FEDERAL REPUBLIC OF NIGERIA

NATIONAL CYBERSECURITY POLICY AND STRATEGY

FEBRUARY 2021

NATIONAL CYBERSECURITY POLICY AND STRATEGY

UNITY AND FAITH, PEACE AND PROGRESS

FEDERAL REPUBLIC OF NIGERIA

FEBRUARY 2021

FOREWORD

At the start of the second term of my administration in 2019, we laid out clear national objectives and affirmed our commitment to address some of the most critical issues facing the country. To this end, we set our focus and priority on tackling insecurity, strengthening our economy and fighting corruption, as the pathway for progressive and sustainable national development. An integral part of our approach to confronting these issues has been to hinge on the opportunities offered by the current technological and digital revolution. This approach stems from the recognition that our country is blessed with a large, young and entrepreneurial population, which offers us the unique opportunity to fully exploit the benefits of Information and Communications Technology (ICT) and the current digital environment. Our course of action is also premised on our understanding that the digital environment is central and indispensable to our national and economic security. Based on this, over the last couple of years, we focused our efforts on several ICT-driven initiatives to propel the country towards the attainment of our national objectives.

In March 2020, we launched the National Broadband Plan (NBP) 2020 - 2025 to increase Internet and broadband penetration across the country as part of our Economic Recovery and Growth Plan (ERGP). We also released an Economic Sustainability Plan 2020 targeted at mitigating the effects of a deep recession and ensuring social stability and addressing long-standing economic vulnerabilities as envisaged in the ERGP. Furthermore, we spearheaded the implementation of several ICT-driven schemes such as the Treasury Single Account (TSA) and Bank Verification Number (BVN) to enhance accountability and improve delivery of commercial and financial services across the country. We also hinged on ICT to drive the implementation of our National Identity Program, Data Privacy and Protection Framework and several other national initiatives designed to encourage and increase the conduct of transactions and interactions as well as government functions over the Internet and cyber domain. The series of platforms provided by the cyber domain also serve as enabler for tackling some of the myriad of security challenges facing our country. Specifically, the cyber domain creates the nexus for synchronising the efforts of our security and law enforcement agencies towards curbing crime, irregular migration, human trafficking and arms proliferation amongst others, while improving road safety and border security as well as enhancing ongoing anti-banditry, anti-militancy and counter-insurgency operations. Furthermore, the cyber domain provides us with the platform to enhance accountability and transparency thereby supporting our unwavering resolve to combat corruption in the country.

Despite these notable achievements, our ability to effectively harness and fully exploit the benefits of the cyber domain is threatened by several inherent challenges. The recent expansive nature of the Internet has increased the proliferation and diversification of the threats in cyberspace. Similar to other countries, our cyberspace is faced with dangers posed by criminals constantly striving to perpetuate various forms of cyber attacks and crimes such as fraud, identity and intellectual property theft as well as elections interference and destruction of our critical infrastructure. We are also witnessing an increasing use of the Internet for propagation of seditious messages, fake news and hate speech. Moreover, the cyber domain now hosts an increasing pool of illicit actors including foreign and domestic groups, state and non-state elements, as well as lone wolves. The wide playing field offered by cyberspace has also attracted the attention of terrorists and other subversive elements who constantly strive to exploit cyberspace for indoctrination or propaganda and to undermine the government and cause apprehension towards the people. The criticality of the threats affecting our cyber domain has been further exacerbated by recent developments on the global stage. The outbreak of COVID-19 pandemic resulted in massive migration of the populace to cyberspace. The advent of 5G and emergence of other new technologies such as Artificial Intelligence, blockchain technology, cloud computing and Internet of Things have further widened the scope and threat landscape of our cyberspace.

Nonetheless, these challenges are not insurmountable. Beyond these multifaceted threats lie opportunities for us to mobilise as a nation, and develop our human resources and capacity across government and our private sector, to build a strong, resilient and secure national cyberspace. Our approach to national cybersecurity is the development of a robust and adaptive digital ecosystem based on mutual collaboration and synergy of the triad of government, academia and industry, reinforced by strong regional and international alliances. It is for this reason that our national cybersecurity is conceptualised as an integral and indispensable pillar of our national and economic security. We have already demonstrated our resolve and commitment to fully articulate our efforts towards enhancing our national cybersecurity. Our Cybercrimes (Prohibition, Prevention, Etc) Act 2015 empowers us with the legal framework for addressing cybercrime and enhancing our national cybersecurity. In 2014, we developed our maiden National Cybersecurity Policy and Strategy which set the direction for coordination of our engagements in cyberspace over the past 6 years. The cybersecurity programs, institutions and initiatives implemented over these past 6 years have helped to establish us as a formidable global and regional player in the digital domain.

Therefore, the rationale for review of the National Cybersecurity Policy and Strategy 2014 is to continue on this path of progress and build on previous achievements. The objective is also to realign our cybersecurity efforts to effectively confront the dynamic and emergent nature of threats in our cyberspace while hinging us closer to the attainment of our national security objectives. However, our quest for attainment of national security objectives goes beyond reaction to cyber threats. We must continue to coordinate and effectively harness the cybersecurity efforts of our private sector, academia, industry and civil society towards progressive national development. We must also synergise to develop the necessary human and technological capacity to harness the benefits of the digital space to accelerate positive economic transformation. The global disposition of the cyber domain also gives us the platform to renew our commitment to regional and international cooperation. These aforementioned aspirations are the basis for the development of this policy document.

The National Cybersecurity Policy and Strategy 2021 signifies the renewal of my promise and commitment to Nigeria’s national security and economic prosperity and it ensures that our National Cybersecurity Program is prioritised among other national exigencies in my administration.

I therefore endorse the document as the overarching policy and strategy framework for driving Nigeria’s cybersecurity efforts towards the attainment of our national objectives.

MBuhari.

MUHAMMADU BUHARI
President, Commander-in-Chief of the Armed Forces
Federal Republic of Nigeria

PREFACE

Nigeria, like several other countries across the globe, is currently witnessing a surge in digital transformation. Many activities are now migrating to the Internet especially with the advent of the COVID-19 pandemic and the emergence of new technologies. Consequently, Nigeria's cyberspace has become a centre stage for new business innovations, government functions and social interactions. This trend has created an opportunity for the country to realign its priorities and articulate efforts towards the attainment of stipulated national objectives. The current attributes of cyberspace also pave the requisite path for the adoption of new technologies, dismantling of barriers to commerce, reinforcement of economic posture and enhancement of seamless communication across borders. The opportunities offered by the cyberspace revolution also create a platform for the enhancement and effective synchronisation of the efforts of our intelligence, security and defence community towards addressing the myriads of security challenges confronting the country.

However, the increased dependence on cyberspace comes with risks that have significant national security and economic implications. The dynamic nature of cyber threats and the constantly evolving tactics of perpetrators of cybercrime pose serious risks to business, commercial and financial activities which are all now extensively reliant on cyberspace. These cyber threats also constitute hazards to everyday users of cyberspace which cut across government establishments, private sector and the general populace. Furthermore, these threats have the potential to compromise critical networks and systems leading to disruption of essential services. In most cases, these disruptions are perpetrated by individuals or groups using arrays of malicious activities and attacks motivated by financial gains, anti-government or terrorist related activities thus challenging the confidentiality, integrity and availability of data in the Nigerian cyberspace.

In a bid to address these multifaceted cyber threats and embolden the country for efficient and progressive use of the cyber domain, the Federal Government of Nigeria (FGN), through the Office of the National Security Adviser (ONSA), undertook several proactive steps to draw the necessary cybersecurity roadmap for Nigeria. In this light, the National Cybersecurity Policy and Strategy 2014 was developed to provide direction for mainstreaming Nigeria's National Cybersecurity Program and set the path for effective coordination of the activities of all relevant stakeholders across government, academia and the private sector to handle the dynamism of security threats in the cyber domain. The Cybercrimes (Prohibition, Prevention, Etc) Act 2015 was also developed and signed into law as the legal and regulatory framework for the implementation and governance of national cybersecurity in the country. However, in view of the emergent nature of cyber threats as well as the constantly evolving technological and socio-economic imperatives that depend on the cyber domain, provisions were made for the review of the national cybersecurity policy and strategy every 5 years, in line with global best practices. The focus was also to hinge on the significant progress in cybersecurity made by the country between 2014 and 2021 while also realigning efforts with the objectives of Nigeria's National Security Strategy 2019.

Against this backdrop, and on behalf of His Excellency, President Muhammadu Buhari GCFR, ONSA convened a multi-stakeholder committee comprising representatives from all spheres of the Nigerian cybersecurity ecosystem, to develop a comprehensive National Cybersecurity Policy and Strategy 2021 for the common good of the country. The document is an all-inclusive policy and strategy framework which focuses on; strengthening cybersecurity governance and coordination, fostering protection of critical national information infrastructure, enhancing incident response, strengthening legal and regulatory framework, developing cyber defence capability, promoting the digital economy, improving assurance monitoring and fostering regional and international cooperation. The document is the output of an equitable collaborative effort which captures the shared responsibility for articulating Nigeria's engagements in cyberspace. It will serve as a strategic roadmap for all stakeholders in the country to come together and drive the attainment of the national cybersecurity objectives. In furtherance of this, the focus will move to the monitoring and evaluation of the implementation of the proffered initiatives. To this end, ONSA will continue to coordinate efforts of stakeholders and pave way for the use of the cyber domain to foster the realisation of Nigeria's national objectives.

