networks were interconnected which allowed some companies to get involved. As the computing systems spread, the attacks and malicious worms also found a way into the networks. In 1982, the US under the Central Intelligence Agency masterminded one of the first cyber-attacks on Russia which caused an explosion of Siberian gas pipeline. An explosion that resembled a missile lunch but with the insertion of computer code (logic bomb).This and other

breaches of security raised an alarm that computers and the network could be used for destructive purposes.[11]

As the internet shifted from research and educationally oriented to commercial and operational networks, more than 100,000 computers were connected and internet service providers made services available to the general public. At the same time, the sophistication of security problems continued to dramatically evolve, in parallel with the magnitude of the targets. The technical solutions were being developed for these technical problems. Now we reach a threshold where the technical means of leveraging this issue is so meagre.

Presently, the internet and information and communication technology has become part of our life and of everything in a developed society. More things are connected as we move from fixed computing through to Bring Your Own Devices (BYOD); the internet of things to the internet of everything. In 1984 there were only 1000 internet devices, and in the year 2003, 500 million were connected. Presently there are more than 12.5 billion devices in this world of 6.8 billion people [12]. The internet is one of the most influential innovations ever devised by a human. In addition to peoples connected to the internet, the next evolution of internet is characterized by the millions or even billions of things or objects connected in the forms of sensors nodes and automation [5]. Meanwhile, IPv6, VoIP, smart power grids, cloud computing, industrial automation networks, intelligent transport systems, e-government, e-business and much more are the trends shaping these future aspect of Cyberspace. These infrastructures are becoming interconnected. Failure in one can affect others. Alongside greater convenience and efficiency lies greater vulnerability and risks. A new dimension of threats is to be expected and so strategic approaches appear to be feasible and essential.

---

[11] http://www.scmagazine.com/from-sci-fi-to-stuxnet-exploding-gas-pipelines-and-the-farewell-dossier/article/180051/.

[12] Evans, The Internet of Things. How the Next Evolution of the Internet Is Changing Everything. 2011.

1.1.3 Cyber security

Cyber security has been a recent term, widely adopted after the year 2000 [13], and a strategic perspective of mitigating threats, but as threats become more sophisticated and the technology increase in capacity and the field gets wider, so also the perspective and extent of protection must get evolve. The initial concept of security in the information revolution era was computer security, with the main concern being the assurance of the normal operation of a computer system. Later, information security, which is a more encompassing term, extended the scope of understanding to include computer networks and all the information processed or stored. As the information get messy, information assurance arises as the necessary measures to defend valuable information and information systems. Of recent relevance is the misunderstanding that cyber security simply equate to internet security. It is more than that, in fact, cyber security incorporate: internet security, critical infrastructure protection, ICT security, information security and network.[18] Cyber security can be referred to as:

- The measures, activity, process, ability or state whereby information and communications systems and the information contained/process are protected from any damage, abnormal operation or exploitation[14]. This relate to the technical origin of security.
- Strategy, policy/principles, standards and legislation enhancing the security of cyberspace. Involving threat and vulnerability reduction, deterrence, international engagement, resiliency, with application of various means; diplomacy, military, and intelligence for a secure global information and communications infrastructure [14].This relate to Strategic security perfective.
- A degree of protection as a result of the measures, activities and policies employed.

---

[13] http://en.wikipedia.org/wiki/National_security accessed 29/12/2013 15:30.

[14] http://niccs.us-cert.gov/glossary#information_assurance : A Glossary of Common Cyber security Terminology. Accessed 11/10/2013.

- A field of research and study that includes professionalism, research and development.

However, there is not yet a globally accepted definition of cyber security. This hampers protection efforts, which must be undertaken at both national and international levels, given the borderless nature of today's networks and computer systems.

1.2 Terms and the diverging perception

There is no consensus (no single accepted common definition) on a broader scale of what is cyberspace, cyber security and other basic security components and terms used to denote various approaches, and these impede the international moves to mitigate and secure cyberspace when viewed as common global environment. By the same token, at the national level it poses great challenges, as different stakeholders are involved and each may have a specific expertise and focus. Though, a common acceptable definition is not likely as the information technology has been evolving. The consequences of this is that some previous definition may be irrelevant in the near future, hence, relatively understanding the terms and keeping the concept flexible may help to some extent.

Only coordinated and comprehensive approaches that entails public-private sector efforts ensure a reasonable information assurance, infrastructural protection and cyberspace security for a nation. Nevertheless, when vigorous collaborative efforts extended to national-international organizations/governments will tackle the global challenge to cyber security. Moreover, the effectiveness of the measures is determined by the dimension covered: the element of cyber security, the component of Cyberspace, specific area of focus and also the best practice and standards employed[15].

[15] Eric A. Fischer " creating a National framework for cyber security: An analysis of issues and options " congregational Research service report for Congress. 2005.

1.3 Research focus

Cyber security being a major issue, is gaining attention at the international level. Nation states continuously acknowledge the influence of information and communication technology and the effect on critical infrastructures, economy and other facets of national concern. In the same vein, there have been some initiatives to tackle cyber security problems in Nigeria, but, in one way or another they lack comprehensiveness and coherent framework and the initiatives are in slow transitions. In 2009, Nigeria was ranked third in the world by Internet Crime Report (National White Collar Crime Centre and the Federal Bureau of Investigation, 2010). In a similar report in 2012, Nigeria was ranked eighth in a victim list of cyber crime with a loss worth $2,552,944.03. With all these negative statistics, there are neither a Computer Emergency Respond Team (CERT)/ Computer Security Incident Response (CSIR) nor tangible standards and policies employed. Hence, the focus of this dissertation is to elaborate NCSS for Nigeria.

1.4 The objectives and the overall aim

Overall research aim

The overall aim of this research is to discuss the necessity of strategic solutions to cyber insecurity; providing framework and requirement in elaborating NCSS with a model for Nigeria.

The objectives

1. Identify and discuss needs to comprehensive cyber security.
2. Evaluate the approaches and effectiveness.
3. Examine various NCSS of various states.
4. Develop a model NCSS that suits Nigeria.

1.5 Research methods

This study will make use of a number of literature sources (usually open source), including reference to relevant books, journals, reports, conference proceedings, government publications and appropriate websites. Examples of these include: periodical surveys such as the Symantec cybercrime report, the world ICT facts and figures by ITU, ENISA information security publications; the Journal of Information Warfare; and proceedings of the European Conference on Information Warfare and Security; and most importantly, national cyber security strategies of various nations.

CHAPTER 2. NATIONAL CYBER SECURITY STRATEGY (NCSS)

Governments have enabling capabilities and power, nevertheless, not all risks can be mitigated by individuals, organizations or even governments alone. The risk in Cyberspace is the best example in which the responsibility is shared. The ever expanding and influencing nature of cyberspace makes nation states realize that the security of information and information systems constituent of cyberspace is a priority and the specific techniques and procedures employed for each task or the multi-agency coordination of incidents are no longer feasible. The issue needs to be systematized into an organizational structure set to incorporate all means to an end which is compounded in strategic confrontation.

The individual national context would portray what is meant by national cyber security (NCS). There is no universally accepted definition of what it comprise of, never explicitly defined in official strategy. However, we can trace a description of NCS in other documents:

"Is a tool to improve the security and resilience of national information infrastructures and services. It is a high-level, top-down approach to cyber security that establishes a range of national objectives and priorities that should be achieved in a specific timeframe. As such, it provides a strategic framework for a nation's approach to cyber security."[16].

"The focused application of specific governmental levers and information assurance principles to public, private and relevant international ICT systems, and their associated content, where these systems directly pertain to national security."[17].

[16] ENISA, National Cyber Security Strategies. Practical guide on development an execution, 2012.

[17] National cyber security framework manual, NATO cooperative cyber Defense Centre of Excellence, Tallinn, Estonia, 2012.

"Outlines a vision and articulates priorities, principles, and approaches to understanding and managing risks at the national level."[18] .

Hence, what is expected of NCSS is strengthening the resilience of the cyber domain and bridging the gaps left by traditional and technical information security capabilities.

2.1 Evolvement

While all National cyber security strategy came into being after the year 2000, the United States (U.S.) has focused on cyber security since the 1990s with responsibilities assigned to different departments. It is the first country to acknowledge cyber security as a strategic issue of national concern. The Initiator term National security was largely used within the U.S. with the first publication "National security strategy" in 1987 [19]. In those days the notion of computer security and or information security was not so much a national concern. Technical precautions and measures had been in place to counter specific threats. So also the national security was narrowed, usually perceived as the territorial integrity of a state with focus on military sectors.

Since the end of the Cold War there has been a considerable development in security policies, a notion of "comprehensive security" breaking a new ground encompassing security in various domains such as economic security, energy security, environmental security, and critical infrastructure protection and the security threat acknowledging non-state actors, natural disaster etc. in addition to the State-centric territorial view[20]. These change in security perspective, policy procedure and the need for a concretely unified approach to meet the security challenges with all the available resources minimally used, leading to newly

---

[18] Goodwin F. C, J. Paul Nicholas "Developing a National Strategy for Cyber security" 2013 Microsoft Corporation.

[19] John K. Bartolotto " The origin and developmental process of the national security strategy" U.S. Army war College 2004 http://history.defense.gov/docs_nss.shtml.

[20] http://en.wikipedia.org/wiki/National_security accessed 4/01/2014 18:2.

published white papers, security policy documents and national security strategies to be drafted.[21]

Cyber security has been identified as another domain in national security, as generated threats affected national assets seems to have driven the creation of national security strategies or a shift to a more overarching strategy. The NCSS identified cyber threats capable of impacting other domains the and new security challenge shifted toward the strategic level, which requires lots of attention. Some national cyber security strategies have direct link with NSS and other policy documents as the issue is horizontal in all sectors of national importance.

As part of the effort to protect the U.S. the "National Strategy to Secure Cyberspace" was released in February 2003 by the Department of Homeland Security as part of the overall National strategy for homeland security, developed in response to the attack of 9/11. The strategy developed purposely to "engage and empower Americans to secure the portions of Cyberspace they own, operate, control or they interact in." [22]. It was all about awareness, threat assessment and information sharing with focus on critical infrastructure protection and public-private partnership. These strategic confrontations leads to the creation of information-sharing organizations (e.g. CERT-US, information-sharing and analysis centre, national information protection centre)[23].

For similar needs, necessities and reasons cyber security policy documents, a action plans and strategies began to spread and draw the attention of policy makers across the globe. Most states had some form of information system security policies or specific to critical information protection which predated the actual creation of a comprehensive NCSS. For example Germany, in 2005 adopted its "National Plan for

---

[21] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world.

[22] White House, The National Strategy to Secure Cyberspace (Washington, D C: White House, 2003).

[23] https://www.dhs.gov/about-national-cyber security-communications-integration-center: accessed 15/01/14, 22:07.

Information Infrastructure Protection"[24], Sweden, in July 2006 developed a "Strategy to improve internet security in Sweden". But documents like these are very limited in focus and action plan and therefore need to be more comprehensive.

The Stuxnet attack in 2007 triggered the development of the Estonian Cyber security strategy in 2008 which focused on information systems. Purposely developed to reduce the vulnerability of cyberspace in and for Estonia, the action plan was regulation, education and cooperation.[25] In the same year, the Finland and the Slovakian cyber security strategy were developed. In the year that followed, a few more strategies were unveiled: the Australian, Canadian and the U.K. strategies. The content of these strategies could be considered comprising of a relatively narrow view of what constitutes cyber security, and without much regard to a global common.[26]

The first Strategy form the African continent belonged to South Africa and was unveiled in 2010. The fifteen page document aims to establish an environment that will ensure confidence and trust in the secure use of ICT. It also focuses on six objectives with emphasis on governmental system and critical infrastructure.[27] With the recognition of the increase in cyber risks, threat incidents, vulnerabilities and potential impact to economy and society at large, 2011 saw the massive adoption of NCSS with about thirteen countries producing one. This came about largely as a result of politically motivated attacks, Distributed Denial of Service (DDoS) and malicious warm. For instance, the Stuxnet, DDoS on Georgia in 2005, Con-ficker in 2009, Aurora in 2010, a attack on the Canadian Government in 2011, "Red October

---

[24] German Federal Ministry of the Interior, national plan for information infrastructure protection 2005.

[25] Estonian Ministry of Defence, Cyber Security Strategy (Tallinn: Estonian Ministry of Defence, 2008) .

[26] Luiijf, E., Besseling, K. and Graaf, P. (2013) 'Nineteen National Cyber Security Strategies.' Int. J? critical infrastructures, Vol. 9, Nos. 1/2, pp. 3-31.

[27] South Africa Department of Communications, Notice of Intention to Make South African National Cyber security Policy (Draft approved 11 March 2012) (Pretoria: South Africa Government, 201.

in 2012 " and the Korean attack in 2013. Essentially, nation states are suffering from breaches of security. Within three years not less than 20 nations drafted or announced the adoption of the strategy[28].

To date, about 36 nations state are said to have announced or released a national cyber security strategy/ national information security: Australia, Austria, Belgium, Canada, Czech Republic, Estonia, Finland, France, Germany, Hungary, India, Italy, Japan, Kenya, Latvia, Lithuania, Luxemburg, Montenegro, Malaysia, New Zealand, The Netherland, Norway, Poland, Panama, Russia, Romania, Slovakia, Singapore, Spain, Switzerland, S/Korea, S/Africa, Turkey, Uganda, UK, and US.[13][29] Half of the these nations have additional military doctrine and organization of cyber warfare[30].

Technically speaking, states with low internet connectivity and information infrastructural development would be less likely to have cyber capabilities, whereas all advanced information societies have cyber policy, legal documents, strategies, defense strategy and/or a specific plan for informational and political operations. Even with limitation of open-source literatures, language barrier (lack of translation of some documents), coupled with the sensitive nature of respective national plans and capabilities, especially with regards to security issues, a total of more than 70 states acknowledge the need or are concerned with cyber security/information security at a national level[31].

---

[28] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world.

[29] NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estoniaccdcoe.org/328.html .

[30] James A. Lewis and Katrina Timlin, Cyber security and Cyber warfare. Preliminary Assessment of National Doctrine and Organization, (Geneva: UNIDIR, 2011), http://www.unidir.org/pdf/ouvrages/pdf-1-92-9045-011-J-en.pdf.

[31] James A. Lewis and Katrina Timlin, Cyber security and Cyber warfare. Preliminary Assessment of National Doctrine and Organization, (Geneva: UNIDIR, 2011), http://www.unidir.org/pdf/ouvrages/pdf-1-92-9045-011-J-en.pdf.

2.2 Scope of the strategies

Most NCSSs adopted a holistic perception of cyberspace but some ended up in marginalizing the actions on specific component of cyberspace. e.g. it was apparent that the Germany, Australian, Spanish, New Zealand and Canadian NCSSs consider information and communication technologies that are internet based, while other strategies tend to be specific and explicit in their discussion in this regard. The Hungarian NCSS goes a little bit further by incorporating a sovereignty consideration child protection policy[32]. A full of range ICTs were not properly addressed; untrustworthy ICT needs to be taken in to account, therefore, supply chains need to be sub-guarded.

Most policies and strategies were not bold enough on insider threats, some of the biggest threats may be a result of "insider" actions. Stakeholders are more concerned with external threats because they are eye-catching. Also, there is little consensus on what constitutes cyber security threats and the threat topology model; the threat outlined within cyber security strategies are five-folded base on motivation (cybercrime, cyber espionage, cyber terrorism, and cyber activism)[33]. All strategies converged with the discussion on cyber crime and many identify cyber espionage and very much fewer mention cyber activism and cyber warfare[34]. These prove the fact that the strategies' core attentions are on critical infrastructure and economic dimension.

2.3 NCSS and other strategies

NCSS relates mostly to National Security Strategy (NSS) and other documents or national policies. All national strategies and policy documents strive to either ensure the prosperous economy, business and productivity, power projection,

---

[32] Luiijf, E., Besseling, K. and Graaf, P. (2013) 'Nineteen National Cyber Security Strategies.' Int. J? critical infrastructures, Vol. 9, Nos. 1/2, pp. 3-31.

[33] *Martti Lehto*, "The Ways, *Means and Ends* in *Cyber Security Strategies*."

[34] Other strategies examined.

defense and critical infrastructure protection, or digital agenda projection or combination thereof. The overall primary aim is the national security, hence, in one way or another the strategies are inter-related especially with a main document "National Security Strategy". The strategies are identify the needs to address cyber security and give the issue the highest priority. In turn NCSSs make a references to NSS by reinforcing the security objectives outlined. Though, it is apparently difficult to trace NCSS relationship with other security documents of national importance. A good NCSS should describe how it relate s to other Strategies e.g. national economic development strategy, national critical infrastructure protection strategy etc.

A considerable number of NCSSs are part of National Security Strategy, and a result of national risk assessment and threat analysis. New strategies are often resulted from "National Security" review. "National Cyber Security Strategy" or "Information Security Strategy" is the second most important Strategic document after "National Security Strategy" because they both identify multiple domains.

2.4 Terms used

The scope of terminologies covered and their extensive usage are influenced by what a nation perceive both cyberspace and its technological advancement to be. However, there is an unacceptable chaos regarding the meaning of even the most basic terms and the analysis of the strategies shows that only about one-third of the strategies explicitly define such terms [35] [36]. Some took a step back by incorporating the concept of "information security" instead of "cyber security" and hence a lack of inherent comprehensiveness.

To begin with, the common global virtual and in some way physical (by means of interactive experience) environment coined "cyberspace" began in the

[35] Luiijf, E., Besseling, K. and Graaf, P. (2013) 'Nineteen National Cyber Security Strategies.' Int. J? critical infrastructures, Vol. 9, Nos. 1/2, pp. 3-31.

[36] Martti Lehto, "The Ways, Means and Ends in Cyber Security Strategies."

