NATIONAL CYBERSECURITY STRATEGY

FOREWORD BY THE NATIONAL SECURITY ADVISER

The emergence of cyberspace, a virtual global domain, is increasingly impacting almost every aspect of our lives. The domain is transforming our economy and security posture more than ever before, creating opportunities for innovations and the means to improve general welfare of the citizens. It is transforming many countries' growth, dismantling barriers to commerce, and allowing people across the globe to communicate, collaborate and exchange ideas.

However, behind this increasing dependence on cyberspace lies new risks that threaten the national economy and security. Sensitive data, networks and systems that we now trust can be compromised or impaired, in a fashion that detection or defence can be hard, thus undermining our confidence in a connected economy.

The Federal government is not unmindful of the diversity of implications of the nation's risk exposure in cyberspace, hence we have put in place cohesive measures towards addressing national risks effectively now and in the immediate future. Furthermore, the government has recognized that for Nigeria and its citizens to continue to benefit from the full potential of information and communication technology revolution, we must take the cyber-risks seriously. It is on this premise that we are determined to confront the threats, uphold and support the openness of the cyberspace as well as balance security with respect to privacy and fundamental rights. If we fail to prepare now and act appropriately, we may be faced with future challenges that will be more complex to manage.

In this context, government has developed a National Cybersecurity Strategy as cohesive national measures towards addressing the challenges. These measures contain strategic initiatives and programs that are aligned with the national doctrines, principles, vision, goals and objectives as enshrined in the National Cybersecurity Policy. The strategy recognizes three key approaches to a successful national cybersecurity engagement: public private sector partnership; stakeholders' collaborations and international cooperation.

Our commitment is to ensure continuity of government in the advent of cyber threat emergency, safeguard critical information infrastructure, and nurture national cybersecurity readiness through the engagement of all stakeholders.

It is in the light of the above that my office, in collaboration with other agencies of

government and key actors from the private sector are championing the urgent need for comprehensive national cybersecurity programmes. It is my hope that the synergy already developed between the stakeholders drawn from different backgrounds will be sustained through all the implementation stages. My office will continue to explore common grounds around which we can sustain this collaboration on cybersecurity for the common good of our country.

We shall keep all channels open for close monitoring and evaluation of the implementation of this policy, which shall be due for comprehensive review in another five years. My office shall facilitate regular collation of feedback from stakeholders that will enhance periodic review of the process.

I therefore wish to express my appreciation to the cross section of contributors and stakeholders, including professional bodies, corporate leaders and captains of industry who have contributed to our efforts towards creating an enduring safer digital environment for our dear country.

M. S. DASUKI CFR.
National Security Adviser

December 2014.

TABLE OF CONTENTS

Chapter Five:

NATIONAL INCIDENT MANAGEMENT STRATEGY

Chapter Six:

STRATEGY ON CRITICAL INFORMATION INFRASTRUCTURES PROTECTION

Chapter Seven:

STRATEGY ON ASSURANCE & MONITORING

Chapter Eight:

NATIONAL CYBERSECURITY SKILL & MANPOWER DEVELOPMENT

Chapter Nine:

STRATEGY ON ONLINE CHILD ABUSE & EXPLOITATIONS

Chapter Ten:

STRATEGY ON PUBLIC-PRIVATE PARTNERSHIP

Chapter Eleven:

STRATEGY ON NATIONAL INTERNET SAFETY

FIGURES

EXECUTIVE SUMMARY

The economy of a modern Nigeria is anchored and sustained on two major infrastructural landscape (i.e. Physical and Digital) working together to sustain critical and non-critical sectors of the economy in Government, Manufacturing, Dams, Defence, Chemical Sector {Oil and Gas}, Power and Energy, Commercial Facilities, Financial Services, Food and Agro-allied, Emergency Services Transportation Systems, Public Health and Healthcare Sector, Water and Waste Water systems. Digital infrastructure is the National Information Infrastructure (NII) component that permeates the physical infrastructural landscape supporting it to function seamlessly, endlessly and sustainably. The NII is the backbone of the nation's active presence in cyberspace. Significant disruption of its operation will undermine the confidentiality, integrity and availability of essential national services, which will be inimical to national economy and security.

In comparison with other industrial and commercial entities, the Internet has been with us for a relatively short period of time. It has been responsible for the most revolutionary and rapid changes to the way we communicate, undertake business, perform job functions as well as boost our military strategies. We have seen the examples in the home schooling, social media and cloud computing rising on the tails of the Internet phenomenon.

The Internet has given the phrase "global village" an appropriate meaning, this is driven home with the illustration that an individual in Nigeria can immediately set up an online conference call and chat with group of people on the other side of the planet in real-time. The majority of users of the Internet conduct their activities in a legitimate and above board manner, while on the other side of the internet there are individuals, organisations, foreign intelligence agencies and state sponsored actors that have used the very benefits of the internet, i.e. its speed, global presence and openness, to carry out criminal activities that can cause havoc to those that are not aware, prepared or equipped to deal with such undertakings.

This document therefore examines the strategic imperative of a national cybersecurity. It highlights various strategies that will be used to implement the measures outlined in the new National Cybersecurity Policy.

These include the following:

- The development and implementation of appropriate legal framework, with initiatives that will allow for the identification and prosecution of cybercrimes that impact Nigeria regardless of whether they originate within Nigeria or are launched from outside of the country. It encompasses training the judiciary, security and law enforcement agencies, seeking international co-operation, public and private sector co-operation and public awareness programmes. It also introduces a special focus on data protection, privacy and lawful interception.

- Establishment of a National Incidents Management Strategy which outlines the commissioning of a National Computer Emergency Response Team (CERT) and introduces the roadmap for implementing Detective, Preventative and Response capabilities to deal with cybercrime activities.

- The strategy for Protecting Critical information Infrastructures including shared responsibility between government and owner operators of critical infrastructure. It also highlights the ways in which early warning, detection, reaction and crisis management will be assessed, developed and implemented to provide a proactive readiness to react to and deal with threats towards Nigeria's Critical Infrastructures.

- The strategy seeks to ensure the development of information security assurance and monitoring plan. It includes a new national mechanism on cybersecurity assurance, adoption of fit for purpose standards for Governance, Risk and Control, Core Assurance Capabilities, National Enterprise Architecture Framework. It also endorses the adoption of application security testing as well as the adoption of a Balanced Scorecard Framework for cybersecurity.
- The introduction of a sustainable strategy to develop, maintain and ensure Nigerians are informed and equipped to deal with cybersecurity events by establishing a mechanism for Cybersecurity Skill and Manpower Development initiatives. These initiatives will be driven through public-private partnership. It introduces a model for certification of individuals to ensure quality of competence in the field of cybersecurity relevant to the nation.

- The strategy for protecting Nigerian Children from Online Child Exploitation and Sexual Abuse includes initiatives, such as the national awareness programmes through multi-stakeholder engagement, and international cooperation in the countermeasures.

- The Strategy on Public-Private Partnership highlights the need for interagency collaboration with private sector. It engages the framework for a public and private partnership in developing a cohesive response to mitigating cyber-risk.

In conclusion, The National Internet Safety initiative is aimed at providing general public awareness, education, and advocacy through multi-stakeholders' engagement, development of local tools, training software and applications in Internet safety and security readiness. It provides mechanism for gauging the nation's cyber security posture.

December 2014.

CHAPTER ONE

AN OVERVIEW OF NATIONAL CYBERSECURITY STRATEGY

1.1 Introduction:

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

1.1.2 The NCSS comprises of short, medium and long term mitigation strategies covering all national priorities, addressing the nation's cyber risk exposure. Specific key cyber threats worldwide inimical to National interest are identified. Such as;

i. Cybercrime
ii. Cyber-terrorism
iii. Cyber conflict
iv. Cyber espionage
v. Child online abuse and exploitation.

1.1.3 These threats have significant capability to damage the integrity of the nation, disruption of critical information infrastructure operations, undermine government operations and national security.

1.1.4 The NCSS articulates, coordinates and guides the country in the implementation of National Cybersecurity Policy and cohesive counter-threat measures for the protection, security and defence of National Cyberspace.

1.1.5 The Strategy provides various initiatives for the focused areas and national mechanisms for developing and implementing Legal & Policy Measures, National Incident Management, Critical Information Infrastructure Protection, Cybersecurity Assurance Framework, Manpower Development, Child Online

Abuse & Exploitation, National Internet Safety, Public Awareness, Multi-Stakeholder Partnership and Global Cooperation on Cybersecurity.

1.2. National Cybersecurity Vision:

The National Cybersecurity Policy has set out a clear purpose, direction and outcome of the country's engagement in cybersecurity.

What is the Nigeria Cybersecurity Vision?

A safe, secured, vibrant, resilient and trusted community that provide opportunities for its citizenry, safeguard national assets and interests, promote peaceful interactions and proactive engagement in cyberspace for national prosperity – Culled from National Cybersecurity Policy 2014

1.3. The Aim of National Cybersecurity Strategy:

The aim of the NCSS is to provide a cohesive roadmap, initiatives, and implementation mechanism for achieving the national vision on cybersecurity.

1.4 Cyberspace Within the Context of National Prosperity & Opportunities:

1.4.1 Cyberspace offers excellent platforms and opportunities for securing and growing the nation's economy.

1.4.2 Every citizen that is connected to cyberspace through the internet is immeasurably impacted and empowered for actions.

1.4.3 In the next few years, Nigeria will become a broadband economy where every individual and corporate citizens will have unhindered wholesome access to the internet.

1.4.4 Cyberspace will become the mainstream for national integration and digital economy empowerment. It is a knowledge driven space with massive capacity to bridge gaps in mobility, commerce, innovations, education, poverty reduction, and economic empowerment.

1.4.5 What is the Cyberspace?

Cyberspace is an interdependent network of critical and non-critical national information infrastructures, convergence of interconnected information and communication resources through the use of information and communication technologies. It encompasses all forms of digital engagements, interactions, socializations and transactional activities; contents, contacts and resources deployed through interconnected networks. – Culled from National Cybersecurity Policy 2014

1.4.6 Why is Cyberspace important to the National Government?

It has been established that we have the contemporary four (4) domains of land, Sea, Air and Space, Nigeria recognizes Cyberspace as the fifth (5^{th}) domain for driving critical national functions such as economic development, commerce and transactions, social interactions, medical and health, government operations, national security and defense.

1.5 Impact of Cyber-Risk on National security and the Economy

1.5.1 The nation's digital economic existence relies on the effective functioning of digital infrastructure. In Cyberspace, the country is not isolated but interconnected to other countries and active actors within cyberspace through interdependent networks of information infrastructures. Thus, the country is exposed to predictable and unpredictable risks.

1.5.2 Just as we have actors with legitimate intentions so also exist other actors with illegitimate and malicious intentions. Within the global network of networks there are critical structural flaws which can be exploited for criminal intents and purposes against the country to compromise the confidentiality, integrity, availability and accessibility of the nation information systems and critical information infrastructure.

1.5.3 Vulnerabilities exist within cyberspace that can be used to exploit national economic interest and constitute threats to National Security. For instance, recent compromise of some government websites, growing underground cybercrime industry, emergence of activism through online backdoors, fraudulent practices, incidence of online exploitation of the young segment of the population, gross abuse of the social media for waging malicious campaign against the state, conflict and violence perpetuated through internet, economic sabotage through distributive denial of critical services, coordinated cyber espionage, malicious intrusion into computer systems and other digital devices, cyber piracy and stealing of intellectual assets, cyber-terrorism, online financial crime and money laundering, distribution of offensive contents and child abuse materials and hosts of other malignant activities committed through cyberspace are all inimical to the wellbeing of the country. The economic impact is destructive to any nation.

1.6 Cybersecurity within the context of National Security Strategy:

Providing security for the critical information infrastructure and other critical components of information system within the current state of affairs is a huge national challenge.

National Security needs the infusion of a cohesive framework on cybersecurity to provide holistic approach to the current and future security landscape, because the nation security and economic terrain is fast paced and is moving towards a digitally enabled and mobile terrain.

State and non-state actors involved in cyber-crimes are adequately equipped with sophisticated cyber tools to cause damage with unprecedented dimension.

The security inclusion of cyberspace domain will help the country prepare and response to such security threat and help address the country's weakness in her own digital vulnerability, as well as strengthening our ability to provide countermeasures in partnership with other legitimate state and non-state actors. This is the strategic rationale for the development of National Cybersecurity Policy and the context within which National Cybersecurity Strategy is articulated for national security readiness.