BABAGANA MONGUNO
Major General (Retired)
National Security Adviser to the President
Federal Republic of Nigeria

ACRONYMS

ACIS	Auto Cyber Indicator Sharing
ATCON	Association of Telecommunications Companies of Nigeria
AU	African Union
CAC	Cybercrime Advisory Council
CAM	Child Abuse Materials
CEMS	Cyber Emergency Monitoring System
CERT	Computer Emergency Response Team
CIIMP	Critical Information Infrastructure Measurable Program
CIIPR	Critical Information Infrastructure Protection and Resilience
CIPMA	Critical Infrastructure Program for Modelling and Analysis
CNII	Critical National Information Infrastructure
CNIIPP	Critical National Information Infrastructure Protection Plan
CPA	Cybercrimes (Prohibition, Prevention, Etc) Act
CSEAN	Cyber Security Experts Association of Nigeria
CSIRT	Computer Security Incident Response Team
DSA	Defence Space Administration
ECOWAS	Economic Community of West African States
ERGP	Economic Recovery and Growth Plan
FGN	Federal Government of Nigeria
FMCDE	Federal Ministry of Communications and Digital Economy
FMITI	Federal Ministry of Industry Trade and Investment
FMoE	Federal Ministry of Education
FMoF	Federal Ministry of Finance
FMoJ	Federal Ministry of Justice
FMST	Federal Ministry of Science and Technology
FMWASD	Federal Ministry of Women Affairs and Social Development
ICT	Information and Communications Technology
IP	Internet Protocol
ISP	Internet Service Provider
ISPAN	Internet Service Providers Association of Nigeria
IXP	Internet Exchange Point
LEAs	Law Enforcement Agencies
MFA	Ministry of Foreign Affairs

MOD	Ministry of Defence
NACWC	Nigerian Army Cyber Warfare Command
NAN	News Agency of Nigeria
NASS	National Assembly
NBC	National Broadcasting Commission
NCAM	National Cybersecurity Awareness Month
NCC	Nigerian Communications Commission
NCCC	National Cybersecurity Coordination Centre
NCDP	National Cyber Defence Plan
NCF	National Cybersecurity Fund
NCPS	National Cybersecurity Policy and Strategy
NCTI	National Cybersecurity Training Institute
NEMA	National Emergency Management Agency
ngCERT	Nigeria Computer Emergency Response Team
NGO	Non-Governmental Organisation
NIIA	Nigerian Institute of International Affairs
NIMC	National Identity Management Commission
NIRA	Nigeria Internet Registration Association
NITDA	National Information Technology Development Agency
NITDEF	National Information Technology Development Fund
NNBP	Nigerian National Broadband Plan
NOA	National Orientation Agency
NOTAP	National Office for Technology Acquisition and Promotion
NSA	National Security Adviser
NTWG	National Technical Working Group
NVA	National Vulnerability Assessment
OCWAR-C	Organised Crime: West African Response on Cybersecurity and Fight against Cybercrime
ONSA	Office of the National Security Adviser
OSGF	Office of the Secretary to the Government of the Federation
PoC	Point of Contact
PPP	Public Private Partnership
SOC	Security Operations Centre
TETFund	Tertiary Education Trust Fund
TISN	Trusted Information Sharing Network
TSA	Treasury Single Account
UAVs	Unmanned Aerial Vehicles
UNGA	United Nations General Assembly
USPF	Universal Service Provision Fund

TABLE OF CONTENTS

VISION AND MISSION

VISION

A safe and secure digital community that provides opportunities for its citizenry and promotes peaceful and proactive engagements in cyberspace for enhanced national prosperity

MISSION

To foster a trusted cyber environment that optimises Nigeria's cybersecurity readiness and coordination capacities towards addressing the nation's cyber risk exposure

EXECUTIVE SUMMARY

Technological advancements have resulted in a variety of breakthroughs, a preponderance of which has been evident over the past decades by the growth of Information and Communications Technology (ICT) and the evolution of the Internet. These ICT and Internet-driven developments are actualised in almost all facets of life and the ensuing transformations have resulted in heavy dependence on the cyber domain. In Nigeria, the evolution, growth and adoption of ICT and the Internet has been at an accelerated pace since the turn of the 21st Century. The country has predominantly embraced ICT and the Internet to drive new initiatives and reach new milestones. A reflection of this is apparent in the high rate of adoption of new technologies, the proliferation of foreign-based technology conglomerates in the Nigerian market as well as the rising number of indigenous technology firms across the country. These new dependencies have transformed Nigeria's cyber domain to a potent game changer in the affairs of peace, security and economic progression. Essentially, the Nigerian economy, government functions and the provision of essential services now rely on the integrity of cyberspace. This new digital era presents significant opportunities to enhance Nigeria's readiness for global economic competitiveness and repositioning for national development.

However, there are several downsides attributed to the widespread use of the cyber domain. Some of these downsides, which are also reflected on the global scale, have profound implications for the nation's security and economic wellbeing. From the threats posed by cybercrime and cyber terrorism, to the dangers emanating from cyber espionage and the use of Internet social media for propagation of hate speech and seditious messages, as well as the risks of breaches to sensitive personal and government data, it is almost impossible to overstate the challenges. In the light of these dynamic challenges and threats, it is crucial for the Nigerian cyber ecosystem to undergo major periodic reforms to better position the nation to effectively harness the benefits of the digital revolution.

Therefore, it is not coincidental that the Federal Government of Nigeria (FGN) developed a national framework for cybersecurity following the approach of several other countries and in line with the exigent national priorities and realities of the country. This national framework, codified as the National Cybersecurity Policy and Strategy, set the clear direction for coordination of Nigeria's cybersecurity engagements in recognition of cyberspace as the fifth domain, and as part of efforts to protect the national interests and sovereignty of the country. Furthermore, with due cognisance of the dynamic nature of threats in cyberspace, provisions were made for review and update of the National Cybersecurity Policy and Strategy, every 5 years in line with global best practices.

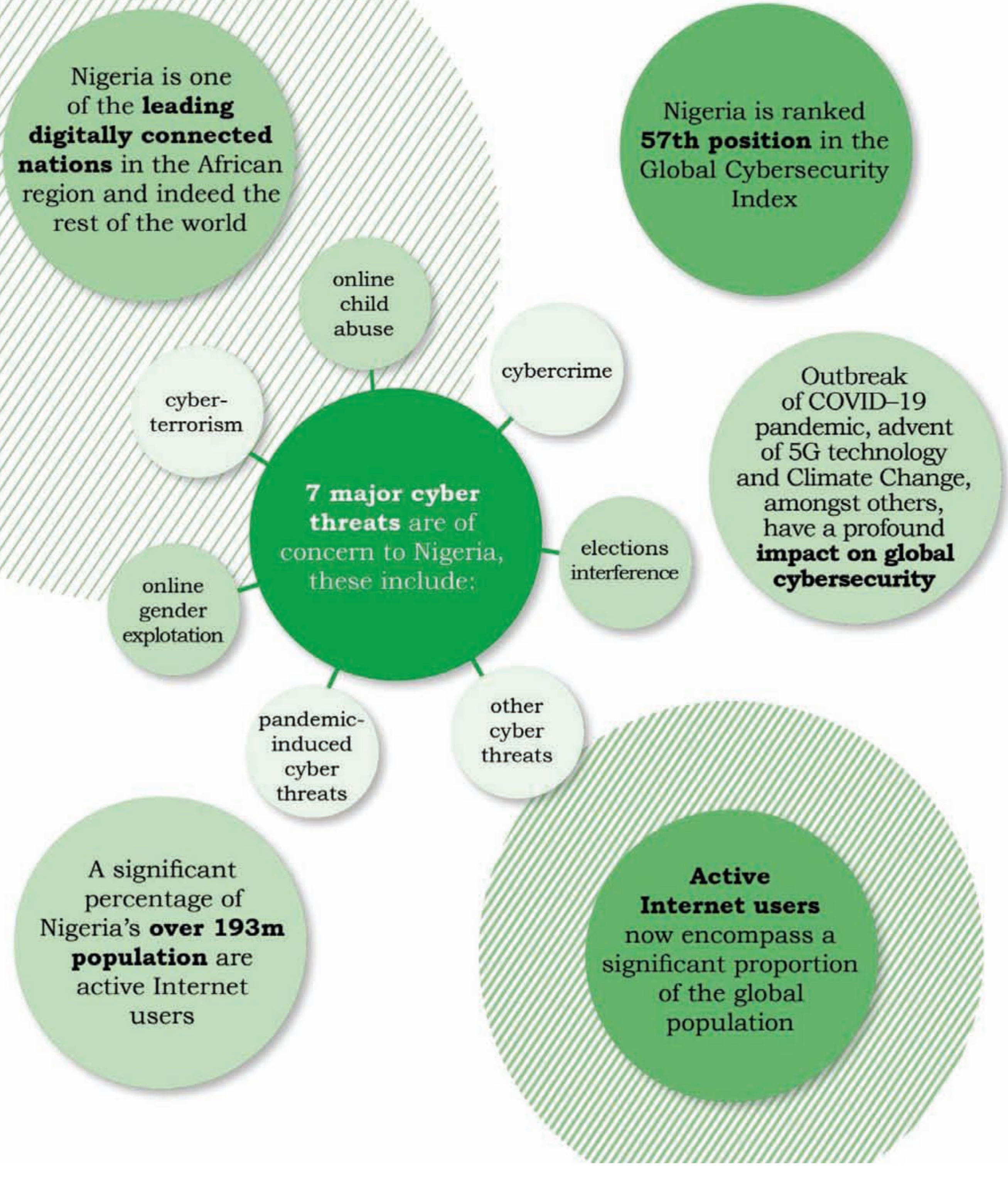
Against this backdrop, the National Cybersecurity Policy and Strategy 2014 was reviewed based on a whole-of-government and multi-stakeholder approach. This culminated in the development of the National Cybersecurity Policy and Strategy 2021 as a purposeful and living document to facilitate the attainment of a secure and resilient Nigerian cyberspace. The document is a confluence of ends, ways and means which emplaces our National Cybersecurity Programme on 8 critical pillars, namely:

- Strengthening Cybersecurity Governance and Coordination
- Fostering Protection of Critical National Information Infrastructure
- Enhancing Cybersecurity Incident Management
- Strengthening Legal and Regulatory Framework
- Enhancing Cyber Defence Capability
- Promoting a Thriving Digital Economy
- Assurance Monitoring and Evaluation
- Enhancing International Cooperation

To this end, we shall establish a national structure to enhance the coordination and cohesion of all our cybersecurity activities and multi-stakeholder efforts. We will also align our direction for ensuring the security and resilience of our critical infrastructure, through collaborative partnership and development of a robust protection plan. Furthermore, we will strengthen our incident response capability through improved information sharing, enhanced crisis management and comprehensive technical training of incident response teams. Additionally, we will build our cyber defence capability through extensive training programmes for our military and other security agencies. Also, we will enhance our capacity to tackle cybercrime by amending our existing legislation and building the capacity of our law enforcement and judiciary. In the area of the economy, we will promote a thriving digital environment by fostering a trusted Internet, launching widespread awareness programmes and engendering extensive development of our human resources. We will also embrace indigenous technological innovations as well as research and development to better empower us to tackle the new and emerging threats in cyberspace. Considering that cybercrimes can occur across international jurisdictions, government will exploit both regional and global collaborative mechanisms to address the use of cyberspace for activities detrimental to our national security. Our country will also continue the promotion of regional and global cooperation in cybersecurity towards strengthening international security, peace and prosperity.

CHAPTER ONE

Overview of Nigeria's Cybersecurity Environment



Nigeria is one of the **leading digitally connected nations** in the African region and indeed the rest of the world

Nigeria is ranked **57th position** in the Global Cybersecurity Index

7 major cyber threats are of concern to Nigeria, these include:

- online child abuse
- cybercrime
- elections interference
- other cyber threats
- pandemic-induced cyber threats
- online gender explotation
- cyber-terrorism

Outbreak of COVID–19 pandemic, advent of 5G technology and Climate Change, amongst others, have a profound **impact on global cybersecurity**

A significant percentage of Nigeria's **over 193m population** are active Internet users

Active Internet users now encompass a significant proportion of the global population

CHAPTER 1

OVERVIEW OF NIGERIA’S CYBERSECURITY ENVIRONMENT

This overview provides substantial information on the current state of cybersecurity in Nigeria. It reflects on the predominant cybersecurity trends on the global stage as the prerequisite for underscoring the current cybersecurity posture of the country. Thereafter, it gives a highlight of Nigeria's current cybersecurity landscape and a summary of the nation's cyber threat profile. This is followed by a brief examination of the country's existing cybersecurity weaknesses and strengths in a bid to identify gaps and spell out the rationale for the institution of this National Cybersecurity Policy and Strategy 2021.

1.1 GLOBAL CONTEXT

Over the last decade, the digital environment across the globe has witnessed exponential growth and intensive adoption of information and communication technologies (ICT). It is intuitive that active Internet users now encompass a significant proportion of the global population. This trend is driven by the rapid increase in the use of mobile devices worldwide and the surge in the social media. The current global digital revolution has birthed the emergence of new technologies including artificial intelligence, cloud computing, blockchain technology and Internet of Things, amongst others. As a result of this digital revolution, cybersecurity is no longer viewed as a mere technical issue. Rather, cybersecurity is now approached as a multi-faceted global concern. This multivariate nature of cybersecurity has informed the different yet convergent approaches by nations of the world in dealing with cyber threats.

Other recent developments across the globe have impacted on cybersecurity. The outbreak of COVID-19 pandemic informed a rise in remote working and widespread adoption of online collaboration, increase in cloud services and rise in electronic transactions, with attendant increase in the potential impacts of cyber threats. The challenges of global security posed by state and non-state actors also have a significant impact on cybersecurity. The use of cyber operations by actors to achieve strategic objectives or economic influence is becoming more common and intense. Similarly, other issues such as the advent of 5G technology and climate change may have a profound impact on the global digital landscape. Cybersecurity is therefore an extensive challenge, which requires enhanced international cooperation to successfully attain an acceptable level of confidence and trust at national and global levels.

1.2 NIGERIA'S CYBERSECURITY LANDSCAPE

Nigeria is at a centre stage in the current cyberspace revolution. In the area of ICT, Nigeria is one of the leading digitally connected nations in the African region and indeed the rest of the world. This is evident from the widespread adoption of ICT across the country. The high number of technology conglomerates and rising rate of indigenous ICT firms in the Nigerian market also point to the current and future potentials of the Nigerian cyberspace. With a population of over 193 million people, according to 2016 estimates by the Nigerian Population Commission, a significant percentage of the Nigerian populace are active Internet users.

In recognition of the potentials offered by the cyber domain, Nigeria has launched several initiatives to capitalise on the available opportunities. Nigeria’s National Digital Economy Policy and Strategy 2020 – 2030 and the Economic Sustainability Plan (ESP) 2020 – 2030 envisage an economy driven by ICT. Nigeria also formulated the National Broadband Plan 2020 - 2025 in line with the Economic Recovery and Growth Plan (ERGP) and the Presidential initiative to boost broadband penetration across the country. Furthermore, the Nigeria Data Protection Regulation 2019 was launched to provide guidelines for electronic data exchange while the Data Protection Bill 2020 is soon expected to be signed into law to facilitate enhanced security and privacy of personal data. The Nigerian private sector has also hinged on the benefits offered by the cyber domain. Commercial and business processes across Nigeria are now constantly migrating to new forms of cyber based technologies. Ultimately, Nigeria fully recognises the centrality and indispensability of the cyber domain to the attainment of national security and socio-economic prosperity.

1.3 NIGERIA'S CYBER THREAT PROFILE

The Nigerian cyberspace is faced with significant threats which result in huge financial losses corresponding to a substantial percentage of the country's Gross Domestic Product (GDP). Equally, a high number of organisations in Nigeria fall victim of cyber attacks, making the country a high target by perpetrators of cybercrime. Similarly, reports from the Nigerian Communications Commission (NCC) suggest that cyber attacks are one of the biggest threats to the country's telecommunications sector. The scale and multiplicity of these threats reinforce the need for us to adopt a whole-of-society approach to cybersecurity.

In line with the current trends in the global digital environment, the main targets of cyber attacks in the Nigerian cyberspace include cloud-based systems, mobile devices, Internet of Things, data centres and networks of corporate establishments, amongst others. Organisations in the financial sector are expected to face the highest cyber risks as reports from the Nigerian Interbank Settlement System (NIBSS) suggest that mobile fraud cases could likely rise. Furthermore, the expansion of cyber threats beyond computer systems and networks to cyber-physical systems such as transportation technologies, air traffic control systems, smart devices and hydropower grids, is another new reality that the country needs to cope with. The current appetite for social media is also prompting new methods of cyber attacks. In view of the foregoing, we have identified 7 major cyber threats of concern, the details are as follows:

1.3.1 Cybercrime

The common forms of cybercrime that feature in the Nigerian cyber domain include Phishing, Business Email Compromise (BEC), ransomware and malwares as well as credentials theft, intellectual property rights violation and online scam amongst others. Nigeria is also mindful of emerging cyber threats such as Machine Learning Poisoning, Deep Fakes, Cloud Hijacking, Artificial Intelligence Fuzzing and Crypto Currency Hacking, amongst others. The expanding pool of data in the Nigerian cyberspace is also indicative of a potential rise in the number of targeted data breaches. Also, the wanton drive for high value currencies by individual or organised cyber criminals has resulted in a predominant rise in international fraud and scams with attendant impact on the country’s national image.

1.3.2 Cyber Terrorism and Terrorists Use of the Internet

The current thriving nature of the Nigerian cyberspace has drawn the attention of domestic and transnational terrorist groups. There is now an increasing likelihood for cyber terrorists to use cyberspace to inflict violence through the targeting of critical assets including, financial systems, military networks, transportation infrastructure, telecommunications systems and government services, amongst others. Terrorists and other organised illicit groups have also mastered the use of cyberspace to enhance their operations or cause apprehension through spreading of fake news and hate speech. In addition, the use of social media by terrorists for recruitment and propaganda is a featuring threat in the Nigerian cyberspace. The typical overall objective of these wanton actors is to use cyberspace to undermine the government and instil a sense of fear or siege on the populace.

1.3.3 Online Child Abuse and Exploitation

Nigeria recognises the importance of the protection and safety of the younger generation and their vulnerabilities in cyberspace. In this light, the country stands against online child abuse and exploitation. Activities classified under this unwholesome practice take place on the Internet or through the use of information systems such as mobile devices. Perpetrators of online abuse of children are also leveraging social media and emerging cyberspace technologies to carry out cyberbullying, online harassment and sexual molestation of children and other vulnerable individuals amongst others.

1.3.4 Online Gender Exploitation

We recognise that abuse and gender violence takes place in cyberspace. We are therefore committed to combating these illicit activities. As Nigerians of all gender are getting increasingly connected to the Internet and getting more involved in cyber related activities, there is a rise in cases of gender violence, online sexual harassment, cyber-stalking, Internet-induced kidnapping, rape, black mailing and cyberbullying amongst others. Increasingly, several Nigerians irrespective of gender across all spheres of society are falling victim to predominant cyber threats such as online defamation, public shaming and identity theft, amongst others. These unwholesome acts have the potentials to result in psychological or mental health challenges for victims.