1980s. Derived from "cybernetic" in the work of Norbert Wiener [37]. The prefix "cyber" was used to denote control (electronic or remote) or of anything associated with the internet or describing entities in cyberspace [38], e.g. cyber-fraud, cyber safety, cybercrime etc. This show that "cyber" and "cyberspace" are the constituent terms to denote other terms, in fact household words. The early perception of cyberspace as defined by William Gibson was the human experience of a new environment identified with it complexity [39]. Late in the 1990s, cyberspace was used as a synonyms for the internet and subsequently as the World Wide Web. In those times the terms internet security, information security, or information assurance were more in used in place of cyber security. The rate at which cyberspace is changing is reflected in the impact and continuous effect it cast on security as whole.

Meanwhile, nowadays cyber security should not be equated to internet security, information security, information assurance or ICT security as the former is more comprehensive as to include perseveration, confidentiality, integrity, availability, authentication and non-repudiation in cyberspace. Though, not all countries are defining or describing what they mean by cyber security in their NCSS, the varying perception falls into either; protection of information systems, secure ICT system and services or mitigation of threat from cyberspace. That is to say there is a more narrower rather than holistic perception and usage.

Similarly, all strategies discussions acknowledge cybercrime as it causes enormous financial loses to individual, companies, nations and the global economy at large, but never define it at first. Though, recent strategies seek to come up with what they mean by the related terms, Romania and Australia are the only nations that

---

[37] http://readtiger.com/wkp/en/Cyberspace#Origins_of_the_term. Accessed 24/01/14 9:12.

[38] http://en.wikipedia.org/wiki/Cyberspace, accessed 24/01/14 12:15.

[39] Gibson, W. (1984) *Neuromancer.*

define almost all cyber related notions in their strategies, some defined the basic terms as can be exemplified in the Turkey Strategy [40].

A typical strategy should establish a common ground by specifying and wording the key concept. While nation states pursue their interest, the cyber domain also lacks accepted norms and principle of proportionality[41]. When international approaches are discussed, this brings about confusion and difficulties. To this effect, US-Russia produce bilateral work on cyber security terminologies.[42] The first concrete step on an international definition of key terms in cyber and information security field, were taken though UN, with others bodies also having sponsored similar efforts, but with no great success.

Moreover, international organizations and treaties are also striving in wording their views on the terminologies of cyberspace. An example of frequently mentioned and fundamental terms are illustrated in the table that follows (Table 2.1). Cyberspace and cyber security were chosen to be analyzed as all other terms are based on, or derived from them.

[40] Luiijf, E., Besseling K. and Graaf, P. (2013) 'Nineteen National Cyber Security Strategies.' Int. J? critical infrastructures, Vol. 9, Nos. 1/2, pp. 3-31.
[41] ITU National Cyber security Strategy Guide, (Geneva: ITU, 2011).

[42] Russia-US Bilateral on Cyber security: Critical Terminology Foundations 2011.

Table 2.1 : Cyberspace and cyber security definitions at international level.

	cyberspace	**cyber security**
ITU	"Systems and services connected either directly to or indirectly to the internet, telecommunications and computer networks"	"The collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets...."
ISO	"the complex environment resulting from the interaction of people, software and services on the internet by means of technology devices and networks connected to it, which does not exist in any physical form"	"preservation of confidentiality, integrity and availability of information in the Cyberspace"
EU	"the virtual space in which the electronic data of worldwide PCs circulate"	"Safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. "

A generalized analysis on what can be considered in individual definitions:

Table 2.2: Cyberspace perceived notion.

	Cyberspace						
	ICT	Information	Service	Internet	Network	Virtual	Users
Australia	●	○					
Canada	●	●	●		●	●	
Estonia	●	●					
Germany	●			●	●	●	
N. Zealand	●				●		
UK			●	●	●	○	●
USA	●	●		●	●	●	●
EU		●				●	
ISO		●	●	●	●	●	●
ITU		●	●	●	●	●	
NATO		●			●	●	

Table 2.3: Cyber security perceived notion.

	Cyber security		
	C-I-A	Top-Down	Bottom-up
Australia	●		●
Canada	●		●
Estonia	○	○	
Germany		●	
N. Zealand	●		●
UK	○	●	
USA	○	○	
EU		●	
ISO	●	●	
ITU	●	●	
NATO		●	

● The definition explicitly refers to this element

○ The definition implicitly refers to this element

User (social human involvement)

C-I-A Basic security Elements which are confidentiality, integrity and availability

In the two tables above, I considered the term from the explicit definition where it was given or an implied description[43].

[43] https://blogs.cisco.com/security/cyberspace-what-is-it/ accessed 10/02/14 10:15.

Conclusively, the varying definitions that are being given for cyber security converge at protecting critical national assets and at securing the use of cyberspace to drive economic prosperity. Cyberspace was defined to consist of globally internet connected hardware, software, data/information and services but unfortunately, the varying definition fails to address this dynamic nature and human users[44]. Moreover, the strategies discuss cybercrime, cyber terrorism and cyber espionage as more frequent threats, with cybercrime occupying the premier position.

The needs for harmonized understanding and definition is an aspect that needs time and sacrifice of some policies and interest by nation states. These in addition have to be lively as to tally with the dynamic cyber environment. International treaties and organizations started to highlight and provide a working guide and recommendations to establishment, maintenance and implementation of NCSS, e.g. ENISA, ITU, NATO etc. In 2011 International Cyber Security strategy was documented by the US, claiming a leading role in the global common 'Cyberspace' and adjoining other nations and international stakeholders to align to this strategy[45]. But, at the very least, a consensus is required on definitions in order to achieve the necessary mutual understanding at international level and among different stakeholders.

2.5 Setting the context

To have a clear direction in this discussion, there must be clear answers to such questions: (1) What are the factors influencing NCSS? (2) What are the approaches and processes? (3) Where is the strategy directed at and the range of stakeholders to be address? In view of these, I conceptualized the issues as: the factors affecting NCSS activities, levels of activities.

---

[44] Rain Ottis, Peeter Lorents "**Cyberspace: Definition and Implications"** Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia.

[45] "U.S. Cyber Command Fact Sheet", US Department of Defense, <www.defense.gov/home/features/2010/0410_cybersec/docs/CYberFactSheet%20UPD>

2.5.1 What factors Influence NCSS ?

National Interest: National security makers attempt to defend their interest in the process of their strategies and in cyberspace as a whole. These interests flow from national values to political context. The set of objectives and actions were being developed in consistent with individual states' interests. Moreover, different features in governmental structure, organizational structures and crisis management approaches exhibit another divergence. In some cases these national interest may have priority over those that are common. Disparate interests of individual states therefore complicate international level approaches.

***Threats and Risk Spectrum*:** The strategies focus on the threats most likely to disrupt essential national activities. Preventing all cyber threats and vulnerabilities is costly and demanding because cyberspace is never risk-free. Each innovation and development reveals new vulnerabilities, and often an open door for complex attacks. All nations address cyber threats to critical infrastructure and increasingly addressing threats to economy. Basically, the types of threats being featured, range from cyber activism to cyber war.

Security Policy and convention: The strategy can be seen as basically a set of policies and the achievable strategic goals. Security policy is the outcome of risk analyses that govern how cyber security will be applied. Therefore policies that will be employed impact on a way and manner in which NCSS activities are to be set. Moreover, cyber security is a global challenge, nevertheless we do not have world government. Therefore, global efforts rely on having international treaties and conventions on cyber security in place to guide the global response. Therefore, national cyber security activities are not as effective as they could be without international agreements that bear upon cyber activities, such as treaties and customary laws. Treaties take years to agree to and are difficult to enforce, but attacks and vulnerability are fast evolving and there is growing consensus around on agreeing acceptable norms.

2.5.2 Approaches and processes

The areas of cyber incident managements can be classified as: Diplomacy, Intelligence, Military, Policy, Law and Economy [46]. NCSS concentrated on certain approaches to counter cyber insecurity by using Military and/or civilian approaches, intelligence and law enforcement tied to the tactical through strategic approaches.

***Military and/or Civilian*:** Usually perceived in the form of cyber security or cyber warfare. Civilian agencies are charged with the responsibility of security in cyberspace in majorities of nation states, a traditional approach where by a special unit is coordinating the operations. However, there is still heated debate on the involvement of military command and planning to acquire offensive cyber capabilities. The links between cyber warfare, electronic warfare and cyber security are likely to be expanded as military s are embedding or creating new divisions for cyber capabilities. e.g. the U.S. created its cyber command in 2009 [20]. Nevertheless, differences in goals, organization and operational culture in these approaches determine and affect NCSS.

Intelligence and law enforcement: Intelligence is a key component of tactical and strategic decision-making in the cyber domain to tackle cyber threats. Intelligence enhances governments and stakeholders' ability to detect threats, assess the cyber-capabilities of adversaries, evaluate the effects of cyber-attacks and mitigate the risk. Unfortunately, security intelligence is a bit lacking in most NCSSs. The formation of an integrated security culture is required. Whereas law enforcement are one of the approaches incorporated in the action plans of all NCSSs. "Interests of the intelligence/counter-intelligence community (IC) are very often in direct opposition to the interests of law enforcement (LE) in general" [47].

---

[46] Tikk E, " Comprehensive legal approach to cyber security" PhD desertion faculty of Law, university of Tartu, Estonia 2011.

[47] National cyber security framework manual, NATO cooperative cyber Ddefense Centre of Excellence, Tallinn, Estonia, 2012.

Tactical through strategic: States devise strategies for land, air, sea and space domains because of their criticality in achieving national interests. Similarly, one may point out that states require a strategy for securing cyberspace because of its growing contribution to the delivery of services essential to daily life, commerce, national security, innovation and the general free flow of information. Therefore, strategies help mitigate the impact of cyber-attacks.

2.5.3 Strategic Ends

Cyberspace is currently secured primarily through private regulatory activity, defensive strategies, national laws and enforcement, and some limited forms of international cooperation and regulations. Cyber security is not an in end itself, but a tool to reach certain objectives and potentials.

- National security
- Protection of critical infrastructure
- Economic prosperity
- Social well being

2.5.4 Three level of activities and stakeholders

Categorically, NCSS considers three wider range of activities which are at the same time the broader stakeholder engagement areas. International, governmental and societal dimensions which entail collaboration, coordination and cooperation respectively. It is a big challenge working with different stakeholders[48].

All strategies give more emphasis on government, whereby the 'Whole of Governance' approach is preferred. This is because employing coordination among government departments is likely one of the most crucial tasks of any NCSS. Applying this approach to NCS is increasingly viewed as being key to success in national cyber security.

[48] National cyber security framework manual, NATO cooperative cyber Defense Centre of Excellence, Tallinn, Estonia, 2012.

2.6 Cyber-attacks

The growth of politically motivated attacks triggered the development of NCSS, although attacks of such nature had occurred before the 2007 attack on Estonia. International attention has understandably greatly increase since then. Table 2.4 below shows more details on these.

Table 2.4: Major cyber-attacks from 2006 to 2013. [49] [50] [51]

YEAR	ATTACKS
2006	• December 2006. NASA was forced to block emails with attachments before shuttle launches out of fear they would be hacked.
2007	• Zeus Botnet: Trojan horse 'Zeus', controlled millions of machines in 196 countries. • Estonia DDoS-attacks: DDoS-attacks against web sites of the Estonian parliament, banks, ministries, newspapers, and broadcasters.
2008	• Conficker: Forms botnets. • Attack on Lithuanian websites • Georgia DDoS-attacks: DDoS-attacks against numerous Georgian websites.
2009	• Ghost Net: Cyber-spying operation, infiltration of high-value political, economic, and media locations in 103 countries. • Operation Aurora: Attacks against Google and other companies to gain an access • American and South Korean government agencies and commercial Web sites temporarily jammed
2010	• Stuxnet: Spies on and subverts industrial systems • Wiki leaks Cable gate: 251,287 leaked confidential diplomatic cables US • Stuxnet: Computer worm that might have been deliberately released to slow down Iranian nuclear program.
2011	• Duqu: Looks for information useful in attacking industrial control systems. Code almost identical to Stuxnet (copy-cat software). • Sony and other attacks: Highly publicized Hacktivists operations.
2012	• Flame May 28, 2012 • The Russian firm Kaspersky discovered a worldwide cyber-attack dubbed "Red October," that had been operating since at least 2007.
2013	• South Korean financial institutions as well as the Korean broadcaster YTN had their networks infected in an incident said to resemble past cyber efforts by North Korea.

[49] http://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm. Accessed 7/11/13.
[50] Timeline: Key events in cyber history http://gocs.info/lektionen/Timeline%20Cyberspace.pdf.
[51] http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history. Accessed 7/10/13.

2.7 Trends in NCSS

- ***Cyber security as strategic paradigm***

The development and adoption of strategies by national states indicate the emerging and fast-evolving nature of the subject matter as well as government willingness and evolutionary shift from a purely tactical and operational view point to an organizational setting to take account of a rapidly changing environment through dynamic policy approaches. "Security is more about architecture and integration than about deployment of more products to build perimeter defenses."[52]. Individual and organizations are often reactive and tactical, but government stresses proactive and strategic.

- ***Cyber security change in focus***

It subsequently appears that there is a shift in the terms of the key focus on cyber-security, away from protection of information infrastructures and to protecting society at large. The recent strategies also indicate that nation state are increasingly concerned about how the threats perpetrated in the cyber domain immensely affect the economy.

- ***Cyber security having highest priority***

Over the past ten years, in all countries, especially where information and communication technology is so highly valued, cyber-security threats have been prioritized to the top tier of security issues in national risk assessments. However, higher prioritization of threat has not consistently translated into greater resources and funding allocated the area, though, significant allocation can be seen in U.S, U.K, Germany and France. NSSs are converging at the need to secure cyberspace and placing the risk on top of other threats. The main consideration that propel this is that ICTs, the internet and information services form a very vital infrastructure and

[52] Andy Purdy " Cyber security towards a strategic approach to cyber risk".

are essential for development in every perspective. But threats are extraordinarily evolving in complexity and targets, therefore security is paramount[53].

- ***NCSS covered in stand-alone strategy***

Cyber security issue policy documents are dealing with cyber security both as its own discrete element, but also as a horizontal issue that crosses a number of other national goals. Moreover the diversity of this domain makes it necessary to have specific documents to address specific threat in a particular sector e.g. within the military realm.

- ***A broader action plan***

As the adversaries continue to explore additional tactics and methods, there is a growing need to adopt action plans to strengthen resiliencies. Improvements in security incident response through trusted analysis, collaboration and coordination, situational awareness and real time monitoring, research and development and cyber security exercises test the effectiveness the defense mechanisms.

2.8 What is lacking in NCSS ?

Performance measures: It is of course difficult to gauge the performance or otherwise of national cyber security schemes as a result of the complexity of the domain. Having a set of milestones and timeframes for the strategy would make it easier to track the progress in accomplishing its core aims and objectives. Its major strategy is in developing and implementing performance measures to track and evaluate the effectiveness of actions. NCSSs lack performance measures and regular update mechanisms.

Clear Allocation of resources: Fewer strategies like that of the U.K. address publically the cost demand of the scheme. Moreover, the allocated budget, resources and funding does not justify that cyber security is being considered as a top-tier security issue.

[53] "Cyber security policy making at turning point" OECD 2012.

2.9 Examples from Different Countries

With respect to specific types of threat characterized within cyber security, other than a fewer exceptions such as Russia, countries generally recognize a common set of cyber threat actors nevertheless with a difference in prioritization and range[54]. The Table 2.5 below elaborate more:

Table 2.5: A summary of nations' NCSS.

	Threat topology	**Main measures**	**Vision**	**Principles/policies**
Australia	Terrorist, criminals, espionage.	Response, detection, awareness, partnership and regulation.	Secure, resilience and trusted electronic environment.	National leadership, Shared responsibility, partnership, risk management, protection of Australian values.
Canada	States (military and espionage) Cybercriminals Terrorist groups.	Partnership, empowerment.	Making cyberspace more secure for all Canadians.	Not Explicit.
Estonia	Focus on effects of threat actors.	Cooperation, education, regulations and change of character.	Reduce inherent vulnerability of cyberspace in Estonia.	Cyber security integrated in NSS, effort of all stakeholders, protection of human right; personal data and identity.
Finland	No typology available.	Collaboration, awareness, detection and legislation.	Secure vital functions, safe cyber domain, Global Forerunner in cyber security	Responsibility, collaboration, R&D, legislation.

Continue

[54] Neil R, Luke G, Veronika H, Kate R. "Cyber-security threat Characterization: A rapid comparative analysis ."

Germany	Terrorism, crime and war; natural hazards and technical failure or human error.	Cooperation, coordination .	Substantial contribution to secure cyberspace.	All stakeholders act as partners, enforcing; rule of conduct standards and norms.
Netherland	States Private organizations Professional criminals Terrorists Hacktivists Script kiddies Cyber-researchers Internal actors Non-actor.	Partnership, threat and risk mitigation.	Security and confidence in an open and free digital society.	Existing initiative linking and reinforcement, clear responsibilities and partnership, legislation, national and human right.
S/ Africa	Implicit.	Legislation, partnership.	Ensuring confidence and trust in secure use of ICT.	Implicit.
UK	Criminals Nation-states Patriotic hackers Terrorist groups Hacktivists.	Risk base respond, cooperative approach.	Vibrant, resilience and secure cyberspace.	Risk based approach, balancing security privacy and freedom, partnership.
US	Criminal hackers Organized criminal groups Terrorist networks Advanced nation.	Diplomacy, defense and development .	Engage and empower American to secure their portion of cyberspace.	Protecting privacy and civil liberty.
EU	None publicly Available.	Partnership.	Resilience, reduce cybercrime, develop industrial and tech. resource, common defence policy.	Protecting fundamental rights, freedom of expression, personal data and privacy, shared responsibility, access for all.