CHAPTER TWO

UNDERSTANDING NATIONAL CYBER-RISK EXPOSURE

2.1 Introduction

In line with the national doctrine on cyber-risk exposure as reflected in the National Cybersecurity Policy document, the country presence in cyberspace exposes it to a new dimension of risk. Therefore, development of the country's Cybersecurity Strategy is approached from examining security risk exposure of the whole country.

What Is Cyber-risk?

Cyber risk is the possibility that a threat and vulnerability exists within the nation's cyberspace inimical to the security and safety of information systems and associated infrastructures. Furthermore, it is the possibility that the threat will exploit a vulnerability to breach the safety and security of an information system and or information networks or infrastructure.

National cyber-risk has two (2) major components:

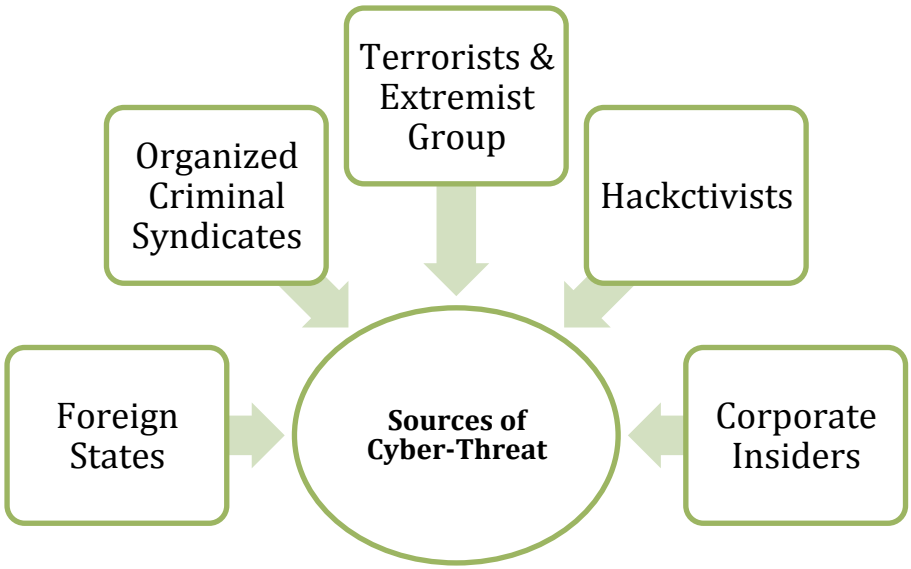
i. Cyber-threat
ii. Vulnerability

2.2 Cyber-threat Landscape & Impacts:

2.2.1 Cyber threat is the possibility of a malicious attempt to damage or disrupt the operations of a vulnerable computer network and information system.

2.2.2 The nature and the dimension of the impact of cyber-threat are diverse and it involves a **threat actor** who performs a pre-mediated attack or exploit circumstances of an accident. A threat actor is engaged by a **threat source** either clandestinely or tactically. A threat source initiates a desire to breach access to critical information or security controls with the purpose of benefiting from the breach, for example for financial gain or competitive advantage in the case of industry cyber espionage.

Sources of Cyber-threat



NCSS Fig. 1

2.2.3 **Cyber threat** is escalated to **cyber-attack** by a **threat actor** where a deliberate effort is initiated to exploit the vulnerability of computer systems, information and communication networks, and internet driven processes for criminal intent and malicious purpose.

2.2.4 It usually involves the use of malicious codes to alter digital codes, logic or data, resulting in disruptive consequences that can compromise the confidentiality, integrity, and availability of data and lead to manipulation of information systems and internetwork infrastructure.

2.2.5 Cyber-attacks may lead to the following consequences: Identity theft, fraud, extortion, Malware, pharming, phishing, spamming, spoofing, spyware, Trojans and viruses, manipulation of hardware, denial-of-service and distributed denial-of-service attacks, breach of access, password sniffing, system infiltration, website defacement, private and public web browser exploits, instant messaging and social media abuse, and intellectual property theft.

2.2.6 Economic Impact of Cybercrime

- Recently, a total of $388billion USD was estimated as the approximate total financial loss to cybercrime in more 24 countries in the last six years.
- The global black market in marijuana, cocaine and heroin combined ($288bn) and approaching the value of all global drug trafficking ($411bn).
- At $388bn, cybercrime is more than 100 times the annual expenditure of UNICEF ($3.65 billion).[1]
- Physical crime are becoming digital. More criminals that were involved in traditional crimes are moving towards the Internet. They know that it's easier, more profitable and the probability of being caught is lower

1

- Nigerian financial consumer loss to Cybercrime in 2010 stood at N2,146,666,345,014.75 ($13,547,910,034.80) to cybercrime in 2012[2]
-

2.2.7 Cyber threat landscape is diverse and diffusely driven by state and non-state actors.

State Actor:

The State Actors are established and well organised to carry out the most sophisticated threat in the cyberspace with the goal of exploiting computers and information and communication networks to gather intelligence on government, military, industrial and economic targets, and opponents of their Regimes. They gathered intelligence data and information which can be used for spreading falsehood and disrupting critical services. Sometimes they install hidden malicious software on a system can be adapted to suit an attacker's changing objectives, lying hidden within the system in readiness for exploitation during times of increased tension or conflict.

Non State Actors:

Organized and unorganized criminals operating in the underground economy exploiting weakness in individual, corporate and government systems and information infrastructure. They used different technology and psychology method to manipulate users and engage highly sophisticated cyber tools to infect, hijack, control and extract value information for criminal purpose. Financial motivation is usually the driven force of this particular non-state actor. They inflict huge financial damage on their victims. Their action damage country reputation and inflict huge collateral damage on the country financial system.

Terrorists and extremist engage resources of cyberspace to perpetuate against the government; falsehood, communication, recruitment, indoctrination, raising of fund activists and distribution of extremist contents. They are active attackers and constitute one of the major threat to national security.

[2] ***Economic Cost of Cyber Crime in Nigeria*** *by Gbenga Sesan, Babatope Soremi and Bankole Oluwafemi as part of the output for the Cyber Stewards Network Project of The Citizen Lab, Munik School of Global Affairs. University of Toronto and Supported by international development research centre.(IDRC)*

Activist with unwholesome pattern of obtaining information used against established authorities. They operate through social media and vulnerable backdoors, usually connecting with an insider with passive attack tendency.

2.2.8 The National Cybersecurity Policy document has identified and classified five (5) major cyber threats as inimical to the national security strategy. These threats have significant capability to cause considerable damage to the integrity of the country's economy.

2.2.9 The underlying ideology of this National Cybersecurity Strategy is to proffer relevant strategic frameworks and mechanisms for addressing these cyber-threats, securing the nation in the advent of cyber-attack, while preparing the nation for a proactive engagement towards building and nurturing a safe and secure cyberspace where trust and confidence are hallmark of Nigeria cyber-community.

2.3 Imperative of a National Vulnerability Assessment

2.3.1 Vulnerability is the structural weaknesses of the nation's information systems and critical information infrastructure ranging from technical flaws, porous measures, to human negligence.

2.3.2 The NCSS requires that national vulnerability assessment be conducted towards determining weaknesses in government information systems, websites, networks, data handling processes and vulnerabilities existing in the nation's critical information infrastructure.

2.3.3 The national vulnerability assessment helps the government appreciate the level of her unpreparedness, the need to safeguard huge investments in information systems and communication infrastructure and commitment made to global partners National ICT developmental goals.

2.3.4 There are efforts aimed at addressing some of these challenges at the sectorial levels. However, NCSS is laying a foundation for the coordination of the country cyber-ecosystem with a unified framework on cybersecurity.

2.3.5 The ultimate goal is to build a collective counter-measures mechanisms that will facilitate the country's capability in addressing the huge vulnerability gaps among the states information systems, critical information infrastructure, and protection of our presence in cyberspace.

2.4 Gauging the Impacts and Opportunities

2.4.1 There are many advantages associated with the implementation of the national Cybersecurity strategy. Building and nurturing trust and confidence in the use of national information systems and critical information and communication technology is crucial to the socio-economic well-being of the citizenry, therefore it is important to secure our nation in cyberspace thereby infusing high level of confidence and trust in the nation digital economy.

2.4.2 The nation depends on the functioning of information and communication technology and the operation of critical information infrastructures. Our interactions, transportation, communication, trading and e-commerce, financial services, mission critical services are relying on the confidentiality, integrity and availability of information flowing through these infrastructures.

2.4.3 National enterprise security architecture is further enhanced with the inclusion of cybersecurity strategy. A new and holistic National Security Architecture will emerge by integrating physical and cyber security as countermeasures against external threat, thus consolidate the country readiness capability.

2.4.4 The country's emerging opportunities as a result of her trusted presence in cyberspace are inclusive of the following;

- A resilient digital economy, stimulating innovations, wholesome engagement, development and inflow of foreign direct investment.

- An opportunity to exploit cyberspace to advance the country's military capability in engaging external threat, conflict, violence and terrorism.

- Nigeria’s readiness to defend her citizens, safeguarding operations of critical information infrastructures and extra-territorial jurisdiction in time of unpredictable cyber-attack, ensures continuity of critical operations amidst adversaries.

CHAPTER THREE

NATIONAL READINESS STRATEGY

3.1 National Cybersecurity Policy Direction

3.1.1 The National Cybersecurity Strategy defines the nation's readiness to safeguard and prepare the whole Nation in advance for global economic competitiveness in cyberspace. It also addresses willingness to empower the nation in building a comprehensive, coherent, structural and procedural capabilities at strategic and tactical levels in mitigating cyber risks.

3.1.2 The strategy involves engagement of government and non-government actors, employing multi-stakeholder's principles of approach, inclusive of all participatory and partnerships of government, industry and other stakeholders.

3.1.3 The critical success factor of NCSS is hinged on comprehensive mobilization, engagement and coordination of critical components towards securing our presence in cyberspace and protecting critical information infrastructures.

3.1.4 The direction of the policy of government on cybersecurity is in agreement with regional and global direction on securing cyberspace.

3.1.5 The paramount focus of the cybersecurity strategy is addressing our cyber risk exposure, protection of our national critical information infrastructure, exploiting cyberspace opportunities for national security and economic goals, and the enthronement of a trusted cyber community remain a paramount focus of the National Cybersecurity Strategy.

3.2. Necessity of a National Cybersecurity Strategy

3.2.1 The multi-dimensional nature of the evolving security threats is moving the current National Security Strategy beyond the traditional scope.

3.2.2 The nature of the current security threats such as cybercrime, violence, conflict and terrorism increasingly exploits the openness and borderless nature of cyberspace. This constitutes a threat to our growing dependence on cyberspace.

3.2.3 Government is leading a coherent national response towards reducing the impact and escalation of cyber threats in a manner that safeguards the nation's presence and guarantee trust and confidence in our connected economy.

3.3. Objectives of National Cybersecurity Strategy

3.3.1 The Strategy aims are to set out a national roadmap with various coordinated mechanisms; harness implementation framework; and actions that will guarantee attainment of the National vision, mission and goals on Cybersecurity as captured in the National Cybersecurity Policy.

3.3.2 Therefore, the Strategy is needed to achieve the following specific objectives:

i. A comprehensive cybercrime legislation and cyber-threat counter measures that are nationally adoptable, regionally and globally relevant in the context of securing the nation's cyberspace.

ii. Provision of measures that protect critical information infrastructure, as well as reducing our national vulnerabilities through cybersecurity assurance framework.

iii. To articulate an effective computer emergency response capability.

iv. National mechanisms on capacity building, public awareness, skills empowerment is necessary to help strengthen our capability so as to respond promptly and effectively to cyber-attacks.

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

vi. To deter and protect government from all forms of cyber-attacks.

vii. To coordinate cybersecurity initiatives at all levels of government in the country.

viii. To build national capabilities against cyber threats with coherent cooperation through public- private sector partnership and multi-stakeholder engagement.

ix. To promote national vision on cybersecurity through awareness, partnership through shared responsibilities and a trusted community of stakeholders.

x. To promote coordination, cooperation and collaboration of regional and global stakeholders on cybersecurity.

3.3.2 The Strategy is further aligned with National Security Strategy and other relevant government documents most especially National ICT policy and National broadband plan.

3.3.3 The Strategy defines the basis for a coordinated national and globally compatible framework for action, cooperation and approach to protecting national critical information infrastructure against cyber threats.