1.3.5 Elections Interference

Elections are foundational to the liberal democracy entrenched in our national endeavours to ensure the wellbeing and stability of the nation. Hence, Nigeria must be prepared to contend with the major threats of the use of cyberspace for perpetrating elections interference or violence. As society incrementally embraces digitisation and as the election process itself becomes more dependent on digital technologies, domestic, external, state and non-state actors have the potential to leverage cyberspace and interfere with the electoral process. These threats could range from direct physical attack on elections critical infrastructure or the conduct of cyber operations to disrupt systems or influence the electorate.

1.3.6 Pandemic-Induced Cyber Threats

The COVID-19 pandemic forced organisations and people across Nigeria to move their activities to cyberspace. The pandemic also resulted in acute changes and innovations in governance and business processes which are more likely to remain in the long-term. Pandemic-induced migration into cyberspace has also changed the nature of threats and increased the risks and potential impacts of cyber attacks. Essentially, the attack playing field for cybercriminals has now widened. There is now a rise in cases of email scam or compromise of global and regional health palliative programmes including several reports of cybercriminals masquerading as legitimate agencies to perpetrate fraud and illegalities. Data theft, cloud compromise and teleconference hijacking are also major challenges associated with the pandemic-era.

1.3.7 Other Cyber Threats

Nigeria is also conscious of the myriad of other predominant and emerging security threats emanating from cyber space such as fragmentation of technology, Advanced Persistent Threats (APTs), cyber conflict, as well as cyber threats posed by climate change and Unmanned Aerial Vehicles (UAVs) amongst others, which could be perpetrated by nation states or non-state actors with the objective of compromising our critical services and undermining our economy and national security. These rapidly changing strategic cyber threats, by a foreign actor or actors, could make our infrastructure susceptible to eaves dropping, military or industrial espionage or other malicious activities.

1.4 WEAKNESSES AND VULNERABILITIES

As a principle of risk management and resilience, it is crucial to identify the major weaknesses and vulnerabilities in the Nigerian cybersecurity ecosystem. The World Bank Digital Economy Diagnostic

Report 2019 noted that shortfalls in human resources capacity development and accessibility to digital technologies are factors limiting cybersecurity development in Nigeria. Similarly, the International Telecommunication Union Global Cybersecurity Index 2018, which surveyed the cybersecurity readiness of member states based on legal, technical, organisational, cooperation and capacity development, ranked Nigeria 57th position out of the 155 countries surveyed across the globe. Moreover, Nigeria currently relies largely on foreign ICT and cybersecurity solutions and technologies.

Human resource capacity, research and development, and awareness on cybersecurity are still relatively low in Nigeria cutting across government, private sector and society in general. This shortfall has been responsible for diminished cybersecurity consciousness at the organisational and individual levels. Consequently, the level of attention and commitment of resources towards cybersecurity is unable to keep pace with the requirements of current ICT and the predominance of evolving cyber threats.

1.5 OUR STRENGTHS

Despite the current cyber threat profile, Nigeria has a strong commitment to defend her citizens, safeguard operations of critical infrastructure and ensure continuity of services. The Federal Government of Nigeria is also conscious of the benefits of the cyber domain and its potential for enhancing the country's economic prosperity. Hence, there is concerted mobilisation of national multi-stakeholder efforts to ensure that the opportunities are exploited and the challenges are effectively mitigated. The programmes, initiatives and frameworks spearheaded by Government, such as the National Cybersecurity Policy and Strategy 2014, the Cybercrimes (Prohibition, Prevention, Etc) (CPA) Act 2015, the Nigerian Data Protection Regulation 2019, National Broadband Plan 2020 – 2025 and National Digital Economic Policy and Strategy 2020 – 2030, amongst several others, have engendered significant improvements to cybersecurity in Nigeria.

Nigeria is also blessed with a proactive and informed private sector that is well placed to play a leading role in the regional and indeed global cybersecurity solutions market. The year 2019 saw an increase in uptake of cybersecurity monitoring capabilities to keep pace and protect operations and infrastructure from cyber attacks. The country's multi-stakeholder National Cybercrime Advisory Council (CAC), has spearheaded several efforts to provide strategic direction for cybersecurity in Nigeria. On the regional and international arena, Nigeria collaborates with partners such as the ECOWAS Commission and Organised Crime: West African Response on Cybersecurity and Fight against Cybercrime (OCWAR-C), amongst others, to further enhance cybersecurity. In 2018, the country in collaboration with other international partners, conducted a Cybersecurity Capacity Review for Nigeria.

CHAPTER TWO

National Cybersecurity Policy Direction

3 national **OBJECTIVES** for the Nigerian people

Protecting National Security

Strengthening Economic Development

Fighting Corruption

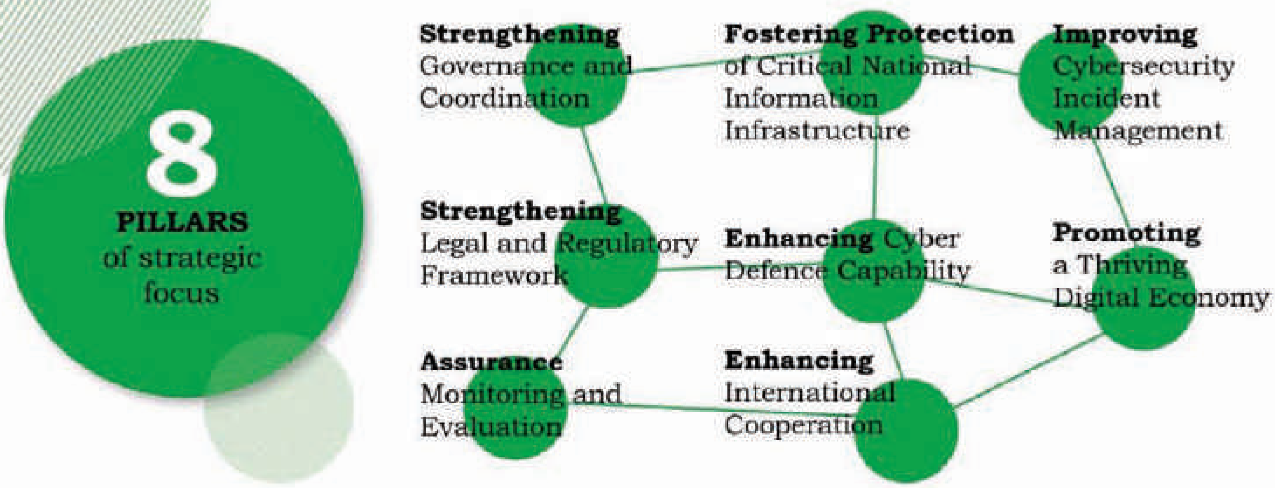
4 Fundamental national cybersecurity **CONSIDERATIONS**

Security and wellbeing of the Nigerian people is as important in the cyber domain as it is in the physical domain

Cybersecurity is a **critical enabler** of economic progression and development

Technology development is critical to the attainment of Nigeria's national priorities

Regional and international collaboration is central and crucial to cybersecurity



8 **PILLARS** of strategic focus

Strengthening Governance and Coordination

Fostering Protection of Critical National Information Infrastructure

Improving Cybersecurity Incident Management

Strengthening Legal and Regulatory Framework

Enhancing Cyber Defence Capability

Promoting a Thriving Digital Economy

Assurance Monitoring and Evaluation

Enhancing International Cooperation

CHAPTER 2

NATIONAL CYBERSECURITY POLICY DIRECTION

This policy direction outlines Nigeria's national priorities, national security imperatives and cyberspace doctrines which cumulatively inform the country's cybersecurity policy initiatives and strategic actions.

2.1 NATIONAL PRIORITIES

Our approach to cybersecurity is anchored on enduring national values, interests and objectives which define who we are as a people and our collective behaviour and commitment to the advancement of nationhood. These factors also guide the formulation of our national cybersecurity policy and strategy while strengthening our commitment to the delivery of the promises of peace, security, freedom, democracy, equality, justice, preservation of human rights, promotion of women rights, safeguarding of individual liberties and respect for the rule of law. Furthermore, our national cybersecurity objectives, policy initiatives and strategic actions are formulated to retain and renew Nigeria's commitment to the preservation of the nation's sovereignty, territorial integrity, human security, prosperity and wellbeing of the people. This approach to cybersecurity is also closely aligned with our commitment to uphold regional and international peace, and security cooperation while embracing the norms and conventions of international law.

2.1.1 National Cybersecurity Policy Considerations

In 2019, the Federal Government of Nigeria outlined 3 cardinal and existential national objectives for the Nigerian people. These include: Protecting National Security; Strengthening Economic Development; and Fighting Corruption. The National Cybersecurity Policy and Strategy therefore supports these national objectives through 4 fundamental national cybersecurity policy considerations as follows:

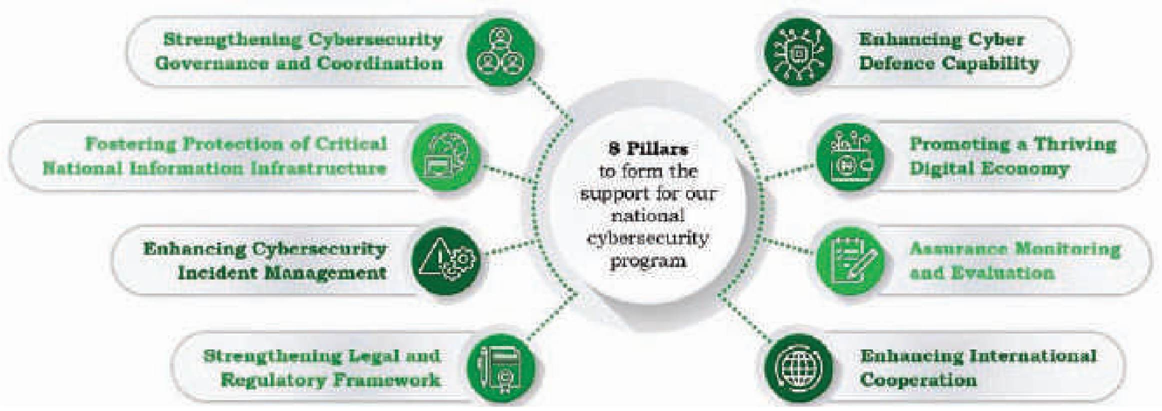
- The security and wellbeing of the Nigerian people is as important in the cyber domain as it is in the physical domain.
- Cybersecurity is a critical enabler of economic progression and development.