CHAPTER 3. THE MAKING OF A NATIONAL CYBER SECURITY STRATEGY

Societies have in every aspect, become much more highly interconnected and interdependent; the modern threats as well as the vulnerabilities and challenges induce an urgent need to address inherent weaknesses in security in a cyber domain. A portion with which a given country operates, owns and its citizen interact with the cyber facilities adds up to the global count. It is beyond reasonable doubt that every nation should have a strategic plan for cyber security and it can no longer be considered optional or an issue to be solely addressed by first-world economies. For example, the US engages in a broad array of approaches and measures; political, military, technical and organizational. Fragmented into threat and vulnerability reduction, deterrence, response and recovery and others. In contrast, developing countries largely focus on increasing connectivity and high speed services not adequately taking into account the corresponding ramifications to security breaches.

Governments primarily exist to maintain social order, protect the lives and property of their citizens and to ensure stable propagation of goods and services enhancing economic well-being; As cyber security metamorphoses to the national level, so too is the national leadership responsible for cyber security by making use of all instruments of national power; devising strategies, concrete policies and frameworks. To prosper in the management and developmental processes, it is paramount to have the cooperation of a wide range of stake holders; an agreement to work on a common course of actions with individual, local, national, cross-sector and global synergism. Strong governance and management structure are equally-vital in this regard.

At any point of time, NCSS can be said to be in one of three broad stages: (1)formulation phase (the making) (2) implementation phase (the actualization) and (3) A review phase (the adjustment) for an existing cyber security policy. This can be

pursued via a linear, lifecycle or hybrid approach[55]: (1) develop the framework, implement the plan, evaluate it and finally terminate it or replace with a brand new one, (2) formulate, implement, evaluate and adjust the same framework, (3) combination of the two approaches by continuous improvement cycles at different levels. From the analysis of various strategies and the examination of the nature of cyber security, the second (i.e. cyclic) is most preferred, being seen as an ongoing and continuous scheme of improvement fitting most appropriate into countering cyber threats and dealing with emerging vulnerability issues. This process of developing a NCSS may be either open or closed to the public; determining by the approach that is deemed best by the respective governing body. For states that are starting to develop their strategy or policy document for the first time, it is often difficult to identify best practices and the ultimate approaches. Many of these states may not have the same resources as the industrialized nations and cannot build complex and comprehensive organizations; rather, they can only focus on implementing only the most urgent measures.

Having had the introduction and the review of related work, now a systematic description of how and what to consider and do in elaborating NCSS will be derived as well as helpful recommendations offered. At the core of our assumption is the political will from the national leadership to ensure government support; allocation of resources, arms of government support (judiciary, executive, etc.).

3.1 What makes up NCSS

Conceptually, a strategy is defined as the relationship among ends, ways, and means. ***Ends*** are the objectives or goals sought, ***Means*** are the resources available to pursue the objectives, and ***Ways*** or methods are how one organizes and applies the resources. Each of these components suggests a related question. What do we want to pursue (ends)? With what (means)? And How (ways)? A strategic management or strategic plan is the set of decisions and measures with analysis focused on the achievements of the predefined sole purposes. A NCSS seeks to model the

[55] ENISA, Guide book on National cyber security, 2012.

relationship between national approach and distinctive notion, the goals, the available resources and the methodology to be employed, which a continuous process is striving to fit national information infrastructures within its changing environment into a trustworthy and resilient domain: a pictorial representation given in Figure 3.1. Thus, we see cyber security from a strategic point of view and upon this a generic constituent of an NCSS to be highlighted. With the differences in NCSS drives, risk and cyber threats.

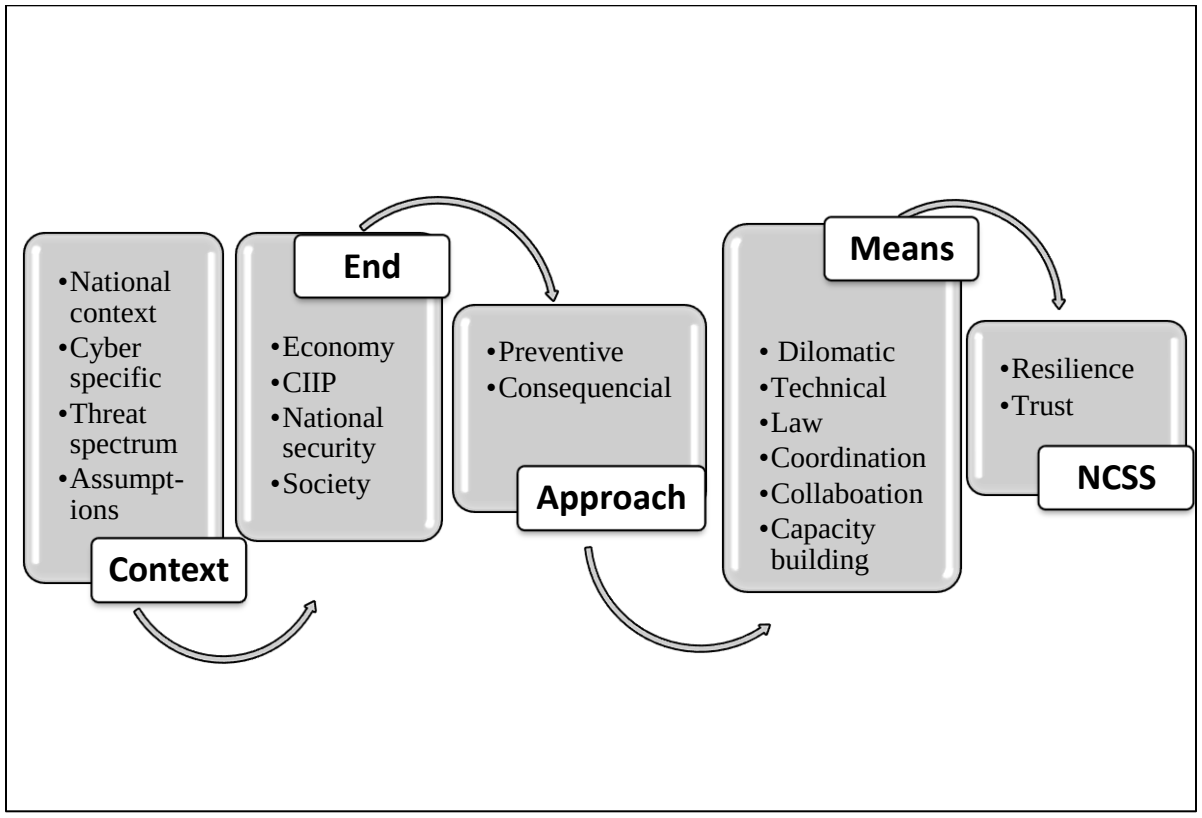

Figure 3.1 NCSS composition.

3.2 **Best Practices**

Below are some considerable best practice and/or philosophical stand to keep in mind while addressing cyber security issues:

- Not a single entity/ nation is able to address the issue on its own.

- Governments to lead by example adopting best practices, technology, compliance, regulation and many more measures. This would serve as an incentive to persuade other stakeholders to do the same.
- Security in cyberspace is not optional and nor traditional measures the solution.
- Note that there is no absolute security in an information system; no perfectly secured system.
- Holistic, integrated and comprehensive security approach.
- Embedded input from key public and private/business entities and academia. Advices from the technical community.
- Effective measures and principles taking into account: internet openness, social values and legal framework (proportionate balance).
- Top-down and risk-based approach strategy.
- A simple, accurate, understandable and applicable security policy. A policy that encourages open standards to enable security solution innovation.
- Framework for coordinating, developing and implementing a robust global culture of cyber security.
- The success of strategies depends upon focusing on the right risks and involvement of all stakeholders.
- Coherent, systematic, and comprehensive mechanisms to be employed.

3.3 NCSS life cycle and what to expect at each step

National capabilities, needs and threat posture vary relatively among countries. Thus, national values and other facets specific to a nation should be a basis for a strategy. A replica of a strategy from another nation may likely do more harm than the supposed security enhancement. An effective approach and culture for strategy elaboration should consider and analyze the relevant strategies and important documents with view to produce a match for the given country.

All the stages in managing a NCSS are equally important and each stage and decision could be viewed as prerequisites to the subsequent. Elaboration/adoption of NCSS attract much media hype, and most drafts of strategies attempt to

communicate minimally less or not even at all with respect to the implementation details of their strategy.

3.3.1 Development Phase

The development phase of a strategy entails analysis and marshalling all the necessary resources and entities to meet the specified goals. Influenced by certain conditions, the process may be managed by a working group or a political leader. But as competence and documents from varying fields are required and as most of the critical infrastructures are operated by private sectors, achieving a common set of standards is paramount to integrate all and sundry. Therefore, a working group of all stakeholders would be preferred.

At the beginning, a number of activities and or events (incidents) may trigger the overall development process or a rethinking of the new policies. On a global scale, at least since the attacks on Estonia, Georgia and Lithuania[56], nations' perception of cyber threats has seriously changed. It has been a wake-up call for policy makers and security experts. Major security breaches, data leakage and/or distributed denial of service may spur NCSS development. Legislators may also pass new laws in a bid to preemptive actions resulting in NCSS formulations. A given resolution could in the same vein serve as the trigger for that purpose. Moreover, another trigger might be an international revolutionizing trend in confronting cyber security and an increasing impediment to realization of full economic development as the case is in Nigeria. Hence, it is paramount to develop a case for action that shows all the concerned individuals the benefits of this coordinated approach. Typically at this point we need to understand and explain the immense value of national cyber security strategy.

Subsequently, we identify and involve all stakeholders and select the right individuals as a working group to facilitate the formulation process. However,

[56] Tikk, E., Kaska, K. and Vihul, L. (2010) International Cyber Incidents: Legal Considerations, Cooperative Cyber Defense Center of Excellence (CCD COE), Tallinn.

executive arms of government are responsible for leading the elaboration process. Every nation has to choose the most effective approach while not forgetting mutual benefits of working together. For instance, in Estonia an inter-agency committee headed by the ministry of defense, with membership from governmental bodies, information security experts and other disciplines from the private sectors were tasked with the development of the strategies[57]. In the specific case of Nigeria and its government's accountability for cyber security the national government may not be in a better position to dictate strategy more than private stakeholders who own and operate the critical infrastructure. Hence, focal government organizations form working group of different agencies and expertise from public, private sectors and academia to create and orchestrate the national cyber security framework. This platform is set to work on a common course of action and is enriched with different input, advice, suggestions and recommendations.

Accordingly, the national perception must then be conceptualize relative to the nation's position within an international strategic context. A thorough analysis in turn performed, based on previous incidents, current cases and anticipated trends to better understand future generic cyber threat sources and actors. The next stage in the development process is modeling the threats and understanding the nation's peculiar key targets, motives and the consequences. E.g. cyber espionage/national intelligence and cyber warfare are higher level threats to national security, cyber crimes and cyber terrorism are intermediate, while others like hacktivism are being seen as low-level threats. Alternatively, cyber crime and related categories might be the primary attention drivers due to their frequency. Accordingly, in employing a risk-based approach, a risk assessment is then conducted a first step in the risk management methodology. Risk assessment identifies, analyzes, quantifies and evaluates risk against criteria for risk acceptance and objectives[58]. This should be performed periodically to address the dynamic nature of information systems. International standards and best practices can help governments to create a solid mechanism in the

[57] Estonia cyber security strategy 2008.
[58] ISO/IEC FDIS 17799:2005(E).

process (e.g. NIST, ISO). The results should guide and determine the appropriate management action and priorities for reducing or eliminating risks and for implementing controls selected to protect against these risks.

Ends are what the strategy is targeting to accomplish. However, there is no perfectly secured information system; we only try to prioritize our objectives in terms of impact to the society, economy or citizen i.e. the vital national interest at stake. Thus, the strategy should be the means to an ends not exactly an end in itself. Cyber security where quantified, is vital in the intensity of national interests[59]. The ends are translatable as a set of objectives (usually highlighted as three or four by most NCSSs) perceived to be a long term goal. Good security decisions can only be made when first the ultimate goals are determined. This helps use effectively the collection of security tools and what restrictions are to be imposed[60]. Typical ends that a given NCSS should aim at are: national security, economic well-being, critical infrastructure protection, promotion of societal value and/or favorable world order[4].

The process is then set to articulate the security policy and principles which should specify among other things the resources, structures, procedures, and plans. It translates what has been understood about the risks and their impact into actionable measures for implementations. Guiding principles also influence security control implementation. The integral plan should mandate all stakeholders, have governance and structure in a framework plan similar to those of other nations. The strategy should also take into account national development plans that might also be relevant to information security and the information society, as well as plans relating to internal security and national defense.

Having identified what we are trying to protect and determined the rational and the threat spectrum we then set in measure in a cost effective manner, organizing appropriate information security best practices. Three dimensions are applicable to

[59] ITU National Cyber security Strategy Guide. Geneva: ITU, 2011.
[60] Site Security Handbook, IETF.

the national security paradigm: law, technology and policy. The policy approach in specific could be organized in the following areas: diplomacy, intelligence, military, law and economics[61]. Adding managerial perspective, the preventive and consequential measures, and the policy approach effectively should manage cyber incidents. ITU highlighted global cyber security agenda through a five-part platform for international multi-stakeholders' cooperation, with measures shaped as legal measures, technical and procedural measures, organizational measures, capacity building and international cooperation. Therefore, the policy makers may reference important documents like this for the approach to adopt and to align themselves in a global cyber security effort.

The efficiency of the framework can be audited by reviewing and validating the assumptions made. An external body may be incorporated for the purpose of examining the audit before it is published/drafted for implementation. In the overall process, goals are directly determined via security tradeoffs like full realization of ICT benefits and services with security, ease of use and security, cost of security versus risk of loss.[5] Dilemmas such as stimulating the economy versus improving national security, modernizing infrastructures versus critical infrastructure protection, data protection versus information sharing and freedom of expression versus political stability are all peculiar to cyberspace[62]. Figure 3.2 summarizes the development stage of the strategy.

[61] Thomas C. Wingfield, Eneken Tikk "Frameworks for International Cyber Security: The Cube, the Pyramid, and the Screen."

[62] National cyber security framework manual, NATO cooperative cyber Defense Centre of Excellence, Tallinn, Estonia, 2012.

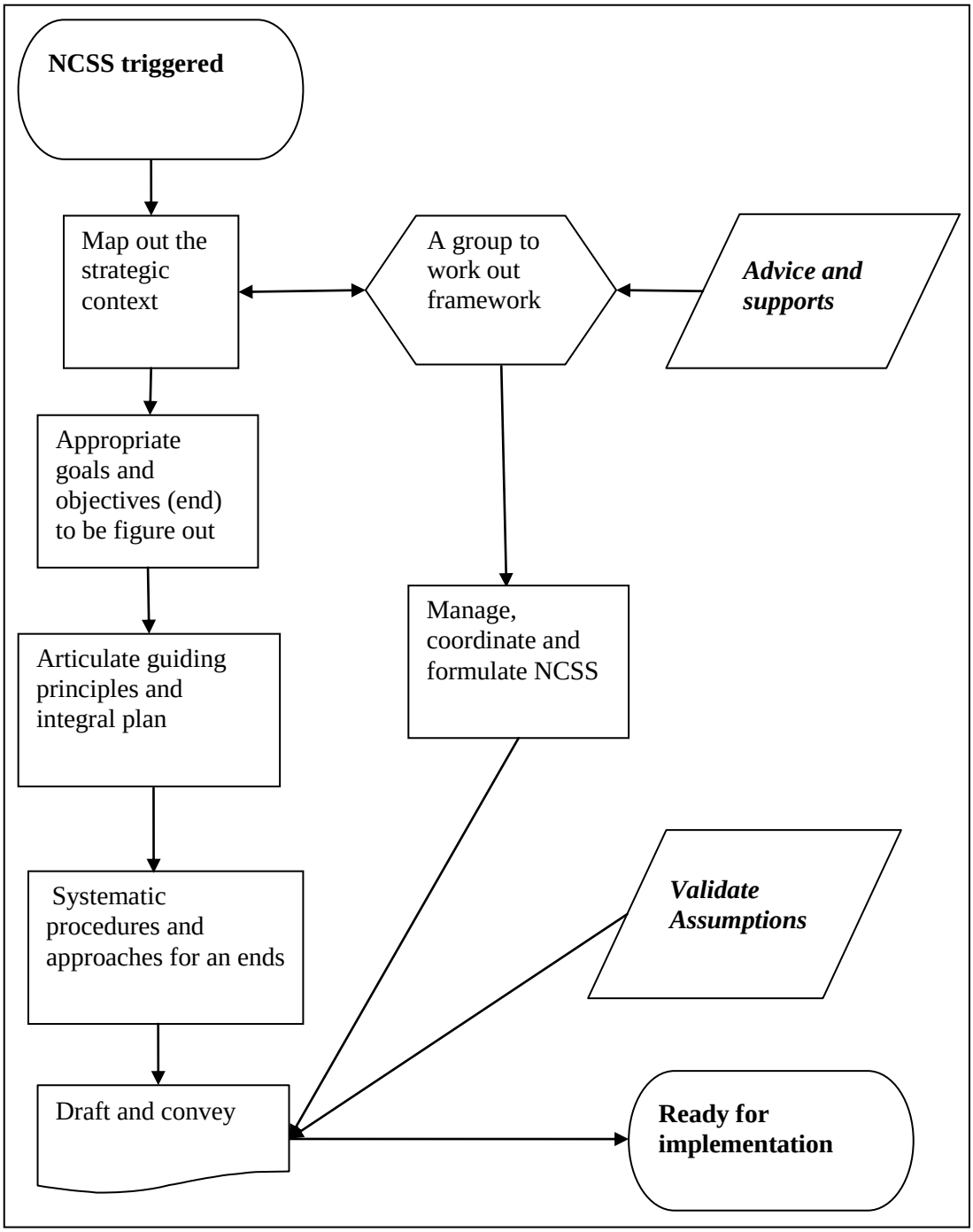

Figure 3.2 NCSS Elaboration Steps Flow chart.

The following strive to highlight non-exhaustive considerations at this step:

Government willingness.