3.4 Scope of National Cybersecurity Strategy

The scope of the national cybersecurity strategy covers the areas of national priorities as well as general framework for partnership and international multi-stakeholder cooperation on cybersecurity.

3.5 Approach, Guiding Principles & National Priorities

The NCSS approach involves coordination of the nation's cybersecurity constituents and public-private partnership which are consistent with the objectives and the guiding principles as encapsulated in the National Cybersecurity Policy.

3.6 Governance Strategy

3.6.1 The implementation of the provision of the strategy will be coordinated through the Office of National Security Adviser in collaboration with other relevant government agencies.

3.6.2 The central coordination model will operate in synergy with federated structures toward achieving comprehensive measures on cybersecurity.

3.6.3 Central coordination model is adopted in line with international best practices and has recommended in the global framework for cooperation on cybersecurity

3.6.4 The sustainability and critical success factor of this governance model is anchored on public-private sector partnership, multi-stakeholder engagement as well as regional and international cooperation.

CHAPTER FOUR

LEGAL FRAMEWORK INITIATIVES

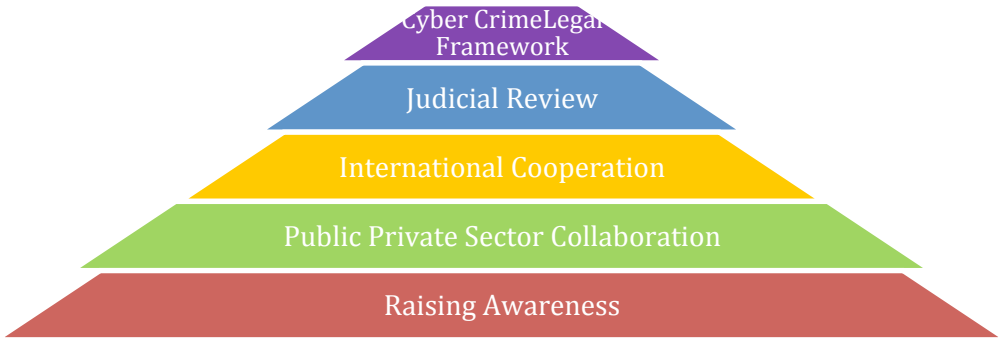
4.1 Objective

4.1.1 The objective of the Cyber Security Legal Framework is to identify the strategy required to ensure areas defined in the Cyber security Policy are implemented, managed, sustained and effective in combating cybercrime in Nigeria.

4.1.2 To achieve this aim, a number of immediate and long term legal framework initiatives will need to be developed, agreed, funded and rolled out to accomplish success.

4.2 Approach

- The approach takes the form of referencing aspects of the Legal Framework in the cyber security policy with a view to prescribing the initiatives that will allow for the implementation of each of the detailed areas.



NCSS Fig 2 Initiatives Pyramid

4.3 Initiatives:

4.3.1 Initiave1: Enacting Fit for Purpose Cybercrime Legislation

- As prescribed in the cyber security policy, fit for purpose legislation will need to be enacted and implemented to combat cybercrime.

- The main focus of this initiative will entail a root and branch review of Nigeria's current and draft cybercrime legislations.

- The objective of this exercise will be to identify any gaps between what is currently available and what has been proposed in the Cyber security policy with a view to updating any omissions or redundancies so that when the legislation is enacted , it will be adequately effective , workable and flexible enough to deter and prosecute cybercrime activities

- This initiative supports a strategy to enact a number of separate and distinct legislations that will make up the cybercrime legislative framework as opposed to a single legislation that has the banner of cybercrime legislation.

- To the barest minimum, the following legislations will need to be included in the new cybercrime framework: Anti-Spam, Child Online Protection, Child Pornography, Cookies, Computer Misuse, Cyber Blackmail, Cyber bullying and Harassment, Cyber Espionage, Cyber Terrorism, Digital Evidence and Preservation, Data Protection, Data Retention, Hacktivism; Identity Theft, Information Security, Intellectual Property Rights, Lawful Interception, Online Fraud, Privacy, tribalism and Xenophobia, Software Piracy, Security Breach Notifications, Unauthorized System Interference etc.

- Aligned to the review and enactment of the cybercrime legislative framework is the need to put in place measures to keep the laws up to date and effective.

- The strategy to achieve this will include the establishment of a Cyber Crime Legislative Review Committee (CCLRC) whose purview will be to advise the National Security Advisor, Legislature and regulatory bodies on aspects of legislations that needs to be amended to ensure current legislations do not become redundant, unenforceable and ineffective.

- This is an immediate initiative and needs to be given special priority as it forms the bedrock of the applicability, enforceability and prosecution of individuals and organisations that breach key segments of the National Cyber Security policy.

4.3.2 Initiative 2.

Preparing and Revamping the Judiciary for Cybercrime Legislations

- Nigeria's current judicial environment is not adequately equipped to handle sophisticated cybercrime cases. In order to ensure the new cybercrime legislations are effective in the prosecution of alleged cybercrimes, when they are brought before the courts, it is the strategic objective of NCSS to ensure the Nigerian Court system is equipped to handle cybercrime cases.

- In fulfilling this strategy, the following initiatives will be undertaken

  a) Capacity building for Judges and lawyers on the new cybercrime laws
  b) Courts will be equipped to handle digital forensic evidence
  c) Provide law enforcement agencies with the processes and procedures for investigating cybercrime activities.
  d) Capacity building for law enforcement and security agencies on digital forensic capability.

- This will be achieved by developing a home grown fit for purpose certified programme of training courses, capacity building, awareness programmes and materials for current Nigerian judges and lawyers.

- The strategy will also include the incision of new cybercrime legislation courses in institutes of higher learning so that newly qualified lawyers have a basic understanding of Nigeria's cybercrime framework.

- This will be a long term and on-going initiative.

4.3.3 Initiative 3: International Co-operation

- To ensure our cybercrime laws are effective and internationally harmonised, the legal strategy is to adopt the provisions of the convention on cybercrime to enable effective cross border law enforcement.

- This will allow for the following:

    I. International harmonisation of our legislations
    II. Collation of all existing conventions and bilateral agreements
    III. International cooperation to combat cybercrime
    IV. wider investigatory capability
    V. Capacity Building and knowledge sharing
    VI. Opportunity for Nigeria to make a contribution to how cyberspace is governed through international instruments of law.

    International co-operation will also include becoming a member of recognised bodies such as:

    - The International Telecommunications Union (ITU)
    - Cybercrime Convention
    - Interpol

    It is envisaged that the processes to engage with international bodies will start to be defined with the objective of implementing and achieving within the next 12 months.

    This is an immediate initiative

4.3.4 Initiative 4: Public/Private Sector Collaboration

- Recognizing that cybercrime can impact both private and public sector environments, the legal strategy is to adopt processes for both public and private sector collaboration in combating cybercrime.

- As an example relationships between Communication Service Providers in assisting law enforcement agencies in preserving communications data for specified periods as dictated by the Data Retention legislations will be encouraged and forged.

- This will also extend to financial institutions in ensuring they retain customer records according to specified time lines.

- The strategy will also entail providing specific guidelines on how to meet these requirements.

- A key part of the public/private sector collaborative strategy will be to put in place measures to reduce reliance on foreign controlled networks to store personal information of Nigeria Citizens.

- This will have the impact of reducing the risk footprint as well as the potential for such data to be compromised and used to the detriment of Nigerians

- This is an immediate and ongoing initiative

4.3.5 Initiative 5: Raising Awareness

- While implementing cybercrime legislations are paramount in combating cybercrime, it is to be noted that making citizens aware of the threats and vulnerabilities that can accrue to them when they use the internet, is a measure that can be used to reduce the likelihood of them being victims of cybercrime.

- Raising awareness of the new laws through high profile campaigns is an initiative that will be used to make criminals aware of the consequences of being in breach of these legislations once they are enacted.

- It is also part of the strategy to socialise these new laws to the wider international community.

- This is an immediate initiative

4.4 Special Areas of Focus:

4.4.1 Data Protection, Privacy and Lawful Interception.

- Personal Information has economic and political value. The recent identification of Nigeria as a MINT (i.e. Malaysia, Indonesia, Nigeria and Turkey) country not only raises its profile in monetary and economic terms, it also raises the risk of infrastructure and systems containing Nigerian citizens data being targeted by unscrupulous individuals, organisations and nation states, leading to data loss, leakage as well as confidentiality, integrity and availability compromise.

- The recent revelations of American whistle-blower Edward Snowden has significantly raised awareness of the need for nations to put in place appropriate measures to protect the personal information, and privacy of its citizens.

- The revelations also identified the need to protect and secure communications of not only high ranking government and high profile individuals from mobile phone tapping but also ordinary individuals from their everyday non-criminal conversations being intercepted and analysed by law enforcement agencies, organisations and foreign countries.

- To protect and legislate for criminal activities against Nigerian Citizens data and their communications special emphasis will be given to the development and roll out of Data Protection and Privacy laws in Nigeria.

NCSS Fig 3 Data Protection and Privacy

- The objective of this initiative will be to ensure individuals and organisations are aware of their responsibilities when handling and processing personal information.

- It will also allow them to be aware of what constitutes unacceptable and illegal behaviour in relation to the use of such information and communication streams.

- The legislative, technical and policy initiatives to fulfil this aim will consist of the following:

i. Developing and enacting fit for purpose Data Protection and Privacy laws.

ii. Defining minimum policy and standards requirements for handling personal information

iii. Defining data Protection requirements for outsourcing initiatives.

iv. Deploying an effective and transparent Lawful Interception regime.

v. Deploying appropriate and workable data retention periods to assist law enforcement agencies in their investigations.

vi. Defining Data Protection Requirements for safeguarding Nigerian Citizens details on government systems

vii. Defining minimum technical measures that need to be in place to safeguard against personal information compromise

viii. Identifying where Nigerian Citizens Data details are held and if systems held on are appropriately protected

ix. Identifying Data Leakage Areas with view to reducing risk

x. Developing and implementing fit for purpose guidelines

xi. Liaison with Communication service providers to provide their customers with advice on how to protect themselves from cybercriminal activities

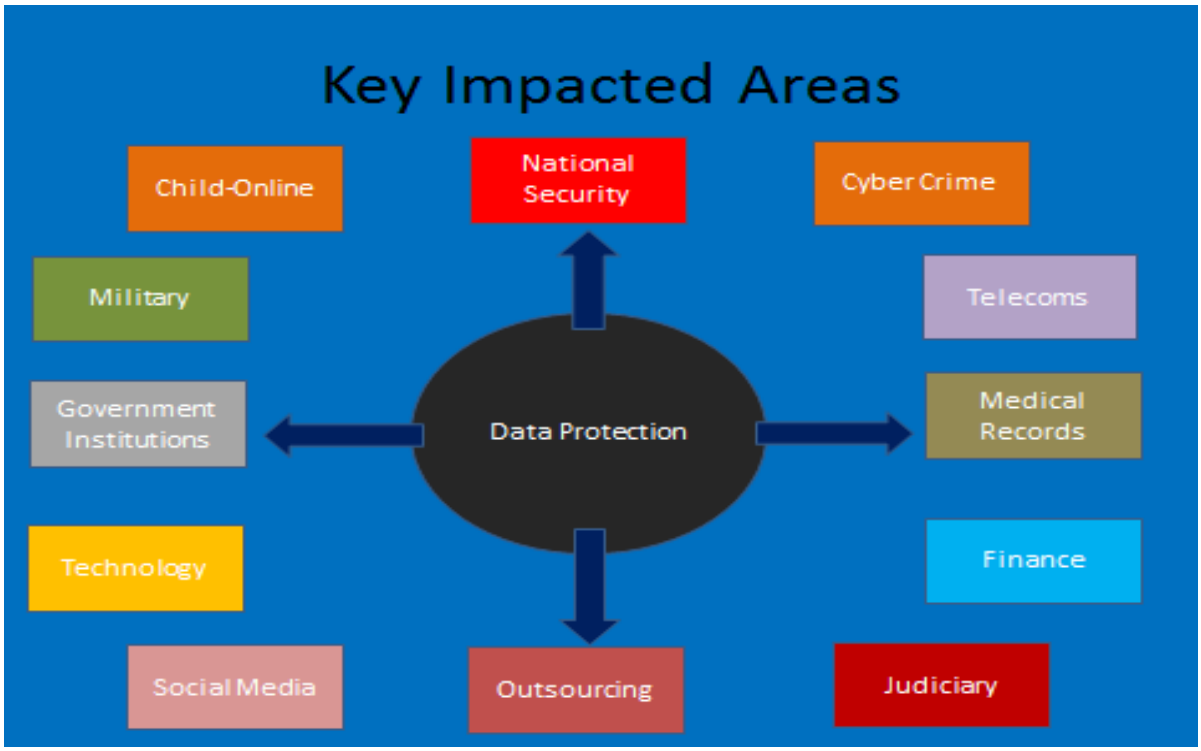
xii. Liaison with both private and public sector commercial organisations to help them understand the measures they need to take to reduce their risks to data protection and privacy breaches

xiii. Liaising with NCC , NITDA, Central Bank , Judiciary and Military to drive data protection in Telecoms, Finance and, government institutions and Judiciary

xiv. Establishment of a new regulatory body for adjudicating and providing guidelines on Data Protection, Privacy and Lawful Interception

xv. Reduce reliance on foreign-hosted cloud services for storing personal data of Nigerian Citizens.

xvi. Long-term strategy is to Partner with Nigerian Service providers to develop capabilities to provide local cloud service capabilities.