- Technology development is critical to the attainment of Nigeria's national priorities.
- Regional and international collaboration is central and crucial to cybersecurity.

Therefore, we recognise that each of these policy considerations requires a set of focused and coordinated strategic actions. This will provide the necessary platform for sound planning and performance tracking towards the execution of our national cybersecurity strategy, thereby enabling all stakeholders to stay focused on delivering the required collective mandate.

2.2 STRATEGIC AREAS OF FOCUS

The overall purpose of the national cybersecurity policy is to set a unified agenda and new direction for our national cybersecurity programme through prioritisation of national requirements. Our strategic areas of focus are based on 8 pillars which form the support for our national cybersecurity programme.


8 Pillars to form the support for our national cybersecurity program
Strengthening Cybersecurity Governance and Coordination
Fostering Protection of Critical National Information Infrastructure
Enhancing Cybersecurity Incident Management
Strengthening Legal and Regulatory Framework
Enhancing Cyber Defence Capability
Promoting a Thriving Digital Economy
Assurance Monitoring and Evaluation
Enhancing International Cooperation

These pillars create the foundation for the delivery of our national objectives and align the direction of all key stakeholders that have a role to play in the enhancement of the progressive use of the Nigerian cyberspace.

2.3 RISK-BASED APPROACH TO NATIONAL CYBERSECURITY

Our cybersecurity policy acknowledges that, rather than forego the benefits of cyberspace in the interest of security, it is more productive for us to accept the likelihood of cyber attacks, while proactively emplacing measures to protect the integrity of cyber infrastructure. On this premise, a sector-based approach to risk management will be adopted to balance security measures with potential benefits in recognition of the differences of each sector's risk profile and consequences of cyber-attack. Furthermore, the focus of the cybersecurity strategy is to prepare stakeholders, in the public and private sector, for the adoption of the risk-based mindset to cybersecurity through promotion of resilient disaster recovery, business continuity, access control and crisis management measures, amongst others. Additionally, we will ensure that our resiliency and recovery plans are adequately designed to address the envisaged cyber risks.

2.4 NATIONAL SECURITY IMPERATIVES

Our National Security Strategy 2019 identifies several issues that are likely to influence the country’s security priorities over the next 5 years. The ones which have a direct bearing on the Nigerian cyberspace include cybercrime, technological challenges, socio-political threats, hate speeches, fake news, terrorism, violent extremism, economic challenges, as well as regional and global security issues. In this light, the National Security Strategy recognises that cyberspace is critical to our quest to address these national security issues. However, the strategy also acknowledges that the Nigerian cyberspace is vulnerable to some major forms of cyber-attack, namely, cybercrime, cyber espionage, cyber conflict, cyber terrorism, interference and destruction of critical national infrastructure and influence operations. Therefore, the National Security Strategy proposes the increased deployment of cybersecurity measures to facilitate the protection of systems and structures against all forms of cyber attacks. The Strategy also emphasises the need for government-led approach as well as coordinated efforts across all sectors at various levels to secure our cyberspace.

2.4.1 Nigeria’s National Security Objectives

Our National Cybersecurity Policy and Strategy draws its strength from the National Security Strategy. It is therefore developed to support the pillars of the National Security Strategy. Furthermore, the national cybersecurity objectives are formulated according to the national objectives spelt out in the National Security Strategy, which include:

- Protecting the Nigerian People and Territory
- Promoting Economic Prosperity and Sustainable Development
- Promoting National Unity and Peaceful Co-existence
- Enhancing Regional and International Interests

Government stakeholders will therefore collaborate with the private sector, academia and industry to hinge on cybersecurity and facilitate the realisation of these objectives.

2.5 NATIONAL CYBERSPACE DOCTRINES

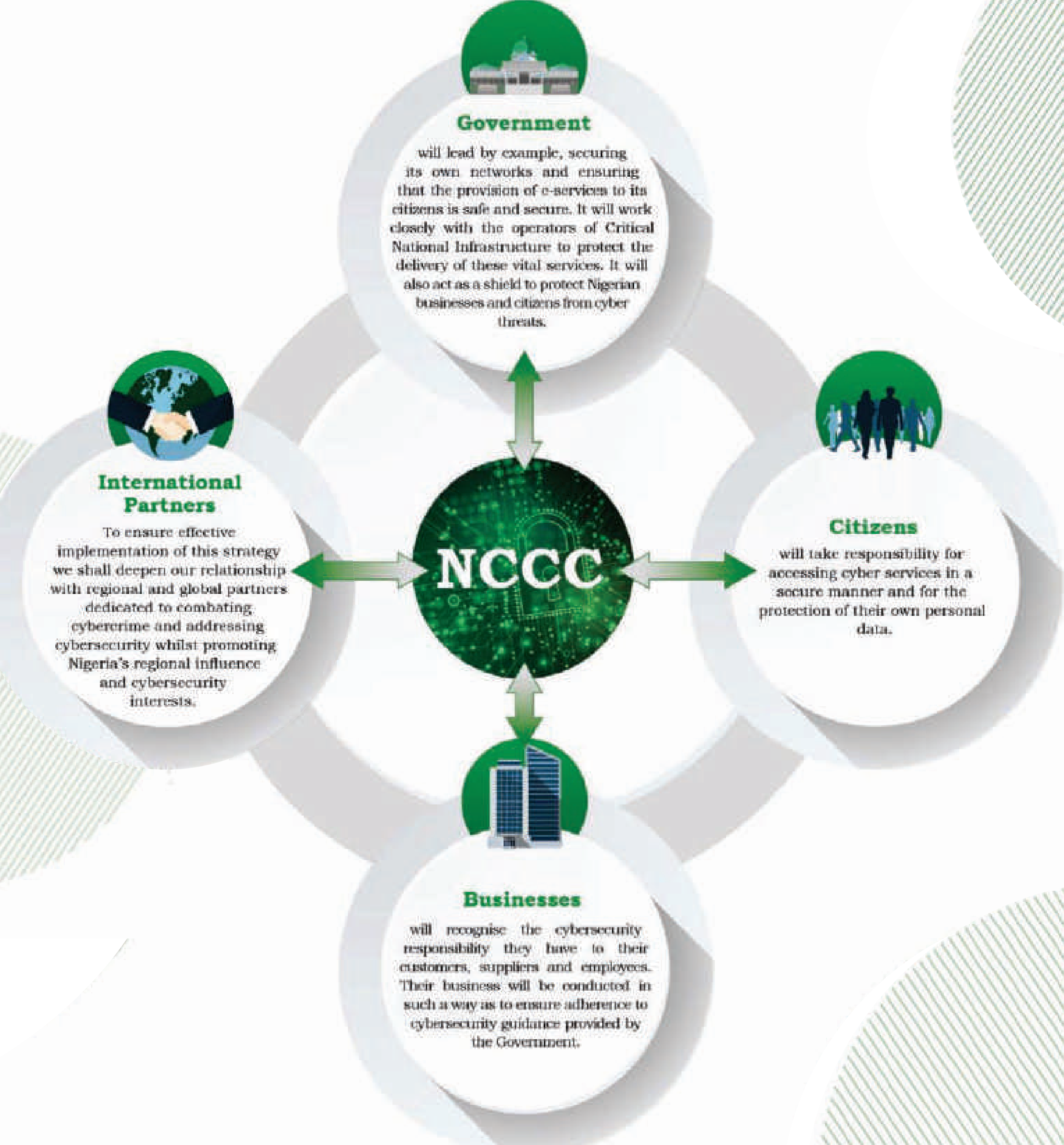
Nigeria shall continue to make the interests of its citizens the priority of her national cybersecurity strategy. Safeguarding the Nation’s information infrastructure is vital to fulfilling this objective. Nigeria will therefore put in place the mandatory framework to facilitate necessary multi-stakeholders collaborative and coordinated actions to safeguard and secure its critical infrastructure, within its jurisdiction. Nigeria will also emplace robust processes and functional world-class systems to promote trust and confidence in the use of its cyberspace.

We will enhance our preparedness to combat emerging cyber threats by investing in People, Process and Technology to develop critical skill sets and assets to identify and repel any threats to our sovereignty and national security. Nigeria shall also continue to collaborate with local and international stakeholders to put in place infrastructure that will ensure national preparedness for global economic competitiveness in cyberspace.

Furthermore, Nigeria shall promote the economic benefits of cyberspace by sustaining the balance between citizens’ expectations on freedom of information and privacy as well as government responsibilities on cybersecurity. We also recognise the transformational capability of emerging technologies. Therefore, our approach is to mainstream a cybersecurity regulatory framework that aligns with our national interests as well as international commitment to e-governance and e-business. In addition, Nigeria is interconnected with other countries in the cyber domain and hence not insulated against irresponsible actions in cyberspace. Therefore, we will mainstream voluntary non-binding norms of responsible state behaviour in cyberspace through enhanced international awareness and engagement. We will also continue to enhance our cyber defence capability by investing in our military through skills and technological assets acquisition to facilitate effective monitoring, identification, prevention and repulsion of any cyber threats to our sovereignty and national security.