Top government dignitaries are in the forefront in shaping the discussion and encouragement to establish additional or newly implemented tighter security. For example, in most advanced societies, the president or the prime minister have appeared to state their commitment in addressing cyber domain as a driver for the socio-economic nervous system of the country. This declaration will be followed by a review of the national efforts to addressing information and communication infrastructures. Hence, this would serve as an incentive for various stakeholders.

In essence, the challenges in meeting an end in cyberspace are complex and require political will to develop, implement and manage the overall process. The considerable responsibility lies predominantly to those in power. Minimally, things to consider with regard to this are:

- Necessity for cyber threats resilience at national, regional and organizational levels.
- Building national incident management capabilities.
- Encourage cooperation among different entities.
- Promotion of law enforcement.
- Reasonable budgeting to sustain the security measures and the organizational structures.
- Awareness of best practices and minimum security requirement.
- Constitute working group and engage stakeholders.

The Analysis/Assessment

Firstly, the critical infrastructure,, asset and services are to be identified. Information and communication should be analyzed with respect to threats targeted and their potential impacts. The measures and considerations of assets with low potential impact cannot be equated to the system with higher potential impact. Basically, among the questions to be asked are: what constitutes our critical infrastructures (potential assets) and the rationale for protecting them? How

interwoven is the system in the cyber domain? On attack or compromise what is the level of consequence? Activities to be examined that further shape these questions are:

- Main security threats.
- Identify constraint, goals and stakeholders.
- Threat actors involved.
- The existing policies and plan.
- Define the integration plan.
- Define the public and private sectors.

Risk assessment

- Adopt a methodology: a standard or reshape it for particular needs of nation.
- Determine the critical infrastructures that need particular plan.
- Define a mechanism for continuous assessment of risk and vulnerability.
- Cover a wider range of risks.

Principles, guidelines and security policies

Identifying a set of guiding principles helps the strategy not go astray. There are principles that are common among nations; preserving the right to privacy and fundamental values and freedom, coordination and sharing of information.

- Cyber security is not just a technical issue.
- Security is an endless and dynamic process.
- Normal operations can be restored within an acceptable time-frame and at an acceptable cost in case of an attack.
- Take note of existing policies, regulations and capabilities.

Visions and aims

The aim of any cyber security strategy should be among other things, to strengthen the global cyber security resilience and security of national information communication infrastructures as well as seek an end as safe secure and effective operations.

- Long and short-term visions to be accomplished in a given timeframe.

- To reflect and reference overall national security goals (consistent with other strategies).
- Critical infrastructures' owners and other stakeholders to get a sense of their inclusive enterprise in security objectives.
- Translatable into prioritized objectives.
- Priority of these objectives in terms of impact.

The scope.

- Define the business sectors and services in the scope.
- Set the scope base on the comprehensive national risk analysis.
- Well-defined terminologies and appropriately applicable in national context.
- Well-articulated guiding principles and security policies.
- Security in cyberspace infrastructures given priority since from the conceptual design.
- Devise the strategic measures stage.
- Define the framework for implementation.
- Take stock of emerging challenges in new innovations.
- Sovereignty and online child protection considerations.

3.3.2 Implementation phase

The action stage of the NCSS includes, establishing annual objectives, matching the planned settings with organizational structure, and budgeting. The implementation process is iterative and ensures that appropriate measures are executed within a specified time frame. The public, private sectors and other concerned institutions and individuals should work closely to realize the envisioned goals.

Implementation framework

Pursuant to the strategy formulation and adoption by the national leadership, an implementation plan is then developed and carried out. The elements under this category among others, are annual objectives, organizational structure, allocating resources, commitment plan, strategic controls, and continuous improvement; which identify areas for improvement to be addressed through future collaboration. The framework models and organizes activities at higher levels that aid top-level management in expressing the containment of cyber security risk and threats. The frame work should[63]:

Identify – The institutional understanding of information systems, assets, data, and capabilities to be protected; determine priority in light of organizational mission, and establish processes to achieve risk management goals[64].

Protect – Make implementable the appropriate safeguards and prioritize them through the risk management process, to ensure delivery of critical infrastructure services.

Detect – Have the appropriate activities placed to identify the occurrence of a cyber security events and breaches of security.

Respond – Implement the appropriate activities to respond to such incidents, effective planning to take action regarding a detected cyber security event.

Recover - Implement the appropriate activities, prioritized through the organization's risk management process, to restore the appropriate capabilities that were impaired through a cyber security event.

Prior Analysis: The analysis to focus different facets, i.e. to be separated into different components so as to be coherent and justifiable to an end and to efficiently take into account the organizational structure and the varying stakeholders, and

[63] http://www.rhsmith.umd.edu/faculty/lgordon/cyber security/Cyber security%20Risk%20Management.htm. Accessed 02/04/2014 3:30.

[64] NIST Framework for Improving Critical Infrastructure Cyber security.

specific with respect to implementers that may be different from those at the development stage. The more professional and diverse the analysis, the more fruitful outcome expected.

Break down of objectives: These are a long-term achievable set of goals. To make them effective therefore, they should be sub-divided into a shorter composition of the longer terms to aid in allocation of resources and individual objectives are to be pursued by setting specific actions.

Develop a clear organizational structure (governance framework)

The structure of a cyber security's organization is revamped at the strategic level of national planning to manage and protect cyber infrastructures, set the security control and adoptable policies, and govern their implementations. For appropriate coordination, a strategy should include a framework of organizational decisions that justify managerial structure. It is to ensure that the strategy is comprehensive and holistic, preventing the possibility of duplication in effort and resources, with adequate security measure used at the appropriate time and place. This can vary from nation to nation.

The desired process is to establish a chain of responsibility, authority and communication, a strong governance-enhanced partnership, coordination and cooperation ability. A standard management structure could be used such as a RACI (who are **R**esponsible, **A**ccountable, **C**onsulted, **I**nformed) matrix[65]. In this static view, the government is Responsible for cyber security, private sectors are Accountable, expertise and academia are to be Consulted and the public needs to be Informed.

- Who does what? The ultimate responsibility.
- How and when? The management structure.

[65] NIST SP800 35.

- ❖ Cyber security policies and practices established to best articulate operational requirements.
- ❖ Defines the roles, responsibilities and accountability of the related stakeholders.
- ❖ A framework for dialogue and coordination of various activities undertaken in the lifecycle of the strategy.

Lead agency: A given agency, department or any other relevant entity should be responsible for the proper execution of the strategy. It might exist or a new entity would be established, based on the structural and functional systems of governance in a given state. It should be consistent with strategy and facilitate realization of the desired end. In addition, the focal point implementations need to proportionally and accordingly allocate the resources (human, financial, technical and physical). Proper allocation of the resources is a critical part to successful implementation, however control and respect for the commitment endured should not be underestimated. Well-allocated resources heighten performance, address costs and security characteristic demands of the strategic planning schemes.

Strategic controls

The overall national objectives are attained by deploying administrative and strategic controls like quality, monitoring, scheduling, human resources and incentives, project management, performance evaluation and correctness, vigilance etc. Qualitative controls ensure that the plans and the processes are accurate, complete and most effective, monitor the implementation and peruse periodic reviews to determine its performance and assess the progress. It helps to provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, identify, assess, and manages cyber risk[66]. In a broader perspective the following important control are to be noted:

[66] NIST " framework for improving infrastructure cyber security" version 1.0 2014.

- **Establish minimum security requirements:** All users of information systems should minimally adhere to set of predefined controls and cultures. Knowing that the impact levels vary considerably within such systems, the minimum security selection may also vary. Among the security-related areas to model these requirements are: access control, capacity-building and education, as well as risk management.
- **Develop national cyber contingency plans:** Develop and revamp a properly managed system for emergency response and recovery with measures for protecting critical infrastructures to ensure persistent operation in emergency situations.
- **Incident reporting mechanism:** Develop a mechanism for cyber security information sharing and engage in constant monitoring and analysis for prospective threats and vulnerabilities.
- **Risk management:** Managing potential harmful events which can be achieved; efficient use of resources, information sharing, technical and organizational improvement[67].

Threat warning and response can mitigate the damage and easily restore the system and as well to be able to operate under attack.

Challenges that may be encountered

- Interdependency and complexity of what to manage.
- Developing information sharing, emergency/incident response and warning.
- Relating and managing security and resilience.
- All hazard approach (including technical failure).

Areas for Improvement: From the analysis of the current strategic plans of a nation state, the following needs to be strengthened and improved:

- Supply chain risk management.
- Cyber security workforce.

[67]http://www.rhsmith.umd.edu/faculty/lgordon/cyber security/Cyber security%20Risk%20Management.htm. Accessed 02/04/2014 3:30.

- Privacy standards.

Profoundly, in regards to the policy that governs cyber security issues, some philosophical positioning might help: cyberspace characteristics appears to be in favor of attackers, and that no matter what structures and security controls are in place threats and vulnerabilities will always be there and security breaches will occur.[68] The overall stages and flow of control is depicted in a chart (Figure 3.3) below:

[68] Phahlamohlaka, L. J., Jansen van Vuuren, J. C., & Coetzee, A. J. (2011). Cyber security awareness toolkit for national security: an approach to South Africa's cyber security policy implementation. Proceedings of the First IFIP TC9/TC11 Southern African Cyber Security Awareness Workshop (SACSAW), Gaborone, Botswana.

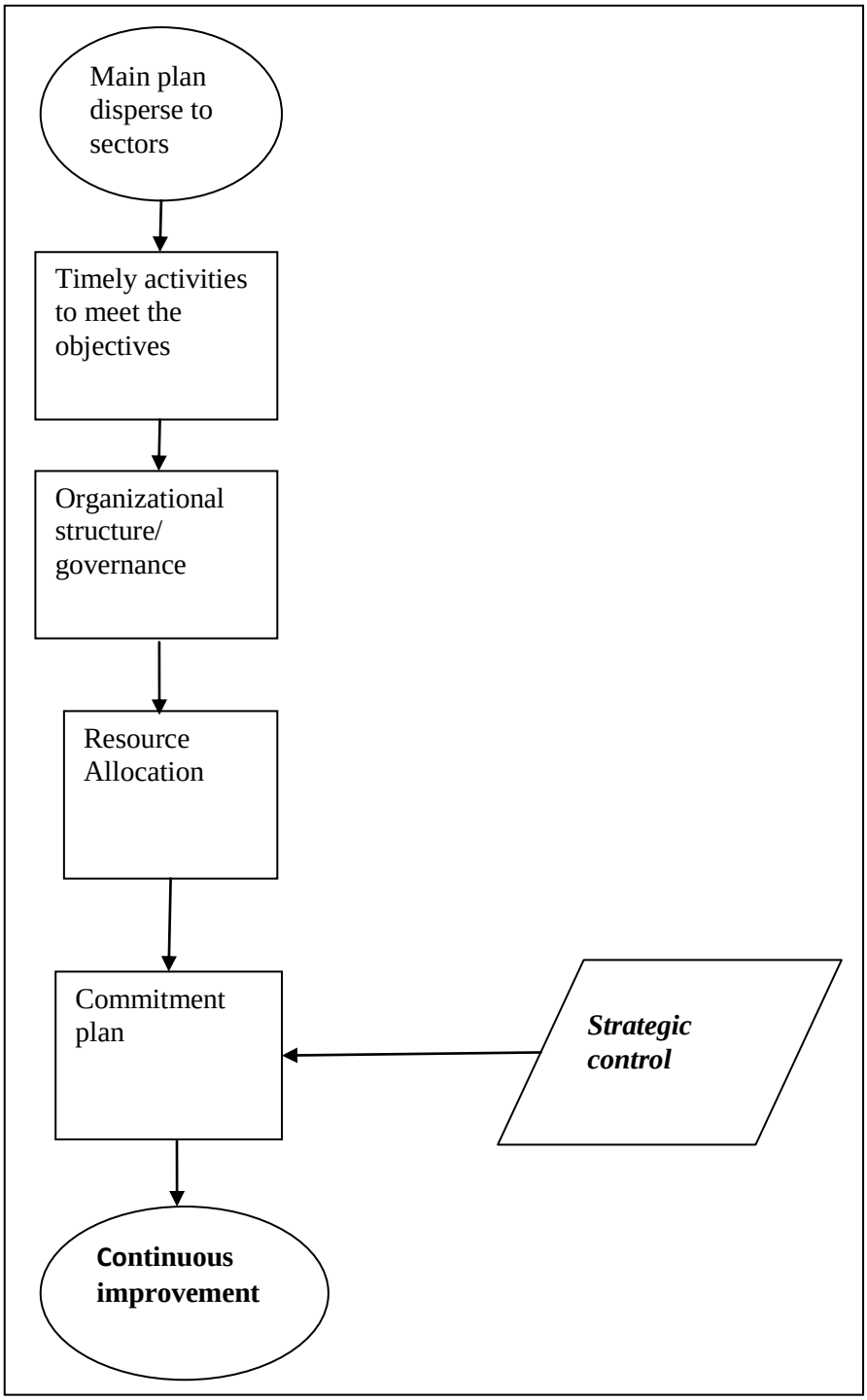

Figure 3.3 Implementation flowchart.

3.3.3 Evaluation and adjustment

The desired strategy that has been developed and implemented is then measured for success and continuous improvement. Define the evaluation of the strategy and specify whose duty it is to perform respective tasks. The achieved result is to be used for enhancing or correcting the actions to better strive toward the aims of the strategy. The range of activities may need to be adjusted as cyber security programs are monitored to ensure that they meet the most current scenarios. Also, cyber security programs require realistic and achievable timescales[69]. The monitoring and measures applied to sectors, services and organizations that will allow security stakeholders to evaluate the performance and seek ways of improvement even when meeting the targeted goals. Information security practices, procedures evolve and the document and policies that underpinned them keep changing, existing measures will cease to have an effect and subsequently new measures need to be developed or adjusted.

Several mechanisms exist to evaluate a strategy and that adhering to a specific one might be doomed to failure, best practice and convertible combination of multiple procedures should be adopted. It is a process to assess actions key goals indicators, checking key performance indicators, continuous improvement through repeatable controls with milestones as a timescale to pinpoint and keep track of events.

Metric / measure and or key performance indicators

To effectively quantify the impact of the strategy and measure the improvement of security within national information and technology systems there has to be various criteria and measures that will be pursued. Though it is apparently difficult to assess, traditional metrics of effectiveness, efficiency and robustness are still applicable. Key performance indicators are metrics but metrics are more dynamic. It can be suggested that employing a metric for the activities of the

[69] ITU National Cyber security Strategy Guide. Geneva: ITU, 2011.

strategy, rather than only the strategy as a whole. The NCSS program is to be tied with meaningful metrics embodied with a comprehensive checklist. In contingency plans and other specific areas, this is to be explicit. Metrics indicate the degree to which security goals are being met; they drive actions taken to improve overall security programs, the security level of specific systems, process or services, and the ability of a nation waking-up to its responsibility of cyber security. There are suggestions that good metrics are those that are SMART, i.e. specific, measurable, attainable, repeatable, and time-dependent[70]. Assessing the threats and the incidents and the controls placed would allow one to deduct why some incidents happen.

Why metrics are used

- How do we know our systems can withstand APT attacks?
- How do we know the program is effective and efficient?
- Ensuring transparency.
- Better understanding and managing: "you can't manage what you can't measure". Says Peter Drucker.
- What is the level of security so far achieved?

Useful metrics

The management of NCSS can choose to use an existing security metrics program or build one of their own, which is more feasible using standards and guidelines for information security metrics from ISO/IEC27004, NIST SP 800-55 etc. If the latter approach is chosen, the following areas need to be thoroughly addressed:

- Defense coverage.
- Vulnerability managements.
- Incident management.
- NCSS Program adequacy.

[70] Shirley C. Payne. A Guide to Security Metrics. SANS Institute Information Security Reading Room, June 2006.

Key performance indicator (KPIs): For reference, below are presented non-exhausted KPIs derived from the strategy facets (governance structure, established policies/principles, contingency plan, risk assessment approaches etc.).

- Number of completed tasks accordingly/timely as specified in the plan.
- Functioning of the established structures.
- Level of trust for ICT uses in the nation.
- Existence of complicating procedures, processes or procedures.
- Risks not addressed by minimum security requirement.

Organize Cyber Security Exercise.

Another strategic action to evaluate a NCSS is simulating incidents and running exercises to test response capabilities that are important to improving the overall security and resilience of Critical Information Infrastructures. In addition to testing the ability of a state or a given sector to respond to a cyber incident it highlights how such can be done in a coordinated approach addressing both human and technical elements of security. Often the exercise are coordinated by a collective union of nations states under a given league/ union e.g. EU or NATO This is due to the fact that problems in one nation can have a tremendous impact on another state as well : as a result in information infrastructures viewed as a whole and as a collection. What is required are exercises that test not only a collection of states' ability to respond to cyber security events, but also the ability of related internal entities, such as organizations, cities and or other industry sectors[71].

The effectiveness of the exercise would be determined by how often it is to be conducted, the number of sectors and expertise/individuals involved, and the plans and systems tested. Though a limited number of individual are involved they should be well-composed to work in a coordinated manner to test and identify weaknesses.

[71] "Cyber Security Exercises: Testing an Organization's Ability to Prevent, Detect, and Respond to Cyber Security Events," by Gregory B. White, Glenn Dietrich, and Tim Goles. Proceedings of the Thirty-Seventh Hawaii International Conference on Systems Sciences, Jan. 5-8, 2004, pp. 170-179.

Steps in conducting a cyber exercise

Each Exercise may vary in its procedure, planning and implementation depending on the scope. However the following steps should guide in organizing the exercise[17]:

- Determine the scope.
- What to be tested.
- Compose the scenario-planning team.
- Draft/select the incident storyline.
- Trace the events leading to the attack.
- Conduct the exercise.
- Provide a report.