NCSS Fig 4: Data Protection Impact Point

CHAPTER FIVE

NATIONAL INCIDENT MANAGEMENT STRATEGY

5.1 Purpose:

5.1.1 The strategy on incident management is designed to effectively deter and respond to cyber threats and cybercrime that will leverage on an efficient emergency readiness and coordination capability.

5.1.2 The strategy will also facilitate, promote and strengthen national commitments to regional and global partnerships and cooperation on cybersecurity.

5.2 Establishing National CERT:

5.2.1 The Nigerian Computer Emergency Team (ngCERT) shall be established to ensure efficient response to security incidents within our cyberspace.

5.2.2 An effective computer emergency response capability is essential to monitor and deter threats that can exploit information system vulnerabilities.

5.2.3 The Nigerian Computer Emergency Readiness Team (ngCERT) will be empowered by a legal framework through which its functions and responsibilities are defined.

5.2.4 However, where existing laws are inadequate, a review or new legislative processes should commence to address legal vacuum that will hinder operations of the national CERT.

5.2.5 The harmonized laws should clearly mandate it to function as of one the strategic components of the central coordinating center for all computer security incident management within our national cyberspace. Additionally, incident classification will be the sole role of the Cyber Emergency Monitoring System (CEMS) administered and managed by ngCERT.

5.2.6 Additionally, incident classification will be the sole role of the Cyber Emergency Monitoring System (CEMS) administered and managed by ngCERT.

5.3 Implementation Approach

5.3.1 A National Incident Response Plan (NIRP) will be formulated to achieve a coordinated emergency response protocols. It will govern both the national and sectorial CERTs

5.3.2 The plan will set out clear definitions and procedures for incident response that will focus on incident classification and its severance.

5.3.3 In addition, incident classification will be the sole role of the Cyber Emergency Monitoring System (CEMS) administered and managed by ngCERT.

5.3.4 CEMS will classify threats that constitute a national-level cyber incident requiring ngCERT involvement and the triggering of incident response protocols.

5.4 Initiative 1: Preventive Strategy

5.4.1 All key national information infrastructures shall have a preventive mechanism for network monitoring system integrated into CEMS.

5.4.2 The preventive strategy will primarily be implemented by CEMS for analysis and detection as well as alert notification.

5.4.3 CEMS operational procedure will define the baseline security monitoring for broad detection of malicious or anomalous network activity within our cyberspace and specify specialized security monitoring for critical assets and critical processes within the context of the National Critical Information Infrastructure Protection Plan (NCIIPP).

5.5 **Initiative 2: Detection Strategy**

5.5.1 The Cyber Emergency Monitoring System (CEMS) will serve as the main provider of data analysis and reporting to other key detection and response partners across the incident management ecosystem.

5.5.2 Its key focus is to consistently monitor indicators within the nation's cyber space in order to detect potential threats and classify them according to its severance level determined. This can serve as an alert to the trigger the next chain of activity in the response protocols.

5.6 Initiative 3 Response Strategy:

5.6.1 After an incident is detected and validated by the CEMS, direct and coordinated action will be implemented immediately to ensure that appropriate actions to stop an on-going incident occur at the right time on the right cybersecurity priorities.

5.6.2 The action plan will require identifying the scope and scale of the incident in order to activate the relevant countermeasures procedures as outlined in NIRP to mitigate damages.

Investigating cybercrime incident requires a strict evidence preservation procedures showing appropriate evidence handling procedure and

established chain of custody.

Therefore, it is necessary for incident handlers to take appropriated measures in order to preserve any artefacts that could be of evidential value by recording, reviewing and resolving security incidents with the established incident management processes as define in the NIRP. Additionally, ngCERT is expected to document all such report as will be required to be submitted by all monitored information infrastructure custodians in order to evaluate the effectiveness of response plan through lessons learned.

5.7 Cooperation and Partnership

5.7.2 The ngCERT under the framework of National Cybersecurity Coordinating Center will coordinate activities of other sectorial CERT and facilitates cooperation and partnership of all cybersecurity stakeholders, including international and multilateral organizations.

5.7.3 It is imperative to note that, sharing of action noteworthy information about new threats and vulnerabilities with partners by ngCERT will avail them the security status of the national cyberspace and the need to protect it

5.7.4 NgCERT also will enable both government and private sector actors through stimulated exercises to support stakeholders understand their roles during a crisis and better prepare for incident response scenarios. This will test incident response capabilities and processes created to communicate, collaborate, and restore services in the event of an incident.

5.8 Capacity Building

5.8.2 To sustain an optimal incident response readiness capability, technical and procedural capacity building will be instituted for both law enforcement as well as judicial officers to build their expertise and facilitate understanding of the dynamics of cybercrime.

5.8.3 Training will focus on methods of handling digital evidence to ensure that it preserves its evidential weight and thus admissibility in Court.

5.9 National Digital Forensic Mechanism

5.9.1 The National Cybersecurity Coordinating Center shall develop a framework for the setting up of a National Digital Forensic Laboratory as a core unit under the coordination of NCCC.

5.9.2 The implementation and coordination of digital forensic technical and management guidelines will help develop guide for the law enforcement and security agency engagement in digital forensic investigation, analysis, interpretation and reconstruction of e-crime scene.

CHAPTER SIX

STRATEGY ON CRITICAL INFORMATION INFRASTRUCTURES PROTECTION & RESILIENCE

6.1 Introduction

6.1.1 This Strategy articulates the various Critical Information Infrastructure (CII) protection and resilience activities the Government undertakes, ranging from how it engages with business, government (international and domestic) as well as other stakeholders.

6.1.2 This Strategy presents the Government's approach to Critical Information Infrastructure Protection and Resilience (CIIPR).

6.1.3 It also acknowledges that CIIPR is a shared responsibility across governments, the owners and operators of critical infrastructure.

6.2 Vision of CIIPR

- To ensure continued operation of CII in the face of all hazards, as this critical infrastructure supports national defense and security, and underpins our economic prosperity and social wellbeing.

6.3 Mission of CIIPR

- To harness all relevant stakeholder's CIIPR Programs into a national holistic agenda capable of supporting the country's national security and ensure provision of essential services.

6.4 Strategic Objectives

i. Assess threats to, vulnerabilities of, and consequences to critical infrastructure through an intelligent and information-led, risk management approach.

ii. Secure CII against physical, human and cyber threats through sustainable efforts to reduce risk.

iii. Enhance CII resilience by reducing impact of unforeseen and unexpected incidents through advance planning and mitigation efforts, as well as effective responses aimed at saving lives and ensuring rapid recovery of essential services;

iv. Share relevant information across the CII community to build awareness and enable a coordinated risk- informed decision making, while promoting a learning and adaptation during and after exercises and incidents impacting on CII.

v. These objectives will be supported by regular developments of more specific priorities by key critical infrastructure partnerships related to risk management and capability enhancement.

vi. Based on the vision, mission, and goals, the critical infrastructure community will work together to set specific national priorities. National priorities will be set considering resource availability, progress already made, known capability gaps, and emerging trends and risks in cybersecurity.

vii. National priorities will drive implementation and will be supplemented by sector, regional, and corporate priorities. Performance measures will be set based on the goals and priorities of each sector, regional or national Government.

viii. The National Annual Preparedness Report will include measurements of progress that will help derive a common understanding of the state of critical infrastructure security and resilient efforts.

6.5 STRATEGIC IMPERATIVES TO ACHIEVE AIMS AND OBJECTIVES

6.5.1 The Government recognizes the importance of critical infrastructure, including those parts that provide essential services for everyday life (such as energy, food, water, transport, communications, health and banking and finance). A disruption to critical infrastructure could have a range of serious implications for business, governments and our social wellbeing.

6.6 Initiative 1: Operate an effective business-government partnership with critical infrastructure owners and operators.

- A significant proportion of the nation's critical infrastructure is privately owned or operated on a commercial basis.

- A business-government partnership will be established to help build confidence and reliability for the continued operation of critical infrastructure that supports national security, economic prosperity, and social and community wellbeing.

- It is important that the business-government partnership offers value and mutual benefit to the parties involved.

6.6.1 Necessity for Trust Information Sharing Network (TISN) Activity for NCIIPP

- There will be need for the establishment of a TISN for National Critical Information Infrastructure Protection Plan (NCIIPP).

- This network will comprise of relevant private sector and government representatives, to raise the awareness of risks to critical information infrastructure, share information and techniques required to assess and mitigate risks, and build resilience capacity within entities in the network.
- Working with the TISN, the private sector is able to bring issues to government that are seen as impediments to achieving critical information infrastructure protect.

- The TISN will be the most visible component of the public-private partnership and will provide an important mechanism to foster cooperation between public- private stakeholders on mutually important issues.

- The TISN will raise awareness on critical infrastructure issues, including potential impediments to achieving CIP. Government agencies directly involved in CIP are able to better represent stakeholder interests in the various machineries of government that are used to develop and implement Government policy and act as critical infrastructure advocates in the broader policy debate.

- Accordingly, Government agencies that have a role in implementing the CIP Strategy are able to influence or shape government policy initiatives that have impact on critical infrastructure organizations and their ability to achieve CIP.

6.6.2 Trusted Information Sharing Network Initiative (TISN)

- The TISN will be established in the Office of the National Security Adviser as an exclusive forum in which the owners and operators of critical infrastructure work come together and share information on threats and vulnerabilities as well as develop strategies and solutions to mitigate risk to the nation's CII.

- TISN members include owners and operators of critical infrastructure, Federal, State and local government agency representatives as well as departments and agencies of government.
- The TISN, through its Sector and Expert Advisory Groups, will promote infrastructure protection to owners and operators as well as promote the need for investment in resilient and reliable infrastructure.

6.6.3 Sector Groups

- Sector Groups form the bridge between government and the individual owners and operators of Nigeria's critical infrastructure.

- Their purpose is to assist owners and operators to share information on issues relating to generic threats, vulnerabilities and to identify appropriate measures and strategies to mitigate risk.

6.6.4 Sector Specific Plans

- There will be sector specific plans for each sector which will highlight sector level performance objectives and feedback to the coordinating agency of government charged with the responsibility of managing the sector.

- For example, the sector specific plan for the Information Technology Sector will be coordinated and managed by the Ministry of Information and Communication Technology. In collaboration with other stakeholders

(public and private sector partners), this Ministry will develop and implement a Sector-Specific Plan (SSP) to enable assessment of national, cross sector critical infrastructure protection and resilience plan. *(Please see appendices pages for a sample approach to implementing sector specific plan and program)*.

- Sector specific plan will be developed for other critical infrastructure sectors including but not limited to:

Communications Sector	Government Facilities Sector
Manufacturing Sector	Dams Sector
Defence Sector	Chemical Sector
Power and Energy Sector	Commercial Facilities Sector
Financial Services Sector	Food and Agriculture Sector
Emergency Services Sector	Transportation Systems Sector
Public Health and Healthcare Sector	Water & Waste Water systems
Information Technology Sector	

6.7 Initiative 2: Identifying and Evaluating Potential Critical information Infrastructure

6.7.1 Identification

- There will be national, sectorial and organizational approach in identifying and refining actual and potential critical information infrastructure.

- The National Critical Information Infrastructure Protection Unit of the Office of NSA (NCIIPU) will work with other government agencies, owners and

operators of critical infrastructure to ensure an on-going identification of critical information infrastructure.