CHAPTER THREE

Strengthening Cybersecurity Governance and Coordination



Government

will lead by example, securing its own networks and ensuring that the provision of e-services to its citizens is safe and secure. It will work closely with the operators of Critical National Infrastructure to protect the delivery of these vital services. It will also act as a shield to protect Nigerian businesses and citizens from cyber threats.

International Partners

To ensure effective implementation of this strategy we shall deepen our relationship with regional and global partners dedicated to combating cybercrime and addressing cybersecurity whilst promoting Nigeria's regional influence and cybersecurity interests.

Citizens

will take responsibility for accessing cyber services in a secure manner and for the protection of their own personal data.

Businesses

will recognise the cybersecurity responsibility they have to their customers, suppliers and employees. Their business will be conducted in such a way as to ensure adherence to cybersecurity guidance provided by the Government.

CHAPTER 3

STRENGTHENING CYBERSECURITY GOVERNANCE AND COORDINATION

Nigeria recognises that an effective governance model and coordination mechanism is fundamental to the enhancement of national cybersecurity. To this end, a national structure is required to coordinate and facilitate the necessary national cohesion at the strategic, operational and tactical levels.

3.1 ESTABLISHMENT OF NATIONAL CYBERSECURITY COORDINATION CENTRE

In line with the provisions of Section 41 of the Cybercrimes (Prohibition, Prevention, Etc) Act 2015 (The Act) which empowers the Office of the National Security Adviser to be the coordinating body for national cybersecurity, the National Security Adviser (NSA) shall establish the National Cybersecurity Coordination Centre (NCCC) to ensure the implementation of Nigeria's national cybersecurity programme in accordance with the provisions of relevant laws and international principles. The NCCC shall be the local and international focal point for cybersecurity in Nigeria. Accordingly, a strategic structural model shall be adopted for the organisation, composition, operation and functioning of the NCCC consistent with the roles and responsibilities of the Office of the National Security Adviser, the National Cybercrime Advisory Council and other functional frameworks as encapsulated in The Act.

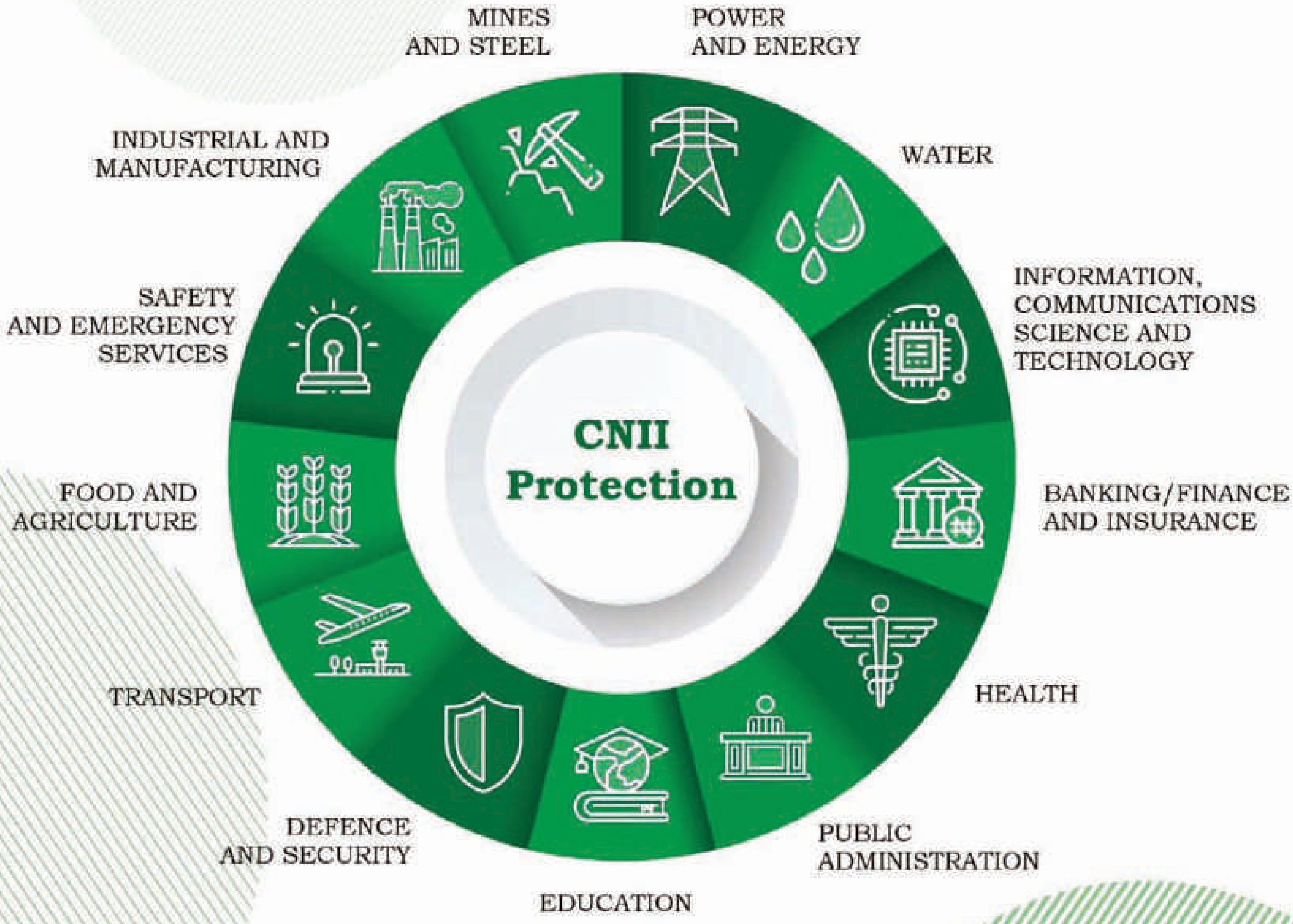
In accordance with Section 41 of The Act, a National Coordinator shall be appointed for the administration and running of the day to day functionalities of the NCCC. The NCCC shall be effectively organised, staffed and resourced to coordinate the activities of all stakeholders and ensure that cybersecurity in Nigeria is facilitated as a holistic whole-of-society effort that impacts the public and private sector, academia, industries, cybersecurity associations and advocacy groups as well as the international community.

3.2 RESPONSIBILITIES OF CYBERSECURITY STAKEHOLDERS

All stakeholders in the country's cyber ecosystem have specific and collective roles to play in ensuring the progressive use of the Nigerian cyberspace. Therefore, stakeholders must be aware of their responsibilities as catalyst for action, participation and seamless coordination of national cybersecurity. In accordance with the mandate of each stakeholder, NCCC in conjunction with all key players in the Nigerian cyberspace, shall identify and map out specific responsibilities for stakeholders to engender defined, convergent and unified efforts towards enhancing national cybersecurity. As a pathway to ensure alignment and synergy of efforts, we shall establish a Cybersecurity Dialogue Platform to enable stakeholders across Nigeria's cybersecurity ecosystem engage in the necessary discourse towards effective articulation of roles and responsibilities. Ultimately, the sustainability and critical success factor of our national cybersecurity programme is anchored on public-private partnership and multi-stakeholder engagement.

CHAPTER FOUR

Fostering Protection of Critical National Information Infrastructure


CNII Protection
MINES AND STEEL
POWER AND ENERGY
WATER
INFORMATION, COMMUNICATIONS SCIENCE AND TECHNOLOGY
BANKING/FINANCE AND INSURANCE
HEALTH
PUBLIC ADMINISTRATION
EDUCATION
DEFENCE AND SECURITY
TRANSPORT
FOOD AND AGRICULTURE
SAFETY AND EMERGENCY SERVICES
INDUSTRIAL AND MANUFACTURING

CHAPTER 4

FOSTERING PROTECTION OF CRITICAL NATIONAL INFORMATION INFRASTRUCTURE

The nation depends on the functioning of certain information and communications technology systems, networks and infrastructure to drive vital national imperatives such as economic development, commerce and financial transactions, social interactions, public safety, power and water supply, medical and health, government operations, national security and defence. These systems, networks and infrastructure underpin our national life and ensure our existence and survival as a country. Any disruption, destruction or interference to the operation of these assets has the potential to undermine government operations, social wellbeing, economic prosperity and national security.

Therefore, the Federal Government of Nigeria is committed to the development of necessary cohesive measures and strategic actions towards assuring the security and protection of these systems, networks and infrastructure. The Government therefore deems it crucial to designate such systems, networks and infrastructure as Critical National Information Infrastructure (CNII), as part of efforts to protect their integrity and assure their continued operation. To this end, Government has identified sectors across the Nigerian economy where critical ICT assets are domiciled, in order to pave a path for their designation as CNII. However, a key aspect of this process is the registration of CNII assets by the various owners and operators. For this purpose, Government created an online portal (publisher.cert.gov.ng) to enable stakeholders that own and operate these critical assets, to register the details of their infrastructure, as a pathway towards joint development of modalities for their protection.

This Strategy therefore presents the Government’s approach to CNII protection. The strategy acknowledges that CNII protection is a shared responsibility across government, private sector (the owners and operators of critical information infrastructure) and the entire populace. It is therefore our cardinal responsibility as a nation to complement Government efforts towards ensuring the protection and continuous operation of our CNII.