Thus, a summary of activities at evaluation stage of NCSS is given below:

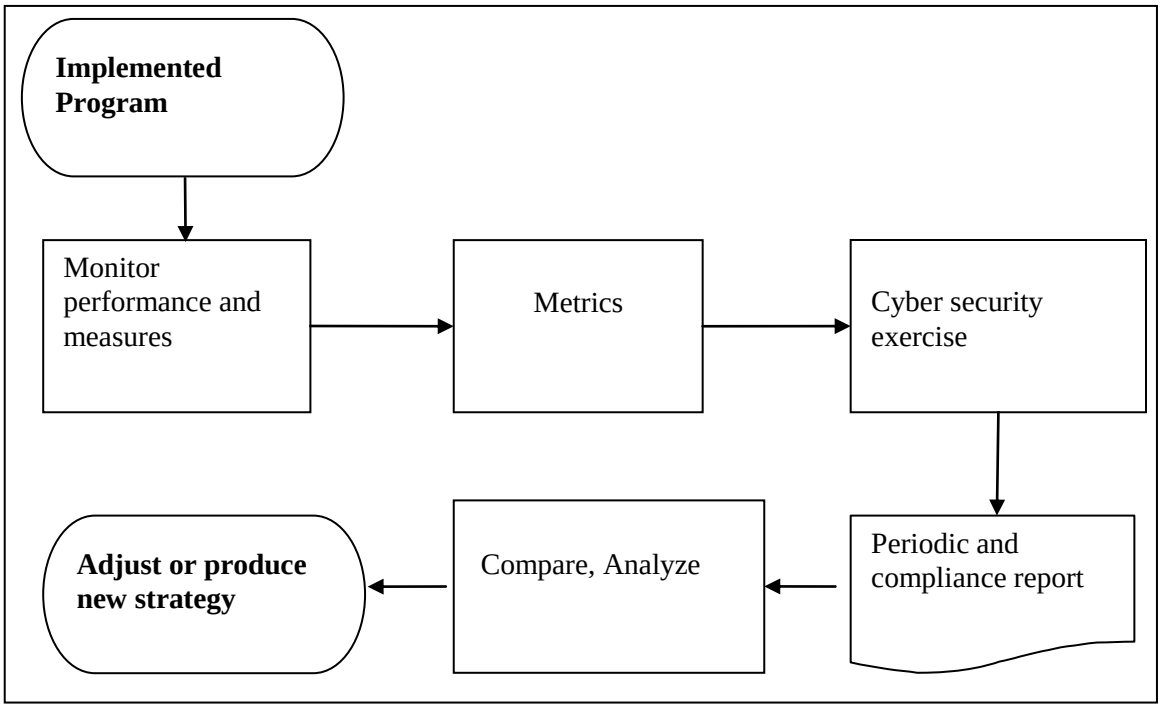

Figure 3.4 An evaluation and adjustment flow chart.

3.4 Algorithm for defining NCSS

NCSS is a methodology that can be used to implement preventive and consequential security controls and policies to effective minimize threats and vulnerabilities. It is based on the given objectives and the potential vulnerabilities. It starts by determining the scope and the high level objective (vision), as the saying goes "Envisioning the end is enough to put the means in motion"- Dorothea Brande. It is impossible to be perfectly secure while in the cyber domains, therefore prepare for the most likely attack by minimizing threats and vulnerabilities. The prerequisite condition is that we have all the necessary (minimally) capacities plus the willingness/determination. Then a risk assessment to be perform as well as predicting the possible attack (including the motives tools and techniques) and re-identifying the critical infrastructures. At the same instance a nation should analyze its specific needs and determine its resource and scheduling requirements and constraints down to each organizations and departments.

For each classified objective upon been prioritized we consider all the possible threats (human and natural) that undermined the resilience and that cause attack on the infrastructure- depriving the objectives. Where there is threats lies vulnerabilities, we dig down to the vulnerabilities to discover the possible exploit so that current security policies and controls can be altered or new ones implemented to minimize these vulnerabilities. We have to assign controls while keeping track of the implementation of the timely line of actions. Assigning controls entails preventive and the consequential measures. Preventive measures determine to prevent attack before they occur by incorporating institutional and basic technical measures and consequential measures; determining the cause of the damage which is necessary to understand what resources the attack was aimed at and what vulnerabilities were exploited to gain access or disrupt system. Then learn from the incident covering all aspect of the attack. Check the adequacy and effectiveness the facets of the strategy and adjust accordingly. Note that in situation where by a nation has no intention to

tackle the issue or not integrated in cyber domain which seems not possible now a day then the whole algorithm makes no effect.

Input : Commitment, support and resources
Output: Trust, resilience and reduced vulnerabilities

National cyber security Strategy

// Bridging the gap, security policies control, objectives and priorities

While integrated in cyberspace
Vision and scope defined
If structure and Capacities exist
Assess risk/ classified infrastructures // ongoing process
For each objectives
Set clear priority and security base line
For every threats
For each vulnerability
Assign Controls
Preventive
✓ Predict possible trends
✓ Legislation and convention
✓ Provide contingency plans
✓ Awareness/ best practices
✓ Specific body or entity // providing early warning
Consequential
✓ Assess impact
✓ Cyber defense league //Analyses attack and devise measures
✓ Implement contingency plan
✓ Additional cooperation
✓ Document and learn
Update intelligence about the threats and vulnerabilities
Line of Actions
Maintain timely implementation of measures
Add the possible missing measures to the strategic plan
Review the strategy effectiveness
If no policies exist // e.g. legal policy
Create new
Adjust accordingly/ update
Not willing or offline/manual system and services use !!!
Exit

3.5 A GENERIC ALGORITHM TO CREATE A CYBER SECURITY STRATEGY

To survive and succeed in cyberspace

Engage cyber Stakeholders
- Define individual and collective accountability
- Understand the value of cyber security

→ **Decide the risks:** *No opportunity without risk*
- Understand generic threats and sources
- Known and unknown risks: *mitigation and resilience*
- Balance risks and opportunities
- Foresight: beyond obvious

→ **Identify cyber security elements**
- Understand cyber security context
- Determine, Analyze and priories gaps

→ **Integration plan/policy framework**
- Operational structure
- Analyze common practices
- Cover digital information chain
- Focal point

→ **SMART Objectives**
- Create target profile
- Consistency with other plans

→ **Agreed approaches/ capabilities**
- People- competence
- Process- best practice
- Technology- tools
- Structure- qualitative services

→ **Operationalize the objectives**
- Effective and efficient management
- Situational awareness
- Proactive, non-linear and multiplayer
- ***For*** known risks- mitigate
- ***For*** unknown risk- resilience against

→ **Prepare and publish a framework**
- Communicate the strategy to concern individual

→ **Return: risk tolerance, safe, secure and effective operations**

3.6 NCSS format structure

The structure of a NCSS is obviously situated between the nation's approaches in dealing with issues and the general framework of strategy. The component and the method of application follow from the elements of the strategy. Hence differences are bound to exist, the major of which is the diversity of the targeted stakeholders. Some NCSSs are precise and lack elements found in others while some mix policies and guiding principles, strategic objectives and visions. However, as we all address a common environment of nearly common courses of action and threats, most NCSSs resemble each other, nations are learning from this and from one another.

Generally and minimally from my analysis a NCSS consists of: executive summary, introduction, the national vision and strategic objectives, the principles and proposed action plan. Furthermore, in a bid to make the strategy more all-inclusive and broader I propose to add some components: glossary of definitions, NCSS relationship with other strategies, proposed implementation hint, national threat landscape and risk assessment, as well as the governance structure recommendation. Aligning closely to the Estonian strategy model as it is comprehensive hence:

- Summary.
- Introduction.
- Threat spectrum.
- National Vision.
- NCSS relation to other document.
- Guiding principles.
- Strategic aims and objectives.
- Action plan and priorities.
- Governance.
- Implementation hints.
- Glossary of definitions.

NCSS PROCESS
The overall procedural roadmap can be summarized as follows:

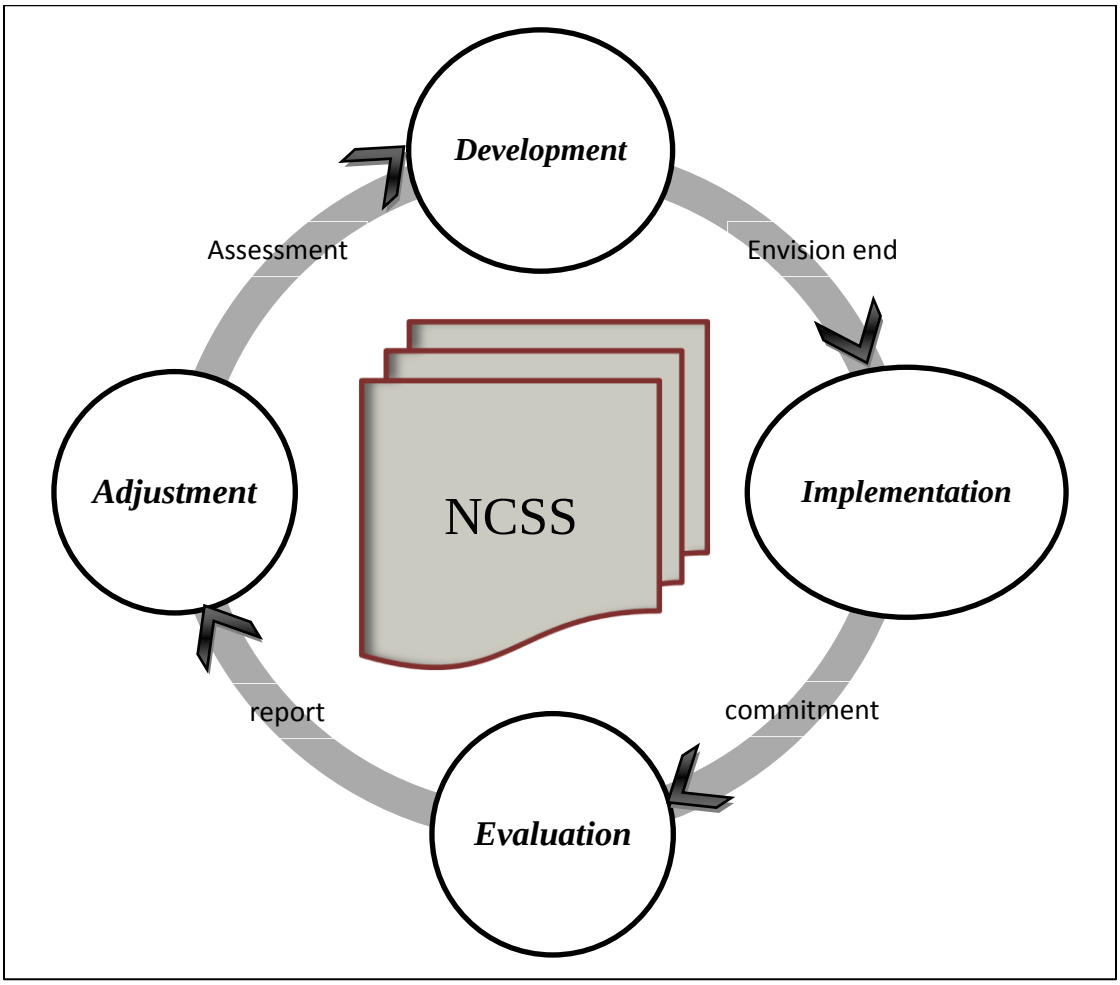

Figure 3.5 Overall NCSS life cycle.

CHAPTER 4. A MODEL NCSS FOR NIGERIA

4.1 Introduction

Nigeria, the most populous nation in Africa, has the second highest internet penetration in Africa, with about 55.9 million users and yet to reach 50% of the population but growing so rapidly[72]. The key economic activities are largely in oil and gas, agriculture and telecommunications; being fast improving and integrating ICT in various facets of economy and governance. The negative influence brought by cyber-attacks and crimes must be noted as well; the estimated annual cost of cyber crime is around $42 m[73], contributing to the degradation of national prestige, threat to national security as well as the threat to education and individual wellbeing. The high statistics, trends and the socio-economic effect is leading to the nation taking steps to increase its security position, but it seems not much is being done because information security is poorly estimated, particularly within the sphere of government officials.

The main concern in securing the cyber domain is that of socio-economic damage. However, the national security is apparently linked with the security of information and communication technology systems in which terrorist groups are taking the advantage to recruit, communicate, and propagate their propaganda and to raise money. Nigeria has a lot of potential but improper use of which leads to the absence/limited cyber-attack defense and controls. Security measures ought to be strengthened in both tactical/operational, organizational and legal areas. Government and all concerned entities are to join hands to maintain and make more realistic the popular Nigerian slogan "Good People Great Nation" by ensuring resilience and trust in the use of cyber infrastructures.

---

[72] 2014 Global digital statistic http://wearesocial.net/blog/2014/01/social-digital-mobile-worldwide-2014.

[73] 2014 the Nigerian cyber threat barometer report.

4.1.1 What has been done so far?

The advent of the internet in Nigeria was in the mid-1990s; then only used by multinational firms, businesses and services which were acquired from the government (Nigerian Telecommunication Company). There was limited use and subscription was expensive and due to a limited area of coverage only elites had received it.

Deregulation of the sectors in the late 1990s enabled private companies and internet service providers (ISPs) to obtain licenses and services became less expensive and ubiquitous. Cybercafés sprang up everywhere and because of the money involved, with much easier tools for attacks and interconnectivity there came cybercrimes ('Nigerian 419', email scamp, fraud etc.). All that while the government watched services being boosted unequally, it did not realize its responsibility in providing the required efforts (e.g. legislations or policies) in securing operations. Security controls were left to be handled autonomously by individual companies until 2003 when a presidential committee was created to investigate the criminal activities that had been perpetrated; coming up with national cyber security initiatives (NCI). The objectives of NCI are to provide public enlightenment on the nature and danger of cybercrime, new legislation to tackle cybercrime, capacity building across law enforcement agencies, establishment of legal and technical framework securing computer systems; networks and critical infrastructures, public-private collaboration to set up guidelines and standards on cyber security and development international law enforcement collaboration.

To realize these objectives, the government set up the Nigerian Cybercrime Working Group (NCWG) in the year 2004; this inter-agency team being made up of different entities mainly from public sectors. The objectives of NCI were focused and due in 2006. The team conducted enlightenment on cybercrime successfully among public and private institutions (NGOs, national assembly, law enforcement agencies) and drafted a computer security and critical information infrastructure protection bill. Moreover, in an attempt to collaborate with different private security companies, a memorandum of understanding was signed with Microsoft Corporation to combat

cybercrimes issues in Nigeria. However, NCWG marginally focused on security of computer systems and networks. Present-day infrastructures are vastly more complex and need dynamic considerations.

In 2006, the Directorate for Cyber security (DFC) under the office of the national security adviser was created and tasked with the responsibility to implement NCI objectives and to coordinate cyber security activities at high level in Nigeria. Among added tasks was the development of framework for CERT and establishment a national computer forensic laboratory. The government started up wonderfully, in 2007 the DFC was funded with a hefty budget of $9.3 million (N 1.2 billion). A recent institutional effort is the creation of the Computer Crime Prosecution Unit (CCPU) under the office of the attorney general in 2010. As part of efforts, ITU also signed a Memorandum of Understanding (MoU) with the Nigerian Communication Commission to set up a Regional Cyber security Centre in Nigeria (July 2013).[74]

Analytically, efforts thought up and drafted were far away from full implementation, lacking a bridge from proposition to implementation. Measures determined to be completed within 2 years are still being struggled with. About seven cyber security related bills have been submitted before the senate and are still pending: computer security and critical infrastructure protection bill 2005, cyber security and data protection agency bill 2008, electronic fraud prohibition bill 2008, Nigerian computer security and protection agency bill 2009, computer misuse bill 2009, economic and financial crime commission act (amendment) bill 2009 and the latest cyber security bill 2013.[75] The DFC that was created in 2006 came to achieve one of its objectives in late 2013, that is setting up CERT Nigeria and is still yet to be functional. Legislation and other facets were supposed to have been handled as matter of urgency.

[74] L. Tomas presentation " cyber security at ITU. "
[75] http://www.internationallawoffice.com/newsletters/detail.aspx?g=fd34fa66-ba56-4426-9f9a-78c2df019ecc.

The initiatives taken so far have reduced some of the perceived problems. The 419 scamp, notably known in Nigeria is now becoming less prevalent. The law enforcement agencies strived in curving this operation. However the present situation needs more viable and comprehensive approaches as many criminals await full development of the proposed 'cashless society' in which without adequate protection as yet unsurpassed damages are bound to occur.

Was it a Success?

Owing to the nature of the information security it is often difficult to access the overall performance of certain measures taken. Nevertheless, one should be convinced that the effectiveness of counter measures can be ascertained. Several questions needed to be addressed: the level of awareness reached, vivid and vibrant organizations constituted, number of expertise provided, number of criminals brought to book, the number of vulnerabilities reduced, and the threats/attacks repelled.

The three main recommendations: raise awareness on cybercrime, pass new legislation criminalizing certain cyber activities, and build Nigeria's institutional capacity to combat cybercrime; have they been met? No; measures taken were one-sided, mostly proposed bills (not yet passed) and that the awareness only targeted top-level officials. Cyber crime awareness should be created to sensitize all users of information systems. Moreover, it is not enough to ensure that the bill is passed but at the same vital point be enforced and executed and recognize the need to create a centre/forum for victims to lodge their complaints. The institutional capacity not yet been reached. Even top officials also acclaim that "Nigeria is still a haven for cyber criminals" said the National Security Advisor.

Nigeria was ranked 2nd as internet fraud perpetrator in the world in 2005, [76] after five years it was down by one position and became 3rd in the top ten list of countries perpetrating internet crimes. The government has been unable to even

[76] 2005 IC3 annual report and 2010 IC3 annual report.

secure its official websites: a number of cases involve defacement of official government agencies' websites (e.g. National poverty eradication program and EFCC websites) which raised to 60%[77]. Nigeria is rich in technology talent, though it is mainly used negatively. Most of these attacks were carried out by hack activists, a threat particularly from unemployed and angry talented citizens. However being a fast emerging market, with a transition to e-economy and e-governance, Nigeria risks higher foreign attacks.