- Due to infrastructure investment and expansion, advent of new technologies, population growth and increasing interdependence of systems and technologies, identification process will be subject to continual review.

.

6.7.2 Evaluation

- After the identification of potential critical components of information infrastructure, there will be the need for the evaluation to understand the mode of operation and estimate its risk levels and criticality.

- The evaluation process relies on the cooperation of infrastructure owners and operators. Having an understanding of the estimated risk and criticality levels is important for the government. However, this does not replace the owner's responsibility to develop a robust risk management program to safeguard their assets from known and unknown threats.

6.8 Initiative 3: Enhancing Strategic Readiness of Infrastructure Owners and Operators

- A key component of the NCIIPP is to sensitize owners and operators to adopt best practices in their approach to planning and preparedness. This will ensure a structured, logical and rigorous approach on the most appropriate steps to take in order to prevent, detect, react and recover from any incident of potential disruptive value.

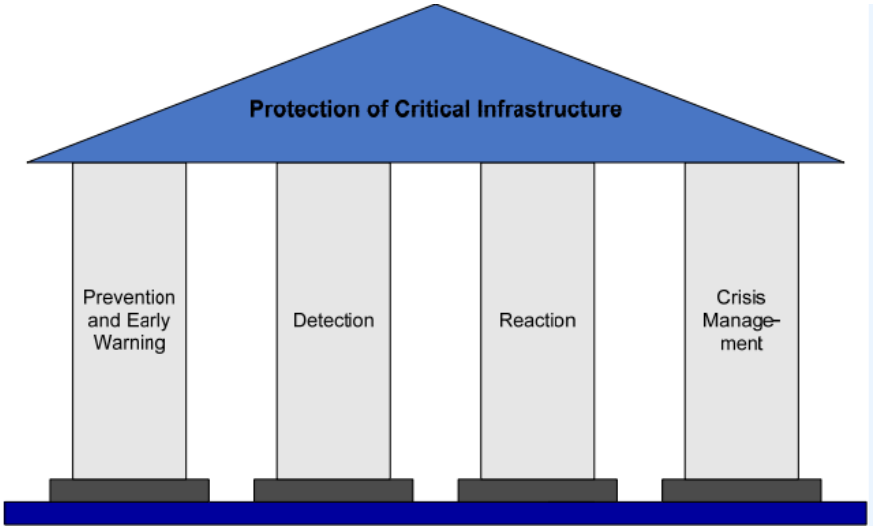
- Strategic readiness will enable owners and operators identify vulnerabilities and interdependencies as well as plan redundancy programmes including risks from acts of terrorism.

- It is suggested that owners and operators consider the following approach in their preparedness towards enhancing the strategic readiness for protection of critical information infrastructure.

  i. Prevention and Early Warning Strategy
  ii. Detection Strategy
  iii. Reaction Strategy
  iv. Crisis Management Strategy

READINESS APPROACH TO NCIIPP	
Prevention and Early Warning Strategy	**Goal**: Ensure CII are less vulnerable to disruptions and impairment duration is short and limited in proportion. **Approach**: Periodic dissemination of guidelines and best practices on specific threats using the TSIN framework
Detection Strategy	**Goal**: Discover and detect emerging threats on a timely basis **Approach**: NCIIPU in collaboration with ngCERT will identify and detect new forms of technical an non-technical attacks
Reaction Strategy	**Goal**: Identification and correction of causes of disruption. **Approach**: NCIIPU in collaboration with ngCERT will maintain a 24/7 incident reporting service. Furthermore, distribution of incident report and reaction among TISN members to share lesson learned in improving crisis and emergency planning
Crisis Management Strategy	**Goal**: Alert key actors of CII of the interdependencies and minimizing effects of disruptions on society.

	Approach: Using TSIN and ngCERT frameworks, constant rehearsals and practice of defined crisis management strategies



NCSS Figure 5: Four Pillars of Critical Infrastructure Protection [adapted from ITU's A Generic National Framework for Critical Information Infrastructure Protection (CIIP)]

6.9 Initiative 4: Identify, analyse and manage cross-sectorial dependencies

- The identification and analysis of cross-sectorial dependencies assists the risk management decision making of critical infrastructure organizations and helps to inform the Government's policy on CIP.

- Critical infrastructure by nature are highly interdependent, so that failure or disruption in one sector can lead to disruptions in other sectors. For instance, owners and operators of water infrastructure rely on electricity for pumping and telecommunications for monitoring operations. Similarly, the communications industry needs electricity to run their networks, and the electricity industry needs telemetry services to run their operations and electricity marketing.

- A cross-sectorial analysis of dependencies will assist owners and operators of critical infrastructure and the Nigerian Government to understand system-wide risks that are beyond the purview of individual organizations or sectors.

- This increases the potential for a more effective sharing of risk to cope with certain incidents. The Critical Infrastructure Program for Modelling and Analysis (CIPMA) is proposed as a key initiative of the Nigerian Government's efforts to enhance the protection and resilience of critical infrastructure in Nigeria.

6.9.1 The Critical Infrastructure Program for Modelling and Analysis (CIPMA)

- CIPMA is a computer-based capability, which uses a vast array of data and information from a range of sources (including the owners and operators of critical infrastructure) to model and simulate the behavior and dependency relationships of critical infrastructure systems.

- CIPMA uses an all hazards approach to undertake computer modelling to determine the consequences of different disasters and threats (human and natural) to critical infrastructure.

- Owners and operators of critical infrastructure can use this information to prevent, prepare for, respond to or recover from a natural or human-caused hazard.

- CIPMA also helps government shape policies on national security and critical infrastructure resilience.

- CIPMA is an important capability to support the business-government partnership, and relies on strong support from stakeholders such as owners and operators of critical infrastructure, Federal, State and local governments, and government agencies for its ongoing development.

- Importantly, CIPMA can show the relationships and dependencies between critical infrastructure systems, and the cascade impacts from a failure in one sector on the operations of critical infrastructure in other sectors.

- NCIPP unit manages CIPMA and works with ONSA-NCCC and other technical service providers to further develop and deliver this whole-of-government capability.

6.10 Success Criteria And Review Of CIIP Strategy

- Critical infrastructure protection and resilience is an ongoing process that requires periodic review and fine tuning of the activities under each strategic imperative will be required as the strategy is implemented.

6.10.1 **Mechanism for Measuring Success:**

Success will be measured through following mechanisms:

- Effective Critical Information Infrastructure Protection is reliant on a strong, collaborative partnership between governments and critical infrastructure owners and operators to deliver the Government's policy aim of the continued operation of critical infrastructure in the face of all cyber threats.

- Need for investment in resilient, robust infrastructure (e.g CIPMA) to identify key cross-sectorial dependencies and vulnerabilities with respect to both cyber and physical infrastructure.

- Businesses and governments collaborating to progress national research and submission of curriculum inputs to training and research on CIP

- Periodic lessons from incident report and reaction exercise activities and real life events propagated to all Sector Groups to enhance organization's

- Understanding of protection and resilience and improve planning arrangements.

- Coordination of Nigeria's international engagement with periodic updates provided to NCCC as required

- In order to ensure Government's policy settings remain appropriate, the CIP Strategy will undergo a comprehensive review after five years of operation.

Chapter Seven

STRATEGY ON ASSURANCE & MONITORING

7.1 Introduction

7.1.1 There is a need to address the issues of cyber threats from risks management and process governance approaches because of the need to address the nation's internal vulnerability and other weakest link.

7.1.2 The development of a National Cybersecurity Strategy designed to address these issues however, is only as good as the National Cybersecurity program that implements it.

7.1.3 The continuous monitoring and review (i.e. assessment and evaluation) of the implementation and management of the National Cybersecurity Program, and the surrounding context that it operates within, will be critical in providing assurance to various stakeholders that the National Cybersecurity program is well able, and continually so, to safeguard our vulnerability and other critical national infrastructure.

7.2 Strategic Objective

i. This strategy seeks to establish and maintain a monitoring and an assurance framework that will ensure that the efforts put in place to secure the nations cyberspace are in compliance with international best practices, perform as expected by the stakeholders involved, as well as to maintain the capabilities necessary to protect our nation's cyberspace and other critical infrastructure.

ii. To harness, profile, harmonize and priorities various technology neutral information security frameworks that will help determine best standards and guidelines suitable to the national peculiarity and in line with international best practices.

iii. To achieve coordination of information security regimes through consensus, collaboration, and partnership with relevant stakeholders.

iv. To facilitate national awareness on the criticality of ensuring and enabling information security conscious operational environment both in the public and private sectors

7.3 The Cybersecurity Assurance context

- The surrounding context within which the cybersecurity assurance mechanism will operate and monitor include the following:

i. The National Cybersecurity Strategy

This is the foundation on which the National Cybersecurity Assurance Program and action plans will be built, it will be periodically reviewed to provide assurance that will continue to address evolving threats in a dynamic threat environment.

ii. Stakeholders' Commitment to Cybersecurity

- An effective and efficient National Cybersecurity Assurance Program will require clear direction, commitment from the highest level of Government, top management and administration executive among others.

- The "tone at the top" will determine to a large extent the commitment shown by others in the lower cadres as it relates to Cybersecurity and also the resources committed to effecting the Program. This will be periodically reviewed and adequate strategies developed to ensure that those at the top are motivated to ensure consistent commitment to the cause of Cybersecurity.

iii. **Cybersecurity awareness level**

- The level to which all citizens of the country become aware of, and educated about cybersecurity issues will to a large extent determine how strong the cybersecurity efforts of the nation will be. As security is only as strong as its weakest link. Initiatives to continually create awareness among the citizens will be established and continually reviewed for effectiveness.

iv. **The Regulatory/Legal environment**

- The Cybersecurity bill, National Cyber Security Policy and other laws, policies and regulations will be periodically reviewed to ensure that they continue to be relevant, properly streamlined and serve as a good legal foundation to support the initiatives to secure the nation's cyberspace.

v. Cybersecurity Capabilities, Skills, Expertise

- The level of skills, capabilities and expertise possessed by the personnel that will be charged with the responsibility of securing the nation's cyberspace, who will essentially be Nigerian citizens, will go a long way in determining how well it will be done.

- Lack of adequately skilled personnel is a major vulnerability, and operating a national cybersecurity program within this context will constitute a major risk to the nation, therefore the capabilities, skills and expertise of personnel as related to the skills required to continually defend our nation in cyberspace will be periodically assessed and recommendations made to address any shortcoming.

vi. Risk Management Program

- An effective cybersecurity risk management process will enable the nation to identify, assess, and mitigate risks to the nation's cyberspace. These will include threat analysis both for determining evolving threats to the nation's cyberspace and emerging trends and threats.

- These information feeds into the Cybersecurity program to ensure that it continues to provide countermeasures that will protect the nation against both current and future threats to the nation's cyberspace and also serve as a basis for prioritizing responses to such threats based on risk/impact level.

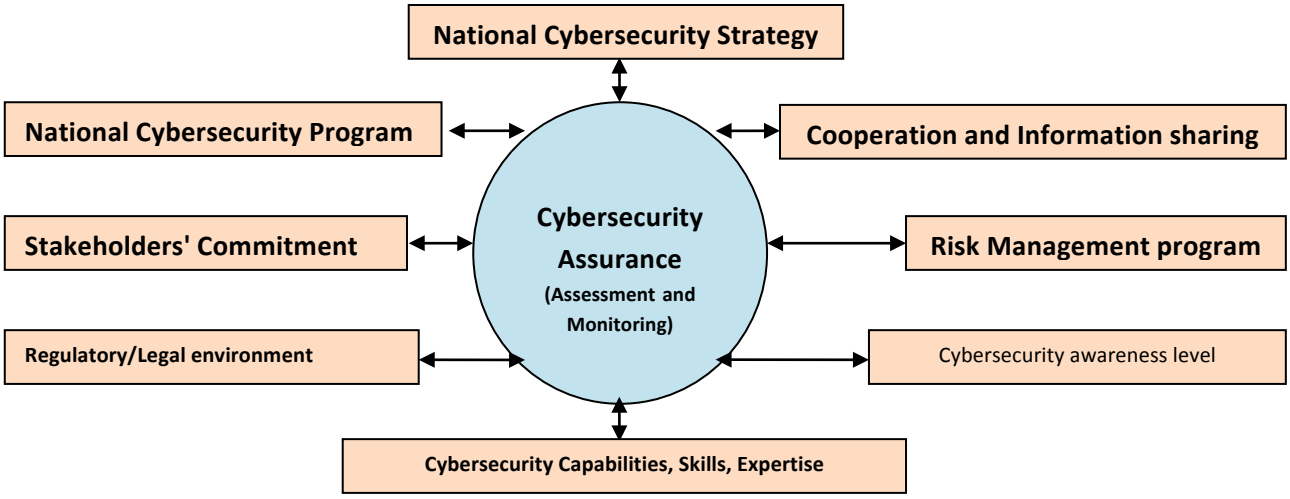
- The Risk Management program will be established and continually reassessed to ensure it continues to provide relevant information to help proactively protect our presence in cyberspace.

v. Cooperation/Collaboration and Communication/ Information sharing

- Level of Public-Private collaboration, intergovernmental, inter-sectorial and international collaboration and communication will continually be assessed to ensure that maximum benefits that leads to a more secure cyberspace are achieved from such collaboration/cooperation and information sharing.

viii **National Cybersecurity program**

Assurance activities including periodic assessment and reviews will be carried out to provide assurance that the cybersecurity program is achieving its objectives and that such objectives will aligned with SMART framework i.e. Specific, Measurable, Achievable, Results-focused and Time-bound



NCSS Figure 6 The Cybersecurity Assurance context - It shows the logical environment within which the Cybersecurity Assurance mechanism will operate and monitor.