4.1 CRITICAL INFORMATION INFRASTRUCTURE PROTECTION AND RESILIENCE

The strategy articulates the various activities to be undertaken by Government and other stakeholders towards CNII protection. To this end, Nigeria will ensure a comprehensive approach to Critical Information Infrastructure Protection and Resilience (CIIPR) through the collective participation of stakeholders in the public and private sector, including owners and operators of CNII and the entire cybersecurity community. We will assess risks to CNII through an intelligent and information-led, risk management approach and secure CNII against physical, human and cyber threats through collective and sustainable efforts. Government will enhance CNII resilience by reducing impact of unforeseen and unexpected incidents through advanced planning and mitigation efforts, as well as effective responses aimed at saving lives and ensuring rapid recovery of essential services. We will also share relevant information across the CNII community to build awareness and enable coordinated risk-based decision making, while promoting learning and adaptation.

Nigeria will also ensure multi-stakeholder collaboration to set specific national priorities considering resource availability, progress already made, known capability gaps, and emerging trends and cybersecurity risks. These will drive implementation and will be supplemented by sectoral priorities. Performance measures will be set based on the goals and priorities of each sector. We will continue to develop appropriate categorisation of CNII in accordance with their priority for protection based on their vulnerability and impact assessment. Accordingly, we shall continue to update the comprehensive list of CNII that require protection priorities and disseminate the CNII list to all relevant stakeholders while developing CNII protection plan in line with this categorisation.

4.2 CRITICAL INFORMATION INFRASTRUCTURE SECTORS

A preliminary requirement for CIIPR is the identification of the sectors. Accordingly, this strategy identifies 13 critical information infrastructure sectors across the Nigerian economy.

4.2.1 Identified Sectors for CNII Protection

- Power and Energy
- Water
- Information, Communications, Science and Technology
- Banking/Finance and Insurance
- Health
- Public Administration
- Education
- Defence and Security
- Transport
- Food and Agriculture
- Safety and Emergency Services
- Industrial and Manufacturing
- Mines and Steel

4.3 STRATEGIC INITIATIVES

4.3.1 Establish Effective Collaborative Partnership with CNII Owners and Operators.

A significant proportion of the nation's critical infrastructure is privately owned or operated on a commercial basis. Therefore, partnership and collaboration will be engendered to help build confidence and reliability for the continued operation of CNII. To this end, a Trusted Information Sharing Network (TISN) shall be established under the NCCC as a forum in which the owners and operators of critical infrastructure would synergise and share information on threats and vulnerabilities as well as develop strategies and solutions to mitigate risks to the nation's CNII. The TISN shall comprise owners and operators of CNII as well as stakeholders from departments and agencies of government.

Stakeholders who own and operate CNII have a major undertaking and collective responsibility to ensure the security of their systems. Therefore, the NCCC shall promote a culture of risk awareness and shared responsibility across stakeholders for CNII protection. This culture shall be cascaded down to all individuals within the CNII protection community through a hybrid top-down and bottom-up approach. This will allow stakeholders across the sectors take ownership and develop specific and tailored approach to CNII protection in their various sectors.

4.3.2 Identify and Evaluate Potential Critical National Information Infrastructure

Government will work with owners and operators of critical infrastructure to ensure periodic and continuous identification of critical information infrastructure in the advent of emerging technologies. Government will also conduct periodic audit and evaluation to estimate the risk levels of the identified CNII. We will also adopt a risk-based approach in the identification and prioritisation for CNII protection.

4.3.3 Identify and Manage Cross-Sectoral Dependencies

Nigeria will continue to identify cyber risks that cut across more than one sector of the economy, or threats that affect multiple sectors of the economy simultaneously. This approach will assist CNII risk management decision-making and help to inform Government's actions on CIIPR. This approach also increases the potential for effective sharing of risks to cope with certain incidents. The Critical Infrastructure Program for Modelling and Analysis (CIPMA) is proposed as a suitable solution to enhance the protection and resilience of CNII in Nigeria.

Our strategy is to ensure that all sectors develop robust cyber risk management procedures and capabilities that are sector-specific and adaptive to emerging cyber threats in collaboration with other sectors and in conjunction with guidelines from NCCC. Nigeria shall establish a mechanism, through the TISN, for continuous information sharing between all CNII owners and operators as well as government stakeholders.

4.3.4 Redundancy Mechanism for CNII and Essential Services

Nigeria shall continue to promote the incorporation of redundancy mechanisms to enhance CNII protection. To this end, we shall ensure that backup mechanisms are developed to cater for communications disruption along any node in the emergency response network. We shall also continue to allocate resources to business continuity and disaster recovery mechanisms. Moreover, Nigeria shall ensure that communications redundancy measures are regularly tested to include provision of fail over or backup sites and availability of redundancy modes of connection, amongst others. We shall also promote the establishment of sustainable cost effective and resilient mechanisms designed to prevent reliance on single points of failure.

4.4 COORDINATION OF CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

Nigeria shall effectively coordinate the execution of its CNII protection. To this end, the country shall develop criteria and best practices for each CNII sector, including sector-level performance objectives as well as establishment of feedback mechanism to NCCC and the regulatory agency of government charged with the responsibility of managing the sector. A National Critical Information Infrastructure Measurable Program (CIIMP) shall also be developed in order to engender progress monitoring and evaluation. On this premise, CNII owners and operators will take responsibility for safeguarding their systems and networks in adherence to guidelines and standards stipulated by NCCC. CNII owners, operators and Sector regulators would also be obligated to participate in cybersecurity crisis response exercises and drills to enhance preparedness for collective response to cyber incidents. Additionally, government shall continue to collaborate with relevant stakeholders towards building capacity and developing professional skills for effective CNII protection.

4.5 CRITICAL NATIONAL INFORMATION INFRASTRUCTURE PROTECTION PLAN

Nigeria shall continue to strengthen its plan for protection of the country's CNII. This Critical National Information Infrastructure Protection Plan (CNIIPP) will be robust enough to ensure the security and resilience of CNII. The plan will also incorporate clear risk management procedures and mitigation mechanisms. The plan must also engender the participation of all relevant stakeholders in the protection of CNII. Furthermore, the plan must incorporate emergency readiness and response mechanisms to facilitate disaster recovery and business continuity. It must also ensure that standard operating procedures and personnel vetting mechanisms are developed and adhered to as guide for action by all stakeholders.

4.5.1 Objectives of the Critical National Information Infrastructure Protection Plan

- Predict, identify, protect, detect, respond and facilitate the recovery of CNII from cyber attacks and unintentional disruption or damage including natural disasters.

- Share important and actionable information among the CNII community in order to build awareness and provide risk-informed decision-making.

- Promote cyber-drills and active incorporation of lessons learnt into the CNII protection process.

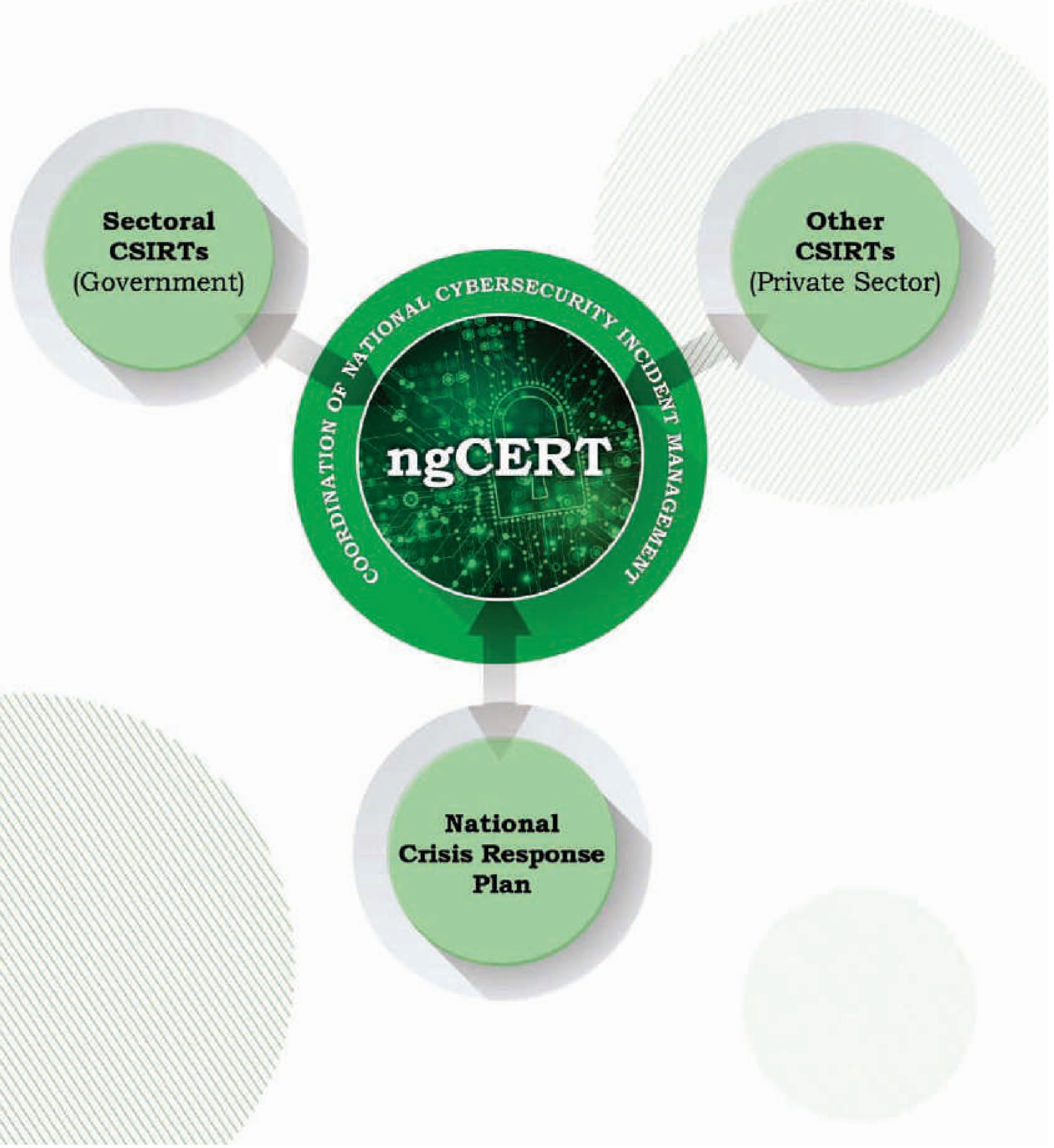
4.5.2 National Vulnerability Management

National vulnerability assessment (NVA) shall be periodically conducted and integrated into the CNIIPP. NCCC in collaboration with the sectoral CSIRTs shall coordinate the NVA with a view to determining weaknesses in the nation’s CNII. To this end, the NVA shall:

- Identify, analyse and assess threats to CNII to facilitate effective risk management and mitigation.
- Assist Government in appreciating the level of preparedness, the need to safeguard huge investments in information systems and communications infrastructure, as well as commitment made to global partners national ICT developmental goals.
- Set the path for the adoption of Security by Design practices as an approach to build security measures into CNII.
- Pave a path for the documentation and archiving of all vulnerabilities. A national record to this effect shall be maintained for review purposes.