Why has it failed?

The solution is so meager that even recovery takes significant time, measures deployed did not match up to the level of the crime and technological transition. The following are considered key factors;

- Lack of respect for commitment.
- Unnecessary change of appointed personnel.
- Ignorance of cyber security field (cyber crime in particular).
- Insufficient technology and technical skills.
- Initiatives were not comprehensive.
- Lack of concrete governing structure.
- Appointment of incompetent personnel.

4.2 The Strategic context

Threat spectrum*:* Modeling the threat is a prerequisite to establishing priority actions. The ICT penetration (highest internet penetration in Africa 2013), level of economic development, military cyber capabilities, and geopolitical factors would determine our stand. As a nation, cyber threat is not our highest level national threat, rather it is highly prioritized as being an economic security threat rated at a $200 million annual cost.[78] the country is aiming for 70 million internet users in 2015 which further puts our country at risk of further breaches and threats if not handled diligently.

[77] http://techloy.com/2013/01/17/nigerian-government-websites-cyber-attack-report.
[78] http://businessdayonline.com/2013/08/rise-in-cyber-attacks-on-government-website-threatens-e-governance/#.U5eI_vmSxsE.

The national information systems were identified and characterized as not being totally reliant on cyberspace, hence the criticality and sensitivity is relatively low. From the history of attacks and trends in our cyber domain it is clear that cybercrime, hacktivism, cyber espionage and terrorism are the threat sources we have. Based on this, firstly we considered all types of risk and threats with a view to blocking them and reducing the vulnerabilities and subsequently came to the conclusion that cyber crime (spamming, credit card frauds, ATM frauds, phishing etc.) is our priority which affects many of our sectors with important ramifications also seen in educational sectors resulting in significant degradation. To make the model more comprehensive threats from natural disaster and technical failure that might result from negligence is also an added consideration.

Though the strategic assumptions about the threats are not openly discussed in the strategies of many countries, in this study it is useful to provide a hint underlying the threat characterization and assessment. That is, to keep track of how the threat is likely to evolve based on either analysis of trends and events, the type of national-level response mechanisms that exist and what is needed to enhance in cyber security and the level that the cyber-security threats are placed in relation to other national security threats.

We maintain that a risk is a product of threat, vulnerability and the consequence[79]. The threats are not mainly nation states but individuals and a group. Vulnerabilities in our cyber domain are lack of concrete structures and legislations, poor cyber security training or a lack of skills within the technical community resulting in poorly managed and coordinated national infrastructures, limited cyber-attack defense and control and poverty. Reducing or eliminating these vulnerabilities is essential as basically threats actors exploit these vulnerabilities to maneuver an attack on systems. The resulting impact might be micro- (individual), medium (losses

[79] Neil R, Luke G, Veronika H, Kate R. "cyber security threat characterization: a rapid comparison analysis "

to firms) or high- (effect upon gross domestic product, economic damage or loss of national prestige). We weigh this intensity of impact against the ends at stake.

4.2.1 What has induced a lack of cyber security in Nigeria?

There are a number of factors making Nigeria susceptible to cybercrimes and attacks, some of which are peculiar while others are cross-cutting. Lack of seriousness from government, increasing bandwidth and use of wireless technologies and infrastructure, high levels of computer illiteracy, ineffective or insufficient legislation to deal with cyber-attacks and threats. The following list more of it:

- The absence of a comprehensive legal and regulatory framework. Cybercrimes are transnational and perpetrators continue to utilize legislative loopholes, intelligence gaps and jurisdictional issues to their advantage.
- The inadequacy of cyber security skills in law enforcement agencies, government and private sectors.
- Lack of awareness which leads to widespread social engineering attacks.
- Week governance: Unemployment, corruption and poverty rate/low per capita income.
- Lack of standards and national central control (and functional databases).
- Low security controls at a personal, institutional, sectors and national level.
- The absence of widespread industry collaboration.
- Absence of single internet gateway.
- The absence of a national database, making criminals more difficult to track.
- Meager technical (lack of infrastructure) and human capacity and IT skills.
- Poorly made and managed systems.
- Nature of internet.
- New technology comes with no legal standing: The recent emphasis on “Cashless Nigeria”, the increase of online retail stores and e-commerce activity, the growth of e-government initiatives.

4.2.2 The Imperatives for Nigeria

Hence, the country needs:

- Cyber security plans, programs and cohesive frameworks.
- Establishment of well-articulated legal and regulatory framework: Passage of the bill and amendment of Nigerian evidence act, cyber ethics and cyber law.
- Establishment of institutional framework for coordination and implementation; a central authority that will address Cyber Security.
- Address cyber security in more than an economic dimension: securing our cyberspace is therefore critical in order to safeguard national security, economic growth and our way of life.
- Standards and regulations; best information security practices.
- Capacity building: Training, education: establishing forums and IT forums.
- Compliance & enforcement.
- Emergency Response & Readiness.
- Public enlightenment: create and promote awareness among users and all stakeholders.
- Cooperation and Collaboration with local and international experts and organizations.
- Technical measures: farewell, antivirus and antispyware, IP Address tracking.

To define our strategy and provide the framework for Nigeria, the Algorithm 3.4 in chapter is to be utilized to hint out and provide a direction for the proposed model, given below. The central concept is to deal with factors that makes Nigeria Vulnerable, thereby contending the threats and managing the risks.

Algorithm for National cyber security Strategy of Nigeria

// Bridging the gap, employing security policies and controls and realizing objectives base on priorities

While integrated in cyberspace

Secure and maintain reliance of infrastructures and services

Customize and optimize existing structures (DCS, CCPU, CERTS)

Engage all cyber Stakeholders

Government: *Responsible*

Private sectors: *Cooperate and advise*

Academia: *Capacity building and R&D*

End users: *Conform & provide feedback*

International partners: *Alliance and collaboration*

If structure and Capacities exist

Assess risk/ classified infrastructures // ongoing process

Balance risks and opportunities

For known risks- Mitigate

For unknown risk- Resilience against

For each objectives

Set clear priority and security base line

For every threats

Crimes, Espionage, Warfare, Activism, Terrorism, Physical threats, Cyber plagiarism and Cyber laundering

→ **For each attack method (known and emerging methods)**

Social engineering, Phishing, information theft, malware, denial of service, physical disconnection, tunneling, defacement, external intrusions, Scanning and probing, Skimming devices on ATMS, Collusion.etc.

→ **For each vulnerability**

Lack of standards and national Central control, Lack of awareness, Lack of infrastructure, Poor patch management and outdated software, Mis-configured: networks, web applications and software applications, computer systems and wireless networks, Use of weak password policies, use of default passwords and unlocked systems, Lack of cyber security skills assessment, Weak Implementation of Cyber Crime Laws, Inadequate Equipped Law Agencies, poor government regulations, Unemployment and use of contract staff, Poverty, greed and loss of moral standards, inadequate security implementation by third parties Limited cyber-attack defenses and controls , Lack of Proper identification system. Etc.

→ **Assign Controls**

Handle All devises

Oversee all traffic

Control all flows
Touches all users

- ***Preventive***
  - ✓ Predict possible trends
  - ✓ Provide contingency plans
  - ✓ Technical measures: Digital forensic, data centre management, Surveillance, information security expert, higher education, cyber ethics, program, end user education, Compliance and enforcement, providing early warning, Awareness/ best practices
  - ✓ Institutional measures: Implement NCSS, Assign cyber security advisor, enhance focal point, Establish CERTs, enhance partnership, organize cyber exercise, implement legislations and convention, establishing forums and IT forums
- ***Consequential***
  - ✓ Implement contingency plan
  - ✓ Technical measures: Establish redundant systems, filter traffic, increase bandwidth, IP Address tracking
  - ✓ Institutional measures: Engage in wide cooperation, Cyber defense league, Apply legislation, collaborate with security operative centre's,
  - ✓ Document and learn
- ***Updating intelligence about changing threats & vulnerabilities***
- ***Optimization of network/ security policies***
- **Line of Actions**
  - Maintain timely implementation of measures
  - Add the possible missing measures to the strategic plan

Review the strategy effectiveness

People- Competence
Process- Best practice
Technology- Tools
Structure- Commitment and Qualitative services

If no policies exist *// e.g. legal policy*
Create new

Adjust accordingly

Update the overall strategy

4.3 Scope

In Nigeria there is no cyber security strategy, no skilled personnel to handle sophisticated cyber-attacks, no methods and structures to recognize large scale attacks against critical infrastructures organizations. We did not basically designate cyber critical infrastructure that underpins our national security. Therefore, this thesis is a proposed model to take appropriate measures to counter misuse of information and services undermining all elements of information security. Nigeria has peculiar threats from insiders (its citizens). We first address this problem including sub guarding our supply chain to restore our lost glory (international respect).

Perceiving cyber security as beyond secure operation and internet safety; it can be used to combat terrorism to some extent. This Strategy does not seek to address all of the cyber threats at the same priority level and it is to be clear that some meaningful amount of risk would be accepted. A focus is necessary on the most needed security threats to our national development, unity and reputation. The policies and programs, shall address inclusively cyber safety, identity security and privacy.

4.4 NCSS relation to other documents

The NSS of Nigeria mainly focuses on maintaining peace and stability in Nigeria, curving the growing domestic terrorism and crises problems (Political Violence, violent Extremism, Communal violence, and crimes) and did not at all recognize cyberspace as another dimension of threat to national stability. However, NCSS should be viewed as complement to NSS and vice versa: while NSS strengthens the security of our physical infrastructure, NCSS strengthens the security of our virtual space. Having not designated our critical infrastructure, the concept of critical infrastructure protection is not much in use, rather in more generic terms; National assets and infrastructure protection. Nearly all documents/strategies/action

plans have divergent visions and should in addition be inspected to avoid duplication of effort and resources.

4.5 National Vision

Categorically, the goal to be achieved is a *secure, resilient and an open cyber environment; mitigating potential threats that undermine the internet economy and national prestige,* adjusting to appropriate structures and mechanisms and inculcating a sense of responsibility among our teaming ICT users. Taking into consideration the diversity in national values, exponential growth in ICT embracement resulted from automations of our manual systems. We stand to safeguard non impeding innovation and to maximize digital economic security, national development and social prosperity and values.

4.6 Framework conditions

As with every meaningful national strategy, this NCSS has a basis that will reflect a nation's specific values and beliefs and at the same time be internationally relevant. There exist guiding principles to frame decisions to maintain equilibrium between an action plan and the corresponding objectionable consequences. Hence:

- A shared responsibility with more burden on government. Corruption in every nook and cranny of our nation made the society pessimistic, individual and groups adhere less to responsibilities. Government leading by example is an incentive and establish that a shared response is obviously needed.
- Balance of measures and innovation: tools and measures used in counter-terrorism often overrun privacy. Thus balance security with privacy, protecting our societal values, Stimulating economy and maintaining national security.
- Keeping track of international standards: we realized that individual capabilities can only deal with a small portion of the perceived threats; a harmonized collaboration is a key thought to attain maximum security of our infrastructure.

What underpinned the model?

It is obvious that cyber security models vary across countries, the drivers, the threat posture and the approaches in which the problem is managed. Carefully taken into consideration the common ground shared by national cyber security strategies in view to analyses where Nigeria can best fit into the schema. Nigeria has emerging trends in "Cashless Nigeria", electronic identification systems, E-government services and E-commerce.

Hence

- Cyber security is viewed as critical in achieving various national development goals.
- Cyber threats have more consequences on our economic prosperity.
- Cybercrime is the primary threat Nigeria as nation is facing.
- A need to designate and protect critical infrastructures sectors such as banking and other financial institutes, communications and telecoms etc. against major cyber-attacks.
- A desire to encourage coordination and sharing of information among stakeholders.
- Comprehensive cybercrime legislation.
- Cyberspace as a means to preserve stability and national unity.

4.7 Strategic aim and objectives

A stock of the existing capabilities taken and important gaps to be addressed were identified. We may wish to accomplish all the four basic ends that every NCSS dreams of; national security, economic prosperity, social well-being and governance because all together they promote national values and guard our interest. However, we propose to first of all contend with the issues at stake that affect us directly and combating cyber crimes and upholding national prestige.

Objectives

- Making all ICT users aware of cyber crimes and threats and take appropriate precautions: individuals to be informed and transformed, firms to have security plans and policies and government to provide the needed supports and structures expanding expertise and information security awareness. This capacity building promotes a culture of cyber security, reduces the vulnerabilities of ICT, systems and networks and the cyber domain.
- Setting institutional structures to reporting, responding, coordinating and to partner for cyber activities. Create relevant structures in support of cyber security.
- Passing bills and implementing the legal and regulatory frameworks.
- Foster cooperation and coordination between entities locally and internationally.
- Promote compliance with the appropriate technical and operational cyber security standards and policies.

4.8 Strategic measures

Below measures which are presented sequentially, based on priority on the corresponding action specific to achieving and sustaining our goals. The strategy should be aligned with both the national security strategy and policies for economic development. The action depends on national structure, needs and cyber security priorities. The first priority focuses on the enhancement and development of cybercrime legislation that is harmonized and applicable. The second priority deals with organizational structures and policies on cybercrime warning incident management and reporting mechanisms. Priority three, focuses on more tactical/operational security protocols, standards and software accreditation schemes. Thus, cyber concerns include aspects such as policies, procedure, awareness, research and the provision of technical security measures.

4.8.1 Legal measures

Legal jurisdiction over information and telecommunication technology and services is by far and away an urgent facet to secure the interconnected space. Over a period of time policy makers reminded passive observers and just watched how we are transforming to an 'information society', unevenly, the laws and regulations accompany these transitions. The rapid development needs to be consistent with legal policy adjustment. Current situations of the risk in cyber domain are of high profile. All sort of crimes perpetrated offline can be achieved or be aided by using computer systems networks as a tools. There are several draft bills pending in the national assembly which in actual sense are supposed to be passed.[80] This is due to the fact that consequential dangers of not criminalizing vicious conduct in the cyber domain are less known.

Security laws are our first means of deterrence, forcing individuals to act accordingly. It has been a big obstacle that has made it difficult to criminalize activities in the cyber domain. Law enforcement agencies are making substantial efforts in arresting the perpetrators but getting problems in prosecuting the cases. One of these agencies: the Economic and Financial Crimes Commission (EFCC), made nearly 300 arrests related to cyber crime but about 240 of these cases are pending in court due to the absence of enabling legislation.[81] Nigeria urgently needs to pass and execute a bill considering the spate of crimes that are connected to the internet and that the nation is now relying more on ICT than it did some years ago. We ought to take this issue more seriously and provide a quick response that will protect both our Cyberspace and its users.

Actions

1 Cybercrime legislation: It is unfortunate that about ten years after the first draft of a bill and the subsequent seven to eight other bills were made, Nigeria is yet to have a cyber law. The rate at which the government is handling the issue is very slow, as if

[80] T. George ' legislation on cybercrime in Nigeria: imperative and challenges'. A presentation
[81] http://efccnigeria.org/20120416_288%20Jailed.html

cybercrimes are not considered as crimes. Only ICT stakeholders and fewer individuals that know the implication that might result are making calls to action. Moreover, The Cyber Security Bills being forwarded to the National Assembly focus on cybercrime and national security and have no provisions for internet surveillance in which the $40 million Internet Surveillance contract to Elbit Systems invaded citizens privacy.[82] [83] They also had similar purposes and overlapping scopes. In essence they lack clearly defined legislative protocols for protecting Nigerian Citizens and assets in cyberspace, as well as securing national assets without endangering citizen rights or limiting their ability to engage freely online. Therefore, there is the need to review the adequacy of the drafted bills in respect to privacy, data protection, commercial law, digital signatures and encryptions and the process should be composed of as many stakeholders as possible.

2 Government legal authority: As cyberspace is characterized by continuous technical development, the risk of a law, treaty or regulation quickly being outdated is one of the philosophical conditions to be held. The president should be authoritatively empowered to create structures and decisions enabled by a defined act. Our Legislative Session expires every four years and that means cyber legislation stakeholders are faced with the tedious process of sponsoring the passage of the same bill. Also, besides criminalizing activities, we ought to have legal and operational guidelines for engagements and integration of relevant activities.

3 Regional cyber regulations: Since cybercrime does not care about geographical boundaries, a comprehensive legislation can only be achieved through partnership with regional and international union and other cyber security organizations and institutions across the world. Nigeria is a key player in West Africa and Africa as a whole and has the capacity and influence in the activities in both African Union (AU) and Economic community of West African states (ECOWAS). Whereas other regional unions of states like the South African development community (SADC) are

[82] http://ir.elbitsystems.com/phoenix.zhtml?c=61849&p=irol-newsArticle&ID=1810121&highlight=
[83] http://www.premiumtimesng.com/news/131249-exclusive-jonathan-awards-40million-

in the process to have common cyber bills for the respective regions, ECOWAS is yet to gear up towards this development. Although each area may tend to be unique in its perspective, but at least shares a significant amount of the same problems. These wider-reaching cyber-security laws allows the countries to work together and poster effective cooperation. In essence, Nigeria should facilitate the establishment of this measure for ECOWAS to reduce cyber-crime and to secure the key systems and infrastructure in the region and the continent as a whole.

Moreover, upon drafting the appropriate bills there is need of law enforcement and anticrime commissions. The existing agencies and commissions lack capacity to handle cyber crimes and most of which have overlapping responsibilities. A given department is to be responsible for cybercrime and other related matters, the agencies shall be well equipped to be equal to the tasks.