7.4 Focal Points

7.4.1 Monitor the implementation program for the Cyber Security Strategy to provide assurance that the program is meeting, and will continue to meet stakeholder's expectations within a dynamic cyber landscape.

7.4.2 Make recommendations on possible improvements in the Cyber Security Strategy itself based on observed changes in threats profile.

7.4.3 Encourage, monitor and review the adoption of national and international best practices as codified in the international frameworks and standards to ensure

national cybersecurity practices that compare well with international standards and practices and also serve as a basis for benchmarking our maturity level.

7.4.4 Monitor and review cybersecurity capabilities of actors at the national, state and sectorial levels to ensure continuous improvement and development of relevant capabilities, skills and proficiencies, enabling them to defend our nation in the face of present and future threats to the nation's cyberspace.

7.4.5 Monitor and review level of preparedness and capacity of various actors at the national, state and sectorial levels to ensure their readiness to defend our nation in the face of present and future threats to the nation's cyberspace.

7.4.6 Ensure a continuous improvement process for cybersecurity.

7. 4.7 To develop performance measures both at the policy, strategic, tactical and operational levels based on the proposed Cybersecurity balanced scorecard and perform reviews based on these measures to ensure feedback on performance of the National Cybersecurity program so that adequate corrective and improvement changes can be made.

7.4.8 Conducting information security audits and process audits for government entities and also coordinating and validating security audits and process audits of self- assessment entities.

7.4.9 Conducting and coordinating information security risk assessment and analysis while establishing reasonable security guidelines and measures to protect data and systems.

7.5 Strategy

7.5.1 Initiative 1

- The National Cybersecurity Assurance Department as an arm of the NCCC will be established to serve as a mechanism for fulfilling all Assurance and Monitoring focal points.

- The department will be charged with the responsibilities of providing assurance as regards the National Cybersecurity program.

- The unit will be set up at the start of implementation of the National Cybersecurity program.

7.5.2 Initiative 2

- The Strategy approach to cybersecurity governance is anchored on a sound technology neutral framework. This is line with global best practice, while emphasizing the need for an effective business governance process from a risk management approach.

- The dynamism of cybersecurity risks requires a flexible and responsive risk management strategy.

- Thus, this Strategy provides adoptable and adaptable fit-for-purpose International Standards and frameworks for information Security Governance, Risk and Control in line with globally consensus.

- This strategy will facilitate cooperation among stakeholders responsible for ensuring the security and safety of our cyberspace and other critical infrastructure towards ensuring commonality in approaches to cybersecurity and standardization.

- This initiative recommends consensus driven international standards and multi-stakeholders' frameworks on information security assurance.

7.5.3. **Initiative 3**

- With a definite timeline, the strategy will implement continuous monitoring software solutions for vulnerability and security configuration compliance monitoring, threat management functions and penetration testing activities to

identify alterations and weaknesses in security configurations on critical national infrastructure.

7.5.4 **Initiative 4**

- An effective Cybersecurity risk assessment program will be established with a definite timeline.

7.5.5. **Initiative 5**

- This strategy will implement a core assurance capability thus enabling the nation to assess the effectiveness and adequacy of cybersecurity controls, when evaluated from an attacker's perspective, to deny the compromise of critical nation infrastructure.

7.5.6**. Initiative 6**

- The Strategy implements an Enterprise Application Security Testing regimen with standardized processes and procedures within application lifecycle development processes to help identify vulnerabilities and weaknesses in custom and source code, web applications and databases deployed to support cybersecurity in the nation.

7.5.7. **Initiative 7**

- This strategy recommends the adaptation of Balanced Scorecard framework and approach to organization's cybersecurity known as the National Cybersecurity Balanced Scorecard framework. This will serve as the basis of developing performance metrics, key performance indicator (KPIs) and key goal indicators (KGIs) that will be used to measure the success of the Cybersecurity program.

7.5.8. **Initiative 8**

- This strategy provides for the design, development and documentation of a National Enterprise Security Architecture Framework that will serve as the basis for the design and continuous improvement of a cohesive, standardized and well integrated infrastructure put in place to safeguard the nation's cyberspace

7.5.9. **Initiative 9**

- Develop Blue team and Red team capabilities among cybersecurity actors.

CHAPTER EIGHT

NATIONAL CYBERSECURITY SKILL & MANPOWER DEVELOPMENT

8.1 Introduction:

Nigeria presently lacks sufficient specialised cybersecurity skilled personnel required for driving national cybersecurity capabilities and empowerment. This national cybersecurity strategy provides for a coherent and coordinated cybersecurity skills and human empowerment framework as envisioned in the National Cybersecurity Policy.

8.2 Objectives:

Cybersecurity skills development is a national priority and also a foundation for the achievement of national cybersecurity readiness. Therefore, this focus area aims to achieve the following objectives:

i. To provide an institutional framework anchors on public-private partnership towards building local professional skills.
ii. To provide central coordination and regulation of skills development within the public sector.
iii. To help build framework for public-private partnership on professional training and capacity building in cybersecurity for private sector

towards promoting common understanding on cybersecurity challenge.

8.3 Scope

8.3.1 The scope of the national cybersecurity skills development include the following;

i. To leverage on cybersecurity in national security and economic innovation for competitive advantage.

ii. To develop cybersecurity professional skills roadmap that will facilitate emergence of local content and expertise.

iii. To harness initiatives that will stimulate emergence of cybersecurity industry in Nigeria.

8.3.2 Therefore, this section focuses on the framework for the creation of programmes to increase the cadre of cybersecurity professionals in Managerial, Technical and Information Assurance areas rather than general user awareness and education. It further advocate for re-organization of the nation's educational priorities to address cybersecurity challenges and opportunities.

8.4 Initiatives

8.4.1 A specialized national skills development and empowerment initiative on cybersecurity covering various level of knowledge in information assurance will be established under the National Cybersecurity Coordinating Center.

- The initiative will be set up under the framework of Nigeria Institution of Cybersecurity (NIOC) in partnership with stakeholders as enshrined in the National Cybersecurity Policy.

  - The framework will involve designing, developing, and implementing level of skills, requirement, coordination, certifications, regulations, capabilities and expertise to be possessed by the personnel that will be charged with

the responsibility of securing and maintaining the nation's presence in cyberspace, who will essentially be Nigerian citizens.

- Lack of adequately skilled personnel is a major vulnerability, and operating a national cybersecurity program within this context will constitute a major risk to the nation, therefore the capabilities, skills and expertise of personnel charged with the responsibility of defending our presence in cyberspace will be periodically assessed, regulated and recommendations made to address identified gaps.

8.5 Roadmap for Nigeria Cybersecurity Industry:

8.5.1 In Nigeria, cybersecurity essential skills at the public institutions and industry level engagement are scarce. The scarcely available ones are extremely limited in their scope and capabilities to safeguard and protect critical industries. Various genuine concerns have been expressed on the apparently incapacity of Nigeria as a nation to protect itself and her industry in the face of a major attacks on her Critical Information and Related Infrastructures.

8.5.2 Stakeholders from Industries, law enforcement agencies, academics, non-governmental organizations, government Ministries, Department and Agencies, Nigeria Professionals in diasporas should emerge together under a proposed framework for cybersecurity profession umbrella body to help the country drive common professional synergy on cybersecurity instrument of research and development, innovations, and trusted cooperation necessary for a national cohesion on cybersecurity.

8.5.3 The proposed government and private sector synergy should culminate into the formation of Nigeria Institution of Cybersecurity (NIOC) that will help develop and drive a coherent body of useful and applicable knowledge in cybersecurity.

8.5.4 The NIOC will be expected to be built on nationwide standards with the aim of harmonizing, developing, promoting and enhancing multidisciplinary professional skills capacity and standards in the development of Cybersecurity industry, while providing opportunity for the citizen positive engagement in cyberspace.

8.5.5 It is expected that by promoting national dignity, preserving national security and economic values, including international standards on multidisciplinary professionalism and expertise, the institution will serve the human resources needs of the country in both the government and private sectors covering all

aspect of cybersecurity as defined through the international framework of cooperation on cybersecurity and other widely recognized international best practices.

Source: Recommendation from 1st National Conference on Cybercrime & Cybersecurity 2008 –An event organised by Global Network for Cybersolution in collaboration with NITDA, NCC, Ministry of Justice

8.6 Institutional Framework

8.6.1 Under the NCCC, NIOC will provide strategic framework for partnership with the following stakeholder on cybersecurity skill development, creativity, innovation and research: academia, research & development agencies, industry, and multi-stakeholder civil society.

8.6.2 The NIOC will develop professional career standard, minimum entry requirement, based on categorizations acceptable to the government and local industry.

8.6.3 It will develop unified scheme for national certifications, training in cybersecurity, capacity building and granting recognized professional status level correspondence to professional categorization.

8.6.4 NIOC will develop professional syllabus standardizations, and prospectus for short term and career focused professional skills development.

8.6.5 NIOC will prepare, coordinate, regulate and conduct NIOC professional examinations in different categories of certification nationwide in collaboration with the industry.

8.6.6 The NIOC will regulate, approve and coordinate the lists of independent and accredited cybersecurity training centres in the country.

8.6.7 NIOC will provide professional guidelines in learning resources, materials and curriculum development that best meet local and international requirement.

8.6.8 NIOC will provide professional measurable benefits in line with national and international best practices to all professional members scalable to fit into various categories of membership.

8.6.9 NIOC will develop industry acceptable waiver schemes or conversion programs for relevant established professionals interested in cybersecurity profession, Public institutions, law enforcement agencies, Military, Para-military and security agencies whose operation and experience are relevant to cybersecurity irrespective of the professional background.

8.6.10 NIOC will develop industry acceptable waiver schemes or conversion programs for relevant established academics in the field of law, ICT, IT,

Finances and relevant to the field of cybersecurity specialization, research and development.

8.6.11 NIOC will develop industry acceptable conversion programs for young Nigeria graduates in any recognized and approved discipline or, and equivalent in line with the NIOC approved levels of certifications and categorization of membership.

8.6.12 NIOC will promote federal government and industry acceptance of certifications Nation-wide.

8.6.13 NIOC will develop strictest professional code of ethical conducts, professional dispute and conflict resolution structures.

8.6.14 NIOC will secure international best practices approval and relevant international standards from global institutions.

8.6.15 NIOC will provide framework for continuous professional development in line with international best practices.

8.6.16 NIOC will interface and collaborate with relevant and other related professional bodies for technical cooperation and partnership on technical exchange programs relevant to cybersecurity.

8.6.17 The NIOC professional training and skills development will be based and focused on generic cybersecurity technology and tested models as adopted globally**.**

8.6.18 NIOC will become a unifying professional body accommodating all cybersecurity stakeholders from existing professional bodies in the country whose professional engagement fall within the purview of NIOC.

Securing Nigeria in Cyberspace:

To build an infinitely sustainable cybersecurity readiness, there is critical need to focus on our collective strength, sense of responsibility, excellence, prudency, and strategic appropriation of our collective ingenuity for the benefit of protecting our common wealth in cyberspace within the current and future dispensation.