4.8.2 Organizational structure

Institutional measures are our second priority which help to analyze, detect and respond to cyber threats. There are a number of institutional measures taken, but are basically characterized by ineffectiveness and lack coordination (no focal point) and no government oversight. There is nearly no structure that coordinates cyber security and related activities at an operational and strategic level. A response to this is to provide standard national cyber security governance structure in order to effectively protect our national infrastructure and to set the security controls and policies and also to govern their implementation. The need to convince and instill confidence across societies, that the networks and information systems that support the national security and economic wellbeing are safe and resilient. These structures should take into account our political setting, local cultures, peculiar economic threats, country size, ICT infrastructure development and users in consideration.

Action

1. *Roles and responsibilities (the Government's in particular)*

It is to be kept in mind that cyber security is everyone's responsibility because countermeasures only work well if all relevant stakeholders play their part, integrating a wide range of stakeholders which include government, private sectors, infrastructure owners, academia and end users. Collaboration is quite important because neither government nor the private sector can independently control and protect information infrastructure in their midst. The following highlight the stakeholders with respective non-exhaustive responsibilities;

Government: In general governments are held responsible, ensuring creation of strategy to address cyber security, sponsor the program and maintain focus for the defined objective and priorities.

Executives:

- Enunciate roles of cyberspace in national developments and in achieving important national goals and interest.
- Sponsoring and resourcing cyber security programs.
- Manage at high level the institutional and human capacity building activities.
- Sign relevant treaties and conventions.
- Justify the Nigerian position on cyber security in Africa and the Globe at large.

Legislative, judiciary and law enforcement agencies

- Develop acceptable and applicable legislations.
- Use legal power and incentive to ensure that all stakeholders are committed to their responsibility.
- Support the executive and parliament.
- Ensure that the strategy does not obstruct other aspects such as national norms, civic freedom etc.
- Law enforcement can advised and make effective the enforceable laws.

Parliament

- Ensure secure use, importation and development of technology.
- Trigger NCSS. Though legislation may do the same by passing laws.

Private Sectors: Their contribution and engagement is critical because of their economic impact to a nation. A given regulation might be in place that impelled information infrastructures owners and operators to comply with security requirements. A willing and voluntary participation would be more prepared drawn from the vivid challenges that we are facing as a government or as private investors.

Critical infrastructures owners and operators

- Sharing knowledge and expertise.
- Contribute to incident management.
- Showing how to balance efficiency and profitability with cyber security.
- Assisting in CERT.

Intelligence community

- Partners, allies.
- Watch and warning for threats and vulnerabilities.

Vendors

- Maintain and improve security in the supply chain.
- Helps in Vulnerability reduction efforts.

Academia

- Human and institutional capacity building.
- Research and development.
- Host CERT.

End user

- Appropriate use of cyber infrastructures.
- Adopt basic precautions.
- Support the initiatives.

2. ***National cyber security agency***

The directorate of cyber security is currently the apex agency that oversees cyber security activities. However, its capabilities are limited and should be made to be a multi-agency body with additional structures and capacities. It should unify the operational cyber security activities of government department and ministries and also leads to collaboration with private sectors. It also addresses performance and security characteristics of existing information and communications systems and infrastructures as well as strategic planning for the future, incorporating standards, research and development and supply chain risk management.

Governance: This is a structure for policy development, coordination and implementation of operational activities related to the national cyber security mission across the executive branch down to organizational level i.e. setting up institutional coordination, control and response mechanisms. This basically includes the review of overlapping missions and responsibilities as a result of authorities being vested on various departments and agencies. The strategy should be governed by a structure: a National Cyber Security Coordinator (an office that direct all cyber security activities in government) reporting to the president. An accountable multi-agency body (Directorate of cyber security) serves as a focal point for coordinating cyber security activities, all ministries that are responsible for different aspects of cyber security report to this directorate.

The national centric CERT to be established as a governmental body governed by the ministry of education with the support from various experienced security organizations and personnel (more importantly private). There should be an intelligence community situated within military command that should be central to all aspects related to critical infrastructure protection and to serve as a provision for cyber warfare in the near future. This seeks to make provision for the separation of control of private networks and that of the critical national assets (security sector) in a situation where the need may arise. Figure 4.1 depicts the structure:

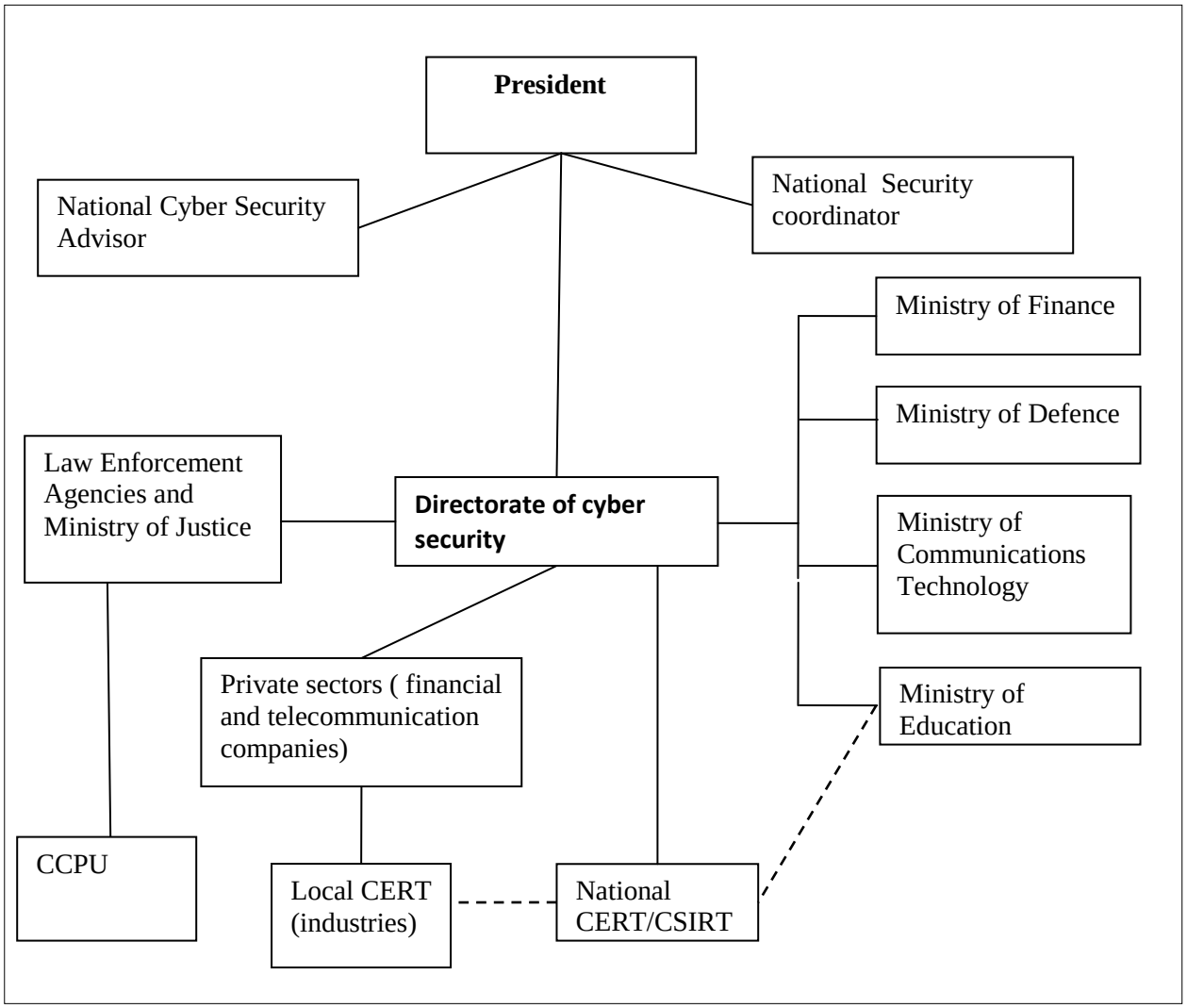

Figure 4.1 Proposed cyber security governing structure.

3. **Partnership:** Partnership shall take place in three dimensions: local, regional and international. Locally (within our national boundary) government departments/agencies and private sectors are to work collectively so as to efficiently exchange and share expertise and real time information about threats and vulnerabilities. A form of information sharing mechanism between public and private sectors to better understand manage the rapidly changing information system domain. This additionally would pave a way for easier incident reporting and handling.

However, as geographical or political boundaries are not an obstacles to conducting cyber-attacks an efficient international cooperation is paramount. Regionally, collaborate with like-minded states to enhance the security situation and to have a harmonized cyber security legislation, policies and framework.

At international level there are lots of conventions that are supposed have been be signed and an additional partnership to collaborate with relevant organizations to use collective defense in countering cyber threats. In this aspect there have been some commendable efforts achieved; Nigeria being a member of the International Multilateral Partnership Against Cyber Threats (IMPACT), the Organization of Islamic Cooperation (OIC), the International Criminal Police Organization (INTERPOL) etc. However, additional efforts are worth striving for, like getting membership in the Forum for Incident Response and Security Teams (FIRST), Global Prosecutors E-Crime Network (GPEN). Among the conventions that are important is to sign the Budapest convention on cyber crime. In addition, the existing bilateral treaties between Nigeria and a number of countries should be well articulated to address issues on cyber security.

Coordinated response pyramid: Cyber security or national cyber security in particular is a broad issue and responding to which of course entails a range of activities at different levels. It needs coordination and response at international level, regional and national level (central authorities, states, private entities and local authorities and individuals). Furthermore, at national level the multi-agencies and multi-stakeholders coordination foster the 'whole-of-government' response. In essence what is needed is collaboration, coordination, corporation and conformity. The needs to merge efforts and resources across the federal government and the system to implement a veritable national cyber security policies.

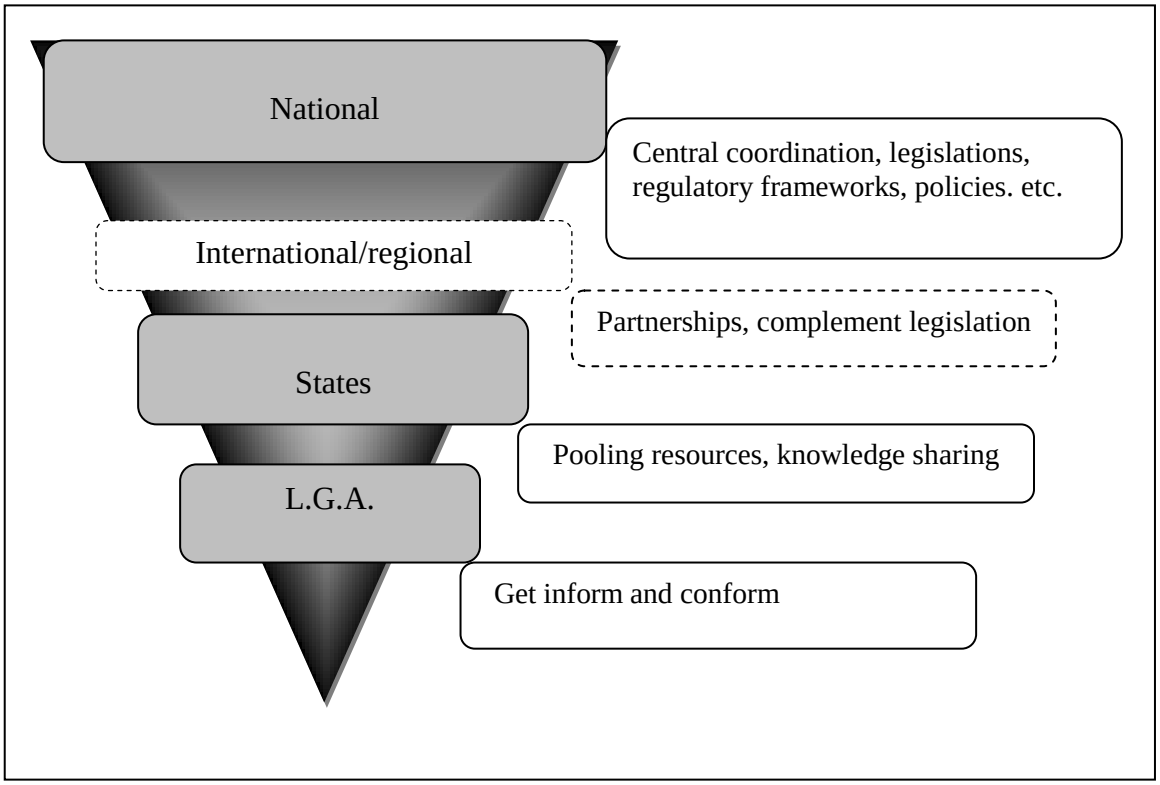

Figure 4.2 whole of government' and 'whole of nation' response.

4. Capacity building

One of the main reasons that fuelled the increase in cybercrimes and cyber threats in our society is exponential increase in the use of ICT and broadband which means more users are having access to and are exposed to the web. Many of these users, unfortunately, do not have an insight as to how to protect themselves, their personal information, and their gadgets against cyber-attacks. Millions of these users are liable to be harmed by unsophisticated and avoidable attack techniques. These small systems of junk operated by the inexperienced users add up to the count of botnets and together pose a serious threat to the society at large.

It seems not enough is done in this regard, therefore, we need a capacity building that will include the overall scale of resources, activities, and capabilities required to secure our systems and to become a more cyber-competent nation. This element will typically include skills and training, research and development, public education and awareness, overall culture of cyber security, and all other activities

that allow the government to interface with its citizens and workforce to build secure digital information and communications infrastructure for our nation.

The skills and training programs are necessary to bridge the gap in technical and managerial expertise. It appears that that the financial sector and other e-business companies usually receive adequate training. But government, law enforcement agencies, regulatory authorities and other critical infrastructure operators have deficiencies in this regard. There is also the need for information security courses spanning to the general public as adequate education and skills can reduce poverty; engage youth in entrepreneurship and self-employment. To this end, this will also provide certification to the unemployed youth and lead to creation of cyber security jobs. Hence the cyber security skills framework should among other things investing in cyber security education and research.

These can be attained by adding fundamentals of information security and cyber security awareness to the national education curricula in primary, secondary and tertiary institutions; a way of spreading knowledge to users and the general public. These result in human and institutional capacity building: as comprehensive user training and education minimizes the compromise of information systems. At the core of this awareness initiative must therefore be the realization that no foolproof technical protection is possible in a socially constructed space; good conduct and security consciousness are the key. The programs ought to target cooperation, end-users and other stakeholders, because currently it is these users that are the main concern regarding cyber incidents. Enterprises are security conscious and typically more protected relative to others and to home users.

National structures responsible for cyber security must also lead the capability building processes that will ensure collaboration on an international level to achieve the goals identified by cyber security policies. There should be a center for cyber security to coordinate awareness programs among higher institutions of learning and to employ other programs like organizing annual cyber security campaigns, launching a website/forum solely for awareness. This sustainable nation-

wide campaign and the programs would go a long way to reducing compromise of information assets.

As part of a model for the capacity building, users must be forced to adhere to a reasonable use of cyber domain via policies, guidelines and procedures where applicable. Then they will be predisposed to a sort of awareness training and education. These are effective in building a "human firewall". Figure 2 illustrates more of this:

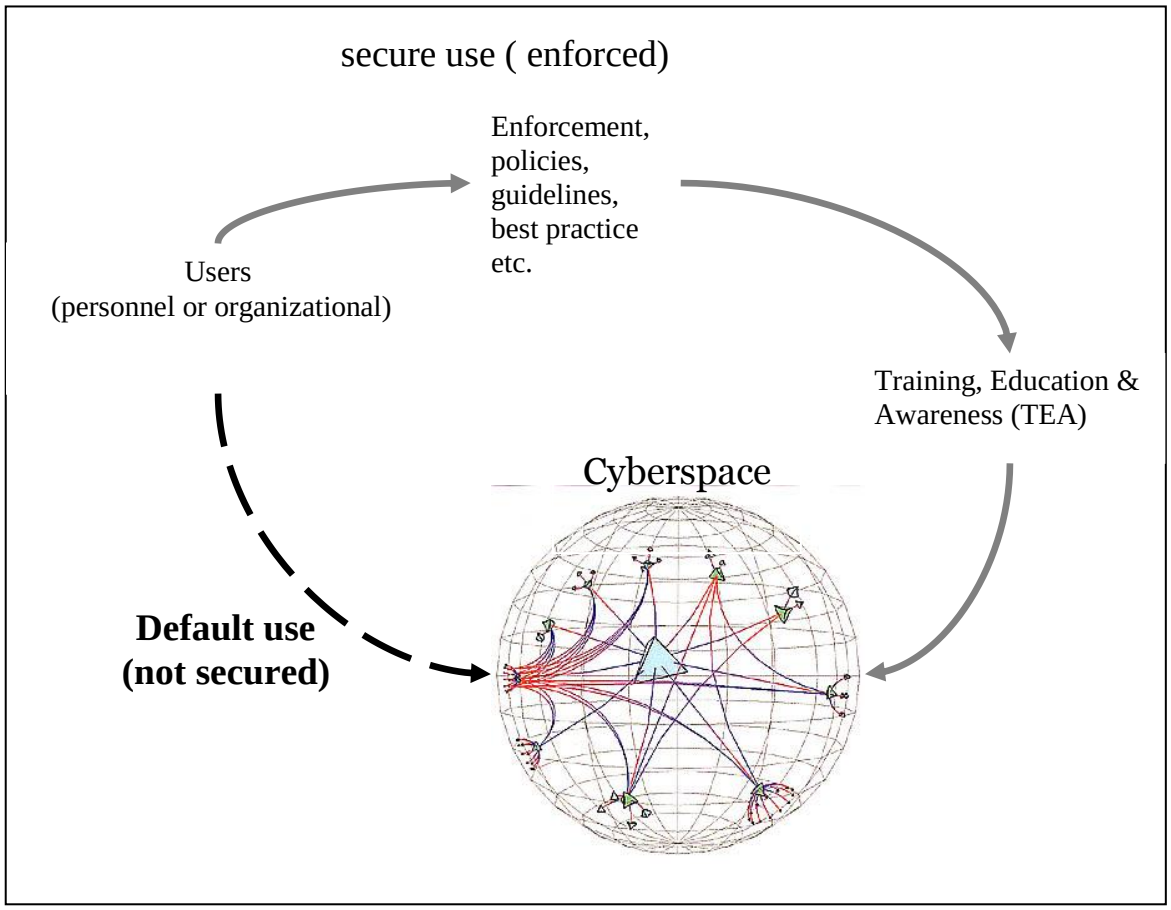

Figure 4.3 A way to a secure use of cyberspace.