CHAPTER NINE

STRATEGY ON ONLINE CHILD ABUSE & EXPLOITATIONS

9.1 Introduction:

- Cyberspace has brought huge benefits to children around the world, with the number of connected households increasing each year. While the potential for good is undisputed, Internet has become increasingly accessible to the critical segment of our population i.e. Nigerian children and young people, both at home and in schools.

- Rather than surfing the Internet passively, children and young people participate in a dynamic online environment that allows them to generate, manipulate and consume internet content like never before, forging their place and identity in online communities.

- More importantly, as a result of the universal availability of Internet access in homes, schools, libraries, mobile phones, etc., children are increasingly becoming involved in the use of the new technological application and taking advantage of the opportunity it provides for learning, research, entertainment and business.

- However, the Internet has also raised new and disturbing issues of vulnerability, especially for children. It exposes children to potentially negative contents.

- Children and Young Persons are the most active participants in online social networking and therefore are potential victims of improperly disseminated and dysfunctional contents that could cause disorientation and threaten their survival and that of the society.

- There are growing concerns on the distribution of online child abuse materials targeted to children which are making them vulnerable to child pornography, sexual abuse, harassment, exploitation, extremism, brain washing for terrorist

acts of violence and human trafficking resulting into unpleasant outcome of the information age.

- In order to address these issues of child online exploitation and its disastrous consequences, the National Cybersecurity Policy viewed it as one of the critical areas of focus.

9.2 Rationale for COAEP

9.2.1 The National Cybersecurity Policy framework provides a rationale and philosophy to guide development of strategy for Nigerian Child Online Abuse and Exploitation.

9.2.2 The Principles on Child Online Abuse & Exploitation and Counter-measures emphasized Social Media as a vital attractive channel and tool for social interactions and productive engagements. Regrettably, the openness and transparent nature of cyberspace have been exploited for good causes and malicious intents.

9.2.3 Therefore, there is need for the following actions;

i. Integration of Child Online Abuse and Exploitation into National legislation on cybercrime and cybersecurity.

ii. There is a need to establish that any act against a child which is illegal in the real world is illegal online and that online data protection and privacy rules for legal minor are also adequate.

iii. Ensure that a mechanism is established and is widely promoted to provide a readily understood means for reporting illegal content found on the internet , for example , a national hotline which has the capacity to respond rapidly and have illegal material removed or rendered inaccessible

9.2.4 It is the intention of government to harness counter-measures through a legislative framework, policy and strategic actions to address cyber abuse and online exploitation of Nigerian Child in a manner that will prevent and curtail cybercriminal intents and related malicious acts inimical to the national dignity, security and economic interests of the country.

9.3 Objectives

9.3.1 To provide common approach in the development and implementation of National Countermeasures strategy.

9.3.2 To provide robust security initiatives, action plan, and roadmap that will give overall direction to the planning and implementation of these countermeasures strategy within the framework of National Security.

9.3.3 The strategy addresses urgent security and law enforcement challenges, roles and shared responsibilities and government interventions.

9.3.4 The strategy harnesses frameworks that provide coherent structure for coordination of multi stakeholder engagement.

9.4 Strategic Approach

These objectives are anchored through the following approaches while considering our socio-economic security peculiarity and vulnerable operating environment for the purpose of protecting Nigerian children and young generations on the internet.

i. The National Cybersecurity Strategy approach adopts multi-stakeholder and multi-sectorial collaboration through partnership and alliances of government and key actors with clearly defined and specific guidelines for policy makers, law enforcement and security agencies.

ii. The partnership and alliances will be forged to ensure cooperation for action and mutual awareness among stakeholders on the consequence of improper engagement in cyberspace.

9.5 Strategy

9.5.1 Initiative 1: Focusing on National Process Mechanism

i. There shall be Infusion of Child Online Abuse and Exploitation Protection Strategy (COAEPS) into the larger framework for National cooperation on cybersecurity.

ii. Establishment of a unit under the National Cybersecurity Coordinating Center (NCCC) to handle matters relating to Child Online Abuse and Exploitation within the scope National Cybersecurity Policy.

iii. The COAEP unit of NCCC will collaborate with industry regulators and operators to implement a coherent Countermeasures Technical Mechanisms (CTM) to prevent access to web sites identified as hosting

contents that are offensive to children and to implement processes to enable the removal of any child sexual abuse content posted on their own services.

iv. The Unit will provide partnership mechanism in regard to the promotion of public awareness, messages and campaigns center on safety and security of Nigeria children interactions online.

v. The unit will train and build the capacity of Nigerian Law enforcement officers to conduct investigations into Internet related crimes against children and young people and maintain a register of convicted online crime offenders.

vi. The unit will facilitate national processes which ensure that all Child Abuse and Exploitation materials found in cyberspace are channeled towards a centralized, national resource.

9.5.2 Initiative 2: Focusing on International Process Mechanism

i. The NCCC will drive Virtual National Taskforce (VNT) which will work with *Virtual Global Taskforce*, a law enforcement body which provides a 24/7 mechanism to receive reports about illegal behavior or content from persons across the globe. The nation will develop modality for working with this global security platform most especially for countermeasures against terrorist recruitment and online predators.[3]

ii. It is strategically essential that the Nigerian law enforcement community becomes fully informed through training and capacity building and empower through legislation to help make the Internet safer for children and young people.

iii. Investing in training for law enforcement, prosecutorial and building capacity of Nigerian Judges through collaboration with National Judiciary Institutes. Investment will also be needed in acquiring and maintaining the facilities necessary to obtain and interpret forensics evidence from digital devices on Child Abuse Materials.

9.6 Operational Measures

[3] www.virtualglobaltaskforce.com

9.6.1 NCCC will ensure that a working mechanism is established and is widely promoted to provide a readily understood means for reporting illegal content found on the Internet, for example, a national hotline which has the capacity to respond rapidly and have illegal material removed or rendered inaccessible.

9.6.2 NCCC will ensure various security and law enforcement agencies in the country implement abuse report mechanisms which will be prominently displayed on relevant parts of any web site that allows user generated content to appear. It should also be possible for people who feel threatened in any way, or for people who have witnessed any worrying activity on the Internet, to be able to report it as quickly as possible to the relevant law enforcement agencies that need to be trained and ready to respond.

9.6.3 NCCC will promote a number of software programmes which can help screen out unwanted material or block unwanted contacts. Utilizing some of the child safety and filtering programmes because they are part of a computer's operating system or they are provided as part of a package available from an ISP or ESP. The manufacturers of some game consoles also provide similar tools if the device is Internet enabled. These programmes are not foolproof but they can provide a welcome level of support, particularly in families with younger children. These technical tools will be used as part of a broader arsenal. Parental and/or guardian involvement is critical.

9.6.4 It is strategically essential that the Nigerian law enforcement community becomes fully engaged with any overall strategy to help make the Internet safer for children and young people.

9.6.5 Nigerian Law enforcement officers will be appropriately trained to conduct investigations into Internet related crimes against children and young people. They need the right level of technical knowledge and access to forensic facilities to enable them to extract and interpret data obtained from computers or the Internet.

9.6.6 NCCC will establish a clear mechanism to enable children and young people, or any member of the public, to report any incidents or concerns they might have about a child's or a young person's online safety.

9.7 National Security Response Measures

9.7.1 With escalation of cybercrime, youths based conflict and terrorist recruitment, bombing attack in the country, the Internet has made possible a range of

ways of abusing children and recruiting young people, e.g., through web cams, chat rooms and internet blog.

9.7.2 The internet has also played a singular role in expanding the scale on which Child Abuse Material (CAM) has become available in all parts of the world. For these reasons, when addressing online safety concerns for children and young people from national security perspective, the Strategy gives special consideration to the following:

i. Outlawing “grooming” or other forms of remote enticement of legal minors into inappropriate sexual contact or sexual activity, possession, production and distribution of CAM, irrespective of the intent to distribute.

ii. Taking additional response steps to disrupt or reduce the traffic in CAM, for example by establishing a national hotline and by deploying measures which will block access to web sites and Usenet Newsgroups known to contain or advertise the availability of CAM.

iii. Ensuring that national processes are in place which ensure that all CAM found in a country is channeled towards a centralized, national resource.

iv. Developing strategies to address the demand for CAM particularly among those who have convictions for such offences. It is important to build awareness of the fact that this is not a victimless crime: children are abused to produce the material being viewed and by intentionally viewing or downloading CAM one is contributing directly to the abuse of the child depicted and one is also encouraging the abuse of more children to produce more pictures.

v. Building awareness of the fact that Nigerian children usually would not consent to being sexually abused, whether for the production of CAM or in any other way. Encourage people who use CAM to seek help, while at the same time, making them aware that they will be held criminally responsible for the illegal activity in which they engaged/are engaging.

vi. Ensuring that law enforcement crime prevention strategies as well as school-based and social programmes include sections on cyber safety and the risks posed by online predatory behavior, with age appropriate advice.

vii. NCCC maintains a register of convicted online crime offenders. Courts have issued judicial orders banning such offenders from using the Internet altogether or from using parts of the Internet which are frequented by children and young people. The problem with these orders hitherto has been its enforcement.

viii. Consideration will be given to integrating the list of convicted sex offenders into a block list which will prevent those on it from visiting or joining certain web sites.

ix. Providing appropriate long term support for victims. Where children or young people have been victimized online, where for example an illegal image of them has appeared on the Internet, they will naturally feel very concerned about who might have seen it and what impact this will have on them. It could leave the child or young person feeling vulnerable to bullying or to further sexual exploitation and abuse.

x. Ensuring that a grassroots' reporting and intelligence gathering mechanism is established and is widely promoted to provide a readily understood and rapid means for reporting illegal content or illegal or worrying online behavior e.g. a system similar to that which has been established by the Virtual Global Taskforce. The use of the INTERPOLi24/7 system will be encouraged.

xi. Ensuring that a sufficient number of law enforcement officials are appropriately trained in investigating Internet and computer-based crime and have access to appropriate forensic facilities to enable them extract and interpret relevant digital data.

xii. Investing in training for law enforcement, prosecutorial and judicial authorities in the methods used by online criminals to perpetrate these crimes. Investment will also be needed in acquiring and maintaining the facilities necessary to obtain and interpret forensics evidence from digital devices.

xiii. In addition, it will be important to establish bilateral and multilateral collaboration and information exchanges with relevant law enforcement authorities and investigative bodies in other countries.

CHAPTER TEN

STRATEGY ON PUBLIC-PRIVATE PARTNERSHIP

10. 1 Introduction

- The present administration has demonstrated her commitment to the prevailing security challenges by taking positive step to re-invigorate National Cybersecurity Strategy as part of the National Security agenda.

- The Cybercrime legislation and the need to actualize the implementation of National Cybersecurity Strategy requires effective machinery of public-private partnership and management framework to drive the buildup process with tripartite synergy of the whole nation including the government, non-government actors and international stakeholders.

- In the light of the above, this section seeks to provide the government with a strategic public-partnership management framework approach for the implementation of National Cybersecurity Strategy.

- The key elements of this strategy are as follows:
    i. The PPP Management Framework to facilitate the cooperation and partnership in the implementation of National Cybersecurity Strategy among the tripartite stakeholders in the country.

    ii. The Nature of the PPP Framework Model, Benefit, Impact & Direction.

    iii. Special Purpose Vehicle and Delivery channel through the setting up of PPP for Cyber security (3PC).

    iv. 3PC Working Document & Terms of Reference

    v. 3PC Sustainable Strategy

vi. Evaluation & Appraisal

10.2 **The Imperative of Public-Private Partnership Framework for National Cybersecurity Strategy**

- In the current dispensation, engagement in cyberspace is central to the existence, survivability, relevancy, as well as security and protection of the public institutions and private sector businesses.

- The public and private sectors' interests are enormously intertwined with a shared responsibility for ensuring a secure cyberspace and a protected critical economic infrastructure upon which businesses and government services depend.

- Public-Private Partnership framework is critical to the build-up process and overall success of the National Cybersecurity Strategy.

- Right from the commencement of the efforts on National Cybersecurity Strategy since 2003, which was reinvigorated in 2010 and till the present time. Most often, private sectors are usually caught unprepared in the buildup process.

- There is a concrete evidence that the Federal government cannot succeed in the many facets of securing National cyberspace if it works in isolation in her build up in the implementation of National Cybersecurity Strategy. Therefore PPPC is set to define roles and responsibilities, integrate capabilities, and facilitate joint ownership of the problems and the challenges towards developing holistic Cybersecurity Strategy. It is only through such sustainable partnerships that the Country will be able to enthrone cybersecurity and reap the full benefits of the digital revolution.

- Furthermore, the National Security challenge of securing cyberspace requires an increased effort in all stakeholders' collaborations. This effort should seek—in continued collaboration with the private sector—to improve the security of national interoperable networks

- The private sector, however, designs, invest, builds, owns, operates and maintains most of the critical information infrastructures that support government and private users alike.

- Therefore Industry and governments share the responsibility for the

security and reliability of the infrastructure and the transactions that take place on it and should work closely together to address these interdependencies.

- There are various approaches the NCSS take to address these challenges, some of which require changes in law and policy.

- Thus private-sector engagement is required to help address the limitations of law enforcement and national security. The Federal government and the private sector have an enduring interest in assuring the security of the digital infrastructure. Accordingly, government-industry collaboration is fundamental to achieving National Cybersecurity Strategy.

- It is, therefore, critically important that government and private sector work together in a proactive way. Successful government-private sector collaboration requires three important component:

i. **A clear value proposition:**

- NCCC will articulate the mutual benefits to government and private sector partners.

ii. **Clearly defined roles and responsibilities**.

- **NCCC will** develop a framework for common understanding that will guide mutual working relation and define basis of relationship between NCCC and private sector with clearly define roles and responsibilities.

iii. **Trust:**

- This is fundamental and necessary for establishing, developing, and maintaining sharing relationships between government and industry.

- NCCC will develop, engender, nurture and infuse a Trust Framework for public-private sector cooperation and understanding on critical issues of cybersecurity assurance and monitoring, sectorial CERT, and critical information infrastructure protection plan.

- NCCC will provide a Trust Framework that respect and address industry areas of concern in a manner that will not jeopardize but

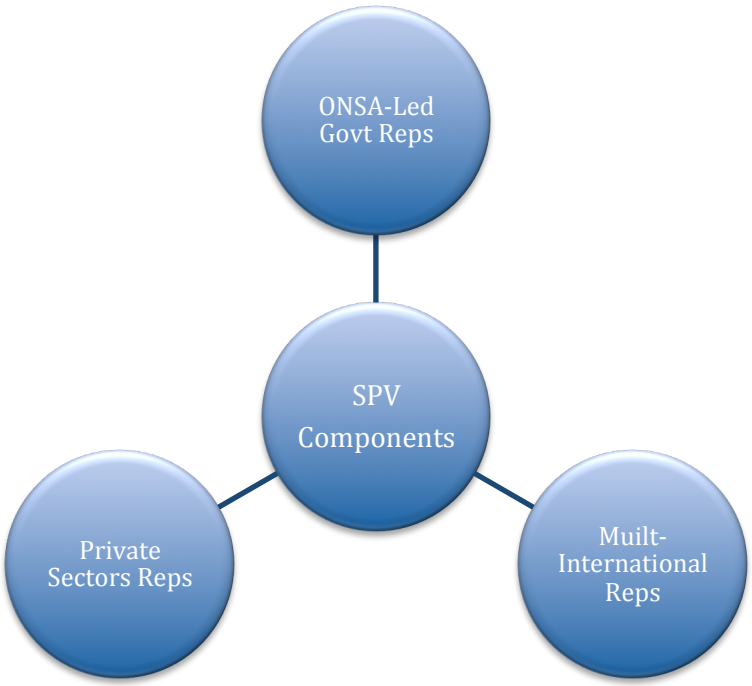
balance intrinsic business interest and National Interest.

10.3 Public-Private Sector Partnership Management Strategy (PPPMS)

10.3.1 The nature of the proposed PPMF Model involves the following:

- A linear build-up structural processes and national coordination through a PPP Special Purpose Vehicle created by NCCC for this purpose
- The SPV drives and coordinates all the PPP buildup processes for the coordination of government and industry partnership.

Fig 7 The proposed linear build-up process coordination through Special Purpose Vehicle (SPV)



- The ONSA through the NCCC will take the lead by establishing PPP- National Technical Working Group (NTWG) composing of representatives from private sector, government organizations and representatives of international multistakeholder partners.

- The NTWG should not exceed a number needed to be sufficient representatives of all the interests but at the same time capable of conducting PPP-MF business.
- To assure its continued connection to the interests it is intended to represent, provisions could be made for term limits for members.

10.3.2 **The Objectives of PPP Management Framework (PPPMF)**

i. To develop and implement public-private partnership action plan to support the review and monitoring of implementation cybercrime and cybersecurity legislation.

ii. To provide and nurture a sustainable trusted platform for National cooperation, understanding and interactions among all stakeholders, while managing all the build-up processes that will lead to the harmonized agreements on National Cybersecurity among the government, lawmakers, and the private sector.

iii. To provide a national mechanism that will unify variety of positions, equities, and knowledge gaps to overcome differences and addresses institutional diverse positions.

iv. To secure other stakeholders inclusion in the development and implementation of National Cybersecurity efforts.

v. To facilitate the development and coordination of private sector groups from different critical infrastructure industries related to Cybersecurity to address common security interests collaboratively with government.

vi. To create and nurture trusted forums to address common Cybersecurity challenges, national discourse and dialogue that will enhance cooperation and understanding among various groups on National Cybersecurity effort.

vii. To institute fundamental arrangements between government and the private sector for Cybersecurity incidence and response management.

10.3.4 Implementation Vehicle for the Public-Private Partnership Management Framework

i. Creation of PPP-National Technical Working Group (NTWG) for the Implementation of the PPP-Framework.

ii. The mandate of the NTWG will be anchored on the implementation of PPPMF objectives with the overall mission of actualizing national adoption and operation of National Cybersecurity Strategy within the country.

iii. A selection criteria for the appointment of the Members of NTWG is based on the value Impact of their respective inputs, in terms of the following;
- Technical contributions
- Critical Infrastructural Operators
- National Platform & Backbone
- Organizational Support: Structure & Coordination
- Media
- Non-government Organization
- Multi-stakeholder Management
- Understanding of Regional and Global framework for cooperation
- Legal Issues
- Public interest

10.3.5 The Benefit & Outcome of PPP-MF

i. It provides opportunity for government to effectively engage the core stakeholders in the country while entrenching nationally acceptable National Cybersecurity Strategy at the onset.

ii. Cybersecurity Strategy is a complex set of issues involving legal, socio-economic, and national security considerations. Several public institutions have significant jurisdictional claim on cybersecurity issues.. The PPPMF will, therefore, provide opportunities to address all the divergent positions of these stakeholders.

iii. Cybersecurity strategy has a deep connection with critical information infrastructure, economy and security. Private sector provides technology innovations, critical resources and technical standards that the government needs to drive National Cybersecurity Strategy. While government provides enabling mechanisms, instruments and authorities to transform industry best practices and standards into the

framework of National Cybersecurity Strategy, thus, PPPMF will assist government to address structural weaknesses.

iv. National Cybersecurity Strategy driven through the public-private partnership of government and private sector has greater national security implication and economy protection values, than government working alone or in partnership with multilateral and multinational institutions.

v. PPPMF enables a trusted platform for strategic information sharing between government and private sector critical for the overall success of National Cybersecurity Strategy.

vi. It provides partnership vehicle for National Executive Council, National Assembly and private sector to achieve mutual understanding and cooperation on the operation of Cybersecurity legislation and implementation of National Cybersecurity Strategy.

vii. PPPMF will facilitate structural coordination across the public and private sector, building public confidence in National Cybersecurity Strategy.

viii. Government depends on a privately operated cyber infrastructure. Through the PPPMF, government engages with industry to continue building the foundation of a trusted partnership. This engagement will build value propositions that are understood by both government and industry partners for the benefit of National Cybersecurity Strategy.

CHAPTER ELEVEN

Strategy on National Internet Safety

11.1 Introduction

- The nation is building various capabilities in computer security emergency response and internet is fast becoming the mainstream for economy and interaction. The government will need to interface with ordinary citizens engaging online on protection awareness, safety consciousness, learning materials, security tools and tips shall be articulated, localized and transmitted online to safeguard the most critical asset of the nation, i.e. her people.

- The Strategy on National Internet Safety is a response to the national need to *plug in* the National Internet Safety capability gap within the currently emerging cybersecurity in the country.

- The initiative fits into the framework of National Cybersecurity Policy, National Security Strategy and National ICT policy.

- The strategy is a product of intensive research, outcome of critical needs assessment, recommendations of various fora and wider consultations on the criticality of pubic internet safety and online vulnerability in Nigeria.

- During the Nigeria Internet Governance Forum (NIGF 2013), it was estimated that over 95% of Nigerian on the internet are ignorant of personal security and safety responsibility online.

- The weakest link within a cybersecurity chain of any country is her people. Therefore, this Strategy provides initiatives and measures that help safeguard general public internet users, provide materials and facilitate tools to help safeguard Nigerian citizens against cyber threats and unwholesome vulnerability.

- The Strategy is focusing on the development and implementation of National Internet Safety Initiative (NISI) under the structural framework and coordination of NCCC.

11.2 National Internet Safety Initiative

- The initiative is a multi-disciplinary *Initiative* that help safeguard Nigerian citizens' presence on the Internet.

- This is a unique home grown government intervention vehicle which seeks to help the nation protect her citizens against her own digital vulnerability and online threats, safeguards the vulnerable groups, and re-channel her citizens online engagement towards a rewarding experience that impact the socio-economic development and healthy digital lifestyles in cyberspace.

- The initiative is anchored on National Cybersecurity Strategy i.e. the strategy is expected to be built through multi-stakeholder engagement.

- It addresses internet safety and online security from the perspective of local and global peculiarities.

- The strategy marshalled counter-measure policy guidelines, roadmap strategy, local ideas, tested tools and materials for the delivery of the initiative.

11.3 Objective

- The overall objective is to facilitate a unifying Nigeria Internet security literacy programs, open ended, with workable guidelines, and with implementation strategy that will engage Nigerians online and safeguard Nigerian public Internet users.

11.4 Scope:

- The initiative scope is focused on Nigerian public internet users covering the following areas which can hamper National Security, economy growth and local innovations.

  i. Blacklisting Inappropriate contents
  ii. Online backdoor distributive channels
  iii. Misuse and abuse of critical internet resources
  iv. User abuse and exploitative materials
  v. Digital vandalism critical to national economic image and online presence
  vi. Internet security and online safety illiteracy
  vii. Non-alliance countermeasures

viii. Local peculiarity & literacy gap

11.5 Initiative

i. Establish a strong NISI presence under an effective multi-stakeholder engagement framework.

ii. Designate NISI counter-measure advocacy requires to address online security and safety awareness and protection of Nigeria Citizens online.

iii. Initiate a national road shows- public awareness and education campaign to promote Citizen Online Safety & Protection in Nigeria.

iv. Setting up NISI hub under NCCC with capability for collaborating Network through which stakeholders can plug-in and interface with tools, materials programs, initiatives within the country.

v. Build public internet safety emergency readiness, national advocacy and awareness gateway which will fit into the emerging e-security ecosystem thus complimenting existing countermeasure efforts from various government agencies and private sector.

vi. Development of monitoring tools and evaluation process to help safeguard local internet community and critical presence.

vii. Building an indigenous capability for local internet presence, security and safety research and development.

viii. Development of local IT tools, materials, contents and software applications appropriate for ensuring internet security and safety of the citizens.

ix. Create local Internet Safety Wall using countermeasures awareness, interactions and information sharing.

x. Establish response mechanism and measures for public alert system

11.6 Importance of NISI to NCCC

- Today, more than ever, government sees a real urgency to get the message out to the community about the emerging threats and abuses of the citizens on the internet. It is within the purview of ONSA through the National Cybersecurity Strategy to provide guidance towards the development of home-grown innovative ideas, tools and materials that will help facilitate internet safety consciousness and online security learning aids to the citizens.

- The initiative is an important focus of NCSS to help design, develop, advocate, train and sustainably deliver resources to government, corporate and individual citizens, families and key players to raise awareness on National Internet safety to make the online community a safe place for productive engagement for government, businesses, kids, young, adult people and families.

- The initiative helps reawaken the nation to its statutory role within the framework of National Cybersecurity Policy towards safeguarding Nigerian Online Presence, developing and implementing local strategies, guidelines and mobilization of all stakeholders to achieve this cause through enterprise and unified platform of National Cybersecurity Coordinating Center.