4.8.3 Technical and procedural measures

Notably there seems to have been a change in both public and private sectors adopting world best practices and use of biometric authentication, though relatively

inadequate. The use of chip and pin based cards significantly reduced the magnitude of fraud, but then came a threat of information theft as well as others. Coordination and increase in usage of the best practices from organization to individual is deemed to enhance the security. Agencies are to be equipped with the state of art infrastructures for tracking and tracing and to enhance security controls. Cyber criminals and other actors are continuously evolving with various techniques. It is very important to keep up with these ever changing techniques. The deployment of proactive measures and the use of modern technological tools is aimed at preventing, monitoring and investigating the menace. The Internet cafes that became prolific and the vast amount of users all make a good use of antivirus software, frequent update and patches, which further strengthen them from being a target by hackers and botnets operators.

Most of the breaches are not discovered in time or not at all. Lack of tools contributed to this in addition to the prevalence of software piracy which make most of the systems prone to attacks. The majority of the users do not want to purchase or update to a legal version. Unemployment or under-employment and corruption to say the least are contributing toward this attitude.

Harmonized information security standards adoption is on the rise, but the rate of this change is not very encouraging. For example, there are few public and privately implemented ISO27001 standards: National identity management commission, galaxy backbone company and internet service providers. A good practice like this shall be encouraged and expanded.

Actions

1 Minimum security requirement, standards and compliance

Norms of Behavior to be inculcated among users of ICT which will include those elements from law, regulation and technical standards and undertakings, as well as consensus-based measures, such as best practices, that collectively define standards of conduct in cyberspace. A few worth noting:

- Adoption best practices. Any ICT infrastructure should integrate basic security.
- Institutional controls.
- Standards (ISO, NIST, PCIDSS etc.).
- Counter software piracy.
- Biometric means of identifications.

2 Single internet gateway

It is not enough to set up points of access to telecommunication networks, but regulations and enforcement. Internet Service Providers (ISPs) often for one reason or another find it effective to use international internet connections to exchange traffic. Nigeria's main sources of international bandwidth companies, major ISPs and mobile operators are not part of the Internet Access Point of Nigeria (IXPN). This access point or gateway is meant to connect all Internet traffic originating from Nigeria to the rest of global internet community and should have been a really harmonized single entity that would allow the government the full right to monitor all traffic that goes through this gateway without passing through any intermediary either inside or outside the country.

3 Facilitation of national database

The national database initiative should employ infrastructures and cyber services that are reliable, maintainable, and robust and secure, while the need to protect systems and valuable information coexist and are harmonized with the protection of the rights and privacy of individuals. A comprehensive national

database could aid in tracking down the criminals by checking into past individual records and tracing their movements.

Moreover, there should exist the establishment of a centrally-managed crime database to serve all security agencies. Currently, there is no proper coordination among security agencies in the country in the handling of security related issues particularly concerning cyberspace.

4.9 Means

The diplomatic, jurisdictional, technological and human resources should be devoted or required to achieve the stated goals by fully implementing the action plans. It should be part of the implementation plan for security reasons. Among these means, the diplomatic capability is well established in which Nigeria enjoys relative influence among African States. However, this seems not to be being utilized accordingly. Security is an art and a science as well involving common sense, research, risks management and design. Hence, all sorts of resources available shall be mobilized. Figure 4.4 (The effective cyber security tackling in Nigeria) below

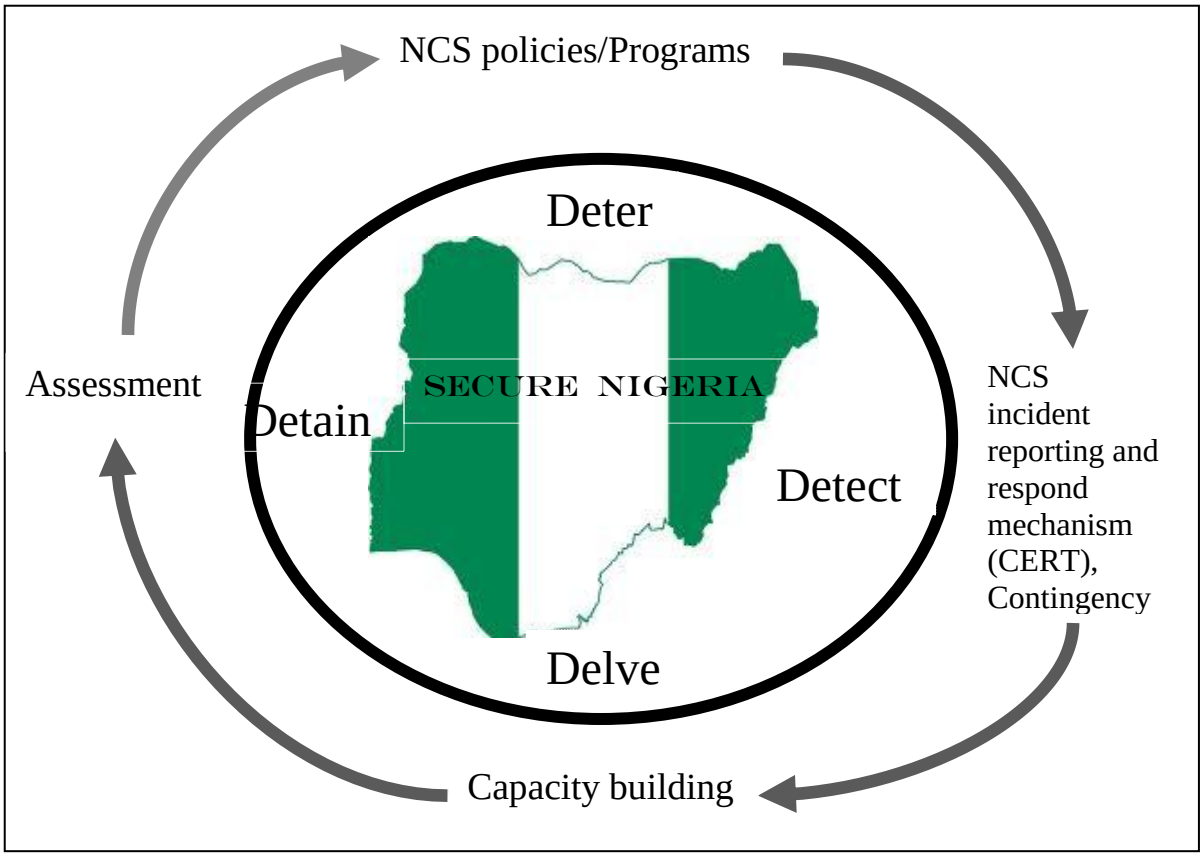

Figure 4.4 The effective cyber security tackling in Nigeria.

4.10 Implementation hints

Implementing a comprehensive strategic solutions to cyber security requires the development of an implementation plan in support of the approach to guide the activities. The strategic document is the starting point that defines the problems and risks intended to be addressed as well as plans for tackling those problems and risks, allocating and managing the appropriate resources, identifying different organizations' roles and responsibilities, and linking (or integrating) all planned actions.

Upon being adopted, the implementation shall be coordinated by the apex office of the cyber security coordinator based on the implementation plans developed by the working group, relating to the different developmental plans. Proper

consideration shall be given to the concrete actions and funds needed to achieve the objectives of the Strategy. The efficiency and effectiveness of the strategy will be assessed by submitting a timely report to be preferred concerning the implementation progress detailing the success towards realization of the objectives.

Realizing IT as a strategic imperative for national development and harnessing its immense benefits, the Government shall give considerable attention and provide a commitment and resources, both financial and otherwise, for not only realization of the National IT vision but in similar proportion a secured avenue for this to prevail.

4.11 Glossary of definitions.

One of the prerequisites for achieving a sound framework is a common understanding of core concepts and how are they are related. Broader concepts relative to the terms used within the strategic documents would be preferable, however, cyber security related issues have been kept untouched in Nigeria while committed to promote the level of IT usage and penetration. Hence, to maintain a globally relevant and Nigerian harmonized contextual focus, definitions from International Standard Organization would be adopted. Though, there has been different interpretations based on context, author's or individual reader conception. A harmony in this regard would clear confusion and ease collaboration.

- **Cyberspace**

  Is a dynamic set of interconnected systems consisting of hardware, software, services, media and human users?

- **Cyber security**

  "Preservation of all elements of information security (confidentiality, integrity, availability etc.) and services in Cyberspace"

- **Information systems**

  Any set of systems used to handle (collect, store, process, deliver) information which may include applications, services or other information handling assets.

- **Critical Infrastructures**

  Systems, assets and/or services, whether physical or virtual, so indispensable to the society that the incapacity/destruction, interception of which would have a negative impact.

- **Information security**

  "Preservation of Confidentiality, Integrity and Availability (C-I-A) of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved."

CHAPTER 5. CONCLUSION AND RECOMMENDATIONS

5.1 Conclusion

Research has been carried out in information security/information assurance with important breakthroughs but they usually turn out to address specific aspects (technology). However, despite this effort a number of incidents increasingly occur with much devastating effect which points to the fact that technology can only solve a small portion of the problems. Strategic cyber security reduces cyberspace vulnerabilities and helps in consequential management of incidents for at least the foreseeable time. The transformation of cyber security from organization to nation state, the involvement of well-resourced actors targeting critical infrastructures and the return on investment in cyber espionage induce an urgent call to National strategy to secure cyber operations.

The key differences observed in the nations' approaches to strategic cyber security originated from the initial aim (cybercrime, cyber warfare or espionage), the level of development in ICT and societal values. Moreover, understanding of NCSS scope contributes to the divergent structure. As noted, there was insufficient international collaboration and rapid recognition of security in cyberspace in this decade.

Nigeria is just started to harness the era of information technology, along with increasing usage of it in commerce, communication, electronic banking and payment systems. This increase in individual and cooperative usage together with power of computing is a strong indication of additional threats. Nigeria expresses interest in cyber security but insufficient actions taken and initiative primarily focus on cybercrime legislation. Hence, the model in this thesis is a making model of a strategic national cyber security proposed to Nigeria for a dynamic and comprehensive resilience in cyber domains. It is the responsibility of government to make hey while the sun shines to strategically secure this fourth domain (cyberspace) as with land, sea and air.

5.2 Recommendations

However, a note that this thesis present a possible guideline that could be used and is not meant to be an exhaustive list as the cyber domain continuously expands its horizons on every dimension. Its' contents and entries could be varied, expanded on and applied at different government levels and institutions pertinent to the context assumed. Much emphasis was given to the developing countries, typically Nigeria. The following are recommend in regards to the model:

- The establishment of CERT.
- Review of cyber security bill to acknowledge privacy and freedom. Passing the bill, implementing as well as its immediate enforcement.
- Needs for comprehensive research and development into cyber offense and defensive capabilities.
- To structure a nation that is aware of challenges and importance of cyber security.
- As a nation (Nigeria) we have the needed resources and capabilities to handle our problems, a minor assist may be of help. But it is an additional threat to solely depend on foreign nationals or governments.
- Viewing cyber security as an end, aim for an absolute security and attempting to accomplish much in a short instance is a key to failure.
- Cyber threats affect everyone irrespective of location and size. It has become a fundamental need.
- Planning and implementing cyber security for both countries, organizations, and individuals.

BIBLIOGRAPHY

Edwin Leigh Armistead "The Development of IO/IW Curriculums in the United States: A Review of Current Efforts and a Case Study From Norwich University" ICIW proceedings paper. 2012, p12.

Fischer, E. A. (2009). Creating a national framework for cybersecurity: an analysis of issues and options. New York: Nova Science Publishers.

D. Evans, "The Internet of Things—How the Next Evolution of the Internet Is Changing Everything," Cisco Internet Business Solutions Group (IBSG), April 2011.

Gercke, Marco. (2009) *ITU/Understanding Cybercrime: A Guide for Developing Countries*. Rep. International Telecommunications Union.

Goodwin, Cristin Flynn; Nicholas, J. Paul (2013), Developing a National Strategy for Cybersecurity: Foundations for Security, Growth and Innovation, Redmond, Microsoft Corporation.

Gregory B. White, Glenn Dietrich, and Tim Goles (2004)"Cyber Security Exercises: Testing an Organization's Ability to Prevent, Detect, and Respond to Cyber Security Events,". *Proceedings of the Thirty-Seventh Hawaii International Conference on Systems Sciences*, Jan. 5-8, pp. 170-179.

James A. Lewis and Katrina Timlin, Cyber security and Cyber warfare. Preliminary Assessment of National Doctrine and Organization, (Geneva: UNIDIR, 2011), http://www.unidir.org/pdf/ouvrages/ pdf-1-92-9045-011-J-en.pdf.

J. Lewis and K. Timlin, "Cyber security and Cyber warfare: Preliminary Assessment of National Doctrine and Organization", Center for Strategic and International Studies, Washington, DC, 2011.

John K. Bartolotto (2004)" The origin and developmental process of the national security strategy" U.S. Army war College http://history.defense.gov/docs_nss.shtml.

Kenneth G "Strategic cyber security", NATO cooperative cyber Defence centre of excellence Tallinn, Estonia. 2011.

Luiijf, E., Besseling, K. and Graaf, P. (2013) 'Nineteen National Cyber Security Strategies.' Int. Journal of critical infrastructures, Vol. 9, Nos. 1/2, pp. 3-31.

Marti Lehto, *(2013) "The Ways,* Means and Ends *in* Cyber Security Strategies*" Proceeding of the European conference on information Warfare. P182.*

Neil R, Luke G, Veronika H, Kate R. (2013) "Cyber-security threat Characterization: A rapid comparative analysis ." RAND Corporation.

Phahlamohlaka, L. J., Jansen van Vuuren, J. C., & Coetzee, A. J. (2011). Cyber security awareness toolkit for national security: an approach to South Africa's cyber security policy implementation. Proceedings of the First IFIP TC9/TC11 Southern African Cyber Security Awareness Workshop (SACSAW), Gaborone, Botswana.

Rain Ottis, Peeter Lorents (2010) "Cyberspace: Definition and Implications" Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia.

Shirley C. Payne. SANS Institute 2007: Infosec Reading Room. "A guide to Security Metrics". SANS Security Essentials GSEC Practical Assignment Version 1.2e. June 2006, 3-7.

Strate, L. (1999) "The Varieties of Cyberspace: Problems in Definition and Delimitation." *Western Journal of Communication*, Vol 63, No 3, pp. 382-412.

Thomas C. Wingfield, Eneken Tikk (2010) "Frameworks for International Cyber Security: The Cube, the Pyramid, and the Screen". International cyber security legal and policy proceedings p 16-22.

Tikk E, " Comprehensive legal approach to cyber security" PhD desertion faculty of Law, University of Tartu, Estonia 2011. http://dspace.utlib.ee/dspace/handle/10062/17914 (last visited Oct 13, 2013).

Tikk E., Kaska, K. and Vihul, L. (2010) International Cyber Incidents: Legal Considerations, Cooperative Cyber Defense Center of Excellence (CCD COE), Tallinn.

Klimburg, Alexander, ed. *National Cyber Security Framework Manual*. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, December 2012.

Australian Attorney-General's Department, Cyber Security Strategy (Canberra: Australian Government, 2009).

White House, The National Strategy to Secure Cyberspace (Washington, D C: White House, 2003) .

German Federal Ministry of the Interior, national plan for information infrastructure protection 2005.

Germany Cyber Security Strategy for Germany (2011).

Estonian Ministry of Defence, Cyber Security Strategy (Tallinn: Estonian Ministry of Defence, 2008).

Indian Ministry of Communications and Information Technology, Discussion Draft on National Cyber Security Policy (New Delhi: Government of India, 2011).

National cybersecurity strategy*:* Cyber Security policy of South Africa (2012).

The White House: International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World (2011).

Information Security Doctrine of the Russian Federation: Approved by President Vladimir Putin on September 9, 2000 (2000).

ITU, The World in 2013. ICT Fact and Figures, (Geneva: ITU, 2013).

Norton Cybercrime Report, September 2012, page 6 http://www.norton.com/2012cybercrimereport;

ENISA, Guide book on National cyber security, 2012.

ENISA, National Cyber Security Strategies. Practical guide on development an execution, 2012.

ITU, ITU National Cybersecurity Strategy Guide, (Geneva: ITU, 2011), http://www.itu.int/ITU-D/cyb/ cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf.

ENISA, National Cyber Security Strategies. Setting the course for national efforts to strengthen security in cyberspace, (Heraklion: ENISA, 2012).
http://www.enisa.europa.eu/activities/Resilience-and-CIIP/ national-cyber-security-strategies-ncsss/cyber-security-strategies-paper/at_download/fullReport.

ITU National Cyber security Strategy Guide, (Geneva: ITU, 2011).

NIST " framework for improving infrastructure cyber security" version 1.0 2014.

ISO/IEC FDIS 17799:2005(E): Information technology Security techniques - Code of practice for information security management.

NIST SP800 35: Guide to information technology security services.

National strategies and policies. NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia. *http://ccdcoe.org/328.html* Accessed 27/12/13 20:03.

Global digital statistic http://wearesocial.net/blog/2014/01/social-digital-mobile-worldwide-2014.

The Nigerian cyber threat barometer report. 2014.

Organization for Economic Cooperation and Development (OECD) (2012), Cybersecurity Policy Making at a Turning Point: Analyzing a New Generation of National Cybersecurity Strategies for the Internet Economy, Paris, Organization for Economic Cooperation and Development (OECD).