CHAPTER FIVE

Enhancing Cybersecurity Incident Management



CHAPTER 5

ENHANCING CYBERSECURITY INCIDENT MANAGEMENT

The ability to pre-empt, respond and expeditiously mitigate the potential consequences of cyber attacks while minimising the impact, is crucial for sustainable governance, national security and socio-economic wellbeing of the people. Accordingly, Nigeria recognises the importance of a comprehensive framework for preparedness against cyber attacks. Therefore, we will ensure robust, adaptive and reliable response to cybersecurity incidents. This shall be achieved through effective coordination of our national cybersecurity incident response mechanism, strengthening of our cybersecurity incident response teams and the development of a National Cybersecurity Crisis Response Plan.

5.1 COORDINATION OF NATIONAL CYBERSECURITY INCIDENT MANAGEMENT

The National Computer Emergency Response Team, known as the Nigeria Computer Emergency Response Team (ngCERT), is the focal point for our national cyber incident management. To this end, ngCERT shall be domiciled under the NCCC to coordinate the activities of sectoral Computer Security Incident Response Teams (CSIRTs) and other relevant CSIRTs in the private sector.

Accordingly, ngCERT shall work closely with the sectoral CSIRTs, CNII operators, government stakeholders and the entire cybersecurity community to respond to cyber attacks. In the event of a national cyber crisis, ngCERT shall coordinate the operational responses of the Sectoral CSIRTs to engender a unified response to the threat. Furthermore, NCCC shall support ngCERT by encouraging and ensuring the:

- Establishment of CSIRTs across all relevant sectors of the Nigerian economy, and through ngCERT, mobilise CSIRTs to lend support to sectors or CNII operators, in the event of exigencies or escalating cyber incidents.
- Promotion of international, multinational and bilateral collaboration towards cybersecurity incident response and management.

- Development of a framework for information sharing on cybersecurity incidents as well as promotion of trust and culture of collective and shared responsibility on incident management across Sectoral CSIRTs and the entire cyber community.
- Establishment of processes, protocols and timelines for reporting and escalation of cybersecurity incidents across all levels from individual users, sectoral CSIRTs and CNII operators to ngCERT.

5.2 RESPONSIBILITIES OF NGCERT

ngCERT is established vide Section 41 (c) of the Cybercrimes (Prohibition, Prevention, Etc) Act 2015 to ensure effective national response to cybersecurity incidents occurring within or emanating from the Nigerian cyberspace. To this end, ngCERT shall propose the mobilisation of human resources from industry and academia where necessary to complement the capacity of CSIRTs to deal with escalating cyber attacks. ngCERT shall also plan and coordinate the conduct of national cybersecurity crisis response drills and simulation exercises to enable sectoral CSIRTs and other stakeholders better understand their roles and responsibilities during cyber incidents while providing a platform for capability assessment and enhancement. In addition, ngCERT shall establish, operate and continually update a National Register of Cybersecurity Incidents in conjunction with sectoral CSIRTs and other stakeholders.

5.3 ESTABLISHMENT OF SECTORAL AND OTHER CSIRTs

Sectoral and other CSIRTs shall be set up by the regulatory body or any other coordinating body within a particular sector of the economy. Key stakeholders on national cybersecurity within government departments and agencies shall be listed to have a centralised, harmonised and unified approach to cybersecurity incident management. Sectoral CSIRTs shall:

- Serve as the single point of contact (POC) for each of the specific sectors and coordinate incident response activities within the sector.
- Promote trust and confidence among stakeholders in their respective sectors.
- Facilitate information sharing with ngCERT and other relevant stakeholders.

- Facilitate provision of criteria, measures, standards, guidelines and best practices for the sector in line with national cybersecurity measures prescribed by ngCERT.
- Undertake cybersecurity readiness, capacity building, information security assurance and compliance administration for their respective sectors.

5.4 NATIONAL CYBERSECURITY CRISIS RESPONSE PLAN

The National Cybersecurity Crisis Response Plan shall outline the protocols governing the response of ngCERT, sectoral CSIRTs, CNII owners and operators, government stakeholders and other members of the cybersecurity community in the event of cyber-attack. The plan will incorporate simulations and drills that can prepare stakeholders for a whole-of-nation response to cyber attacks while also serving as a platform for capability assessment and improvement. As part of arrangements to strengthen the national crisis response plan, NCCC shall, through ngCERT, design, plan, conduct and evaluate national cybersecurity crisis response exercises and drills, on a periodic basis.

5.5 INITIATIVES FOR MANAGING CYBERSECURITY INCIDENTS

The initiatives for managing cybersecurity incidents shall be as follows:

5.5.1 Cyber Emergency Monitoring System

We shall operate a Cyber Emergency Monitoring System (CEMS) for effective detection, identification and interception of cyber threats. The CEMS will be established under the coordination of ngCERT to identify indicators for potential threats to the nation’s cyberspace. Based on the potential threat identified by the CEMS, alerts and warnings will be issued by ngCERT to various Sectoral CSIRTs, agencies and entities for rapid response. Internet service providers and internet exchanges shall also interface with ngCERT for effective utilization of a unified national alert and warning system to be established and maintained by NCCC.

5.5.2 Detection and Response

The deployment of CEMS will ensure that all detected cyber incidents are promptly communicated by ngCERT and relative sectoral CSIRTs to affected persons, businesses, organisations or government establishments. In scenarios where there is no local expertise to respond to cyber incidents, details of such incidents shall be escalated to ngCERT or the relative sectoral CSIRT. Such incidents shall then be recorded, reviewed and resolved following an established incident management process.

5.6 MECHANISM FOR CYBER INCIDENT REPORTING AND INFORMATION SHARING

The global dimension of cyber threat requires policy action and strategic measures on Cyber Incidents Reporting and Information Sharing, both at the national and international level. At the national level, ngCERT shall develop an Auto Cyber-Indicator Sharing (ACIS) System as a national free-to-join system by government, private sector and non-government entities to facilitate real time exchange of information on cybersecurity related incidents. The strategic scope of information sharing on cyber incident shall include threat indicators, malicious Internet Protocol addresses, intrusion attempts, and phishing emails, amongst others. This scope shall be expanded to the global scale in collaboration with stakeholders in the international community.

5.7 CAPACITY DEVELOPMENT TO ENHANCE INCIDENT MANAGEMENT

Government shall promote the development of human resources for enhancement of incident prevention and response. Efforts shall focus on improving the capacity of incident response teams to utilize emerging technologies to manage cyber threats, such as the use of Artificial Intelligence and Machine Learning concepts to analyse data and identify potential cyber risks. To this end, Government effort shall be geared towards promoting incident management capacity development across public and private sector organisations in the country. We shall also strengthen incentives for public and private sector organisations and institutions to encourage capacity development of their CSIRTs. Efforts shall also focus on encouraging stakeholders to deploy and sustain effective operation of state-of-the-art technologies for Security Operations Centres (SOCs) across the country.

5.8 COLLABORATIVE PARTNERSHIP FOR INCIDENT MANAGEMENT

The Nigerian government recognises that shared and collective responsibility is crucial to the attainment of effective incident management. Therefore, Government has taken proactive steps to re-invigorate measures to address the rising cyber threats through the adoption of collaborative partnership model which is based on a hybrid combination of public-private partnership (PPP) and multi-stakeholder partnership (MSP). This approach stems from the understanding that businesses across the private sector have a significant share of the responsibility to protect the nation's systems and networks from cyber threats. Therefore, a collaborative partnership model is needed to build the requisite synergy of government, industry, businesses, academia and international stakeholders, amongst others, towards enhanced incident response.

5.8.1 Establishment of Collaborative Partnership Model

A National Technical Working Group (NTWG) comprising representatives from the private sector, government organizations and representatives of international multi-stakeholder partners shall be established and coordinated by the NCCC to:

- Collaborate with other countries, industry, academia, civil society and other stakeholders towards advancing support for incident management technology development, digital safety training, and software and hardware systems security enhancement.

- Interface with stakeholders in Government, private sector and the international community to jointly develop and implement a Collaborative Partnership Cybersecure Framework that assures the security of the nation's digital infrastructure.

- Promote the establishment of a Collaborative Partnership-driven Research and Development Centre of Excellence to cater for the shortage of cybersecurity skills as well as a vehicle to propel local development of cybersecurity products and services.

5.8.2 Objectives of Collaborative Partnership Model

- To develop and implement a hybrid PPP and MSP action plan to support cybersecurity incident management.

- 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 harmonised agreements on national cybersecurity incident management.

- 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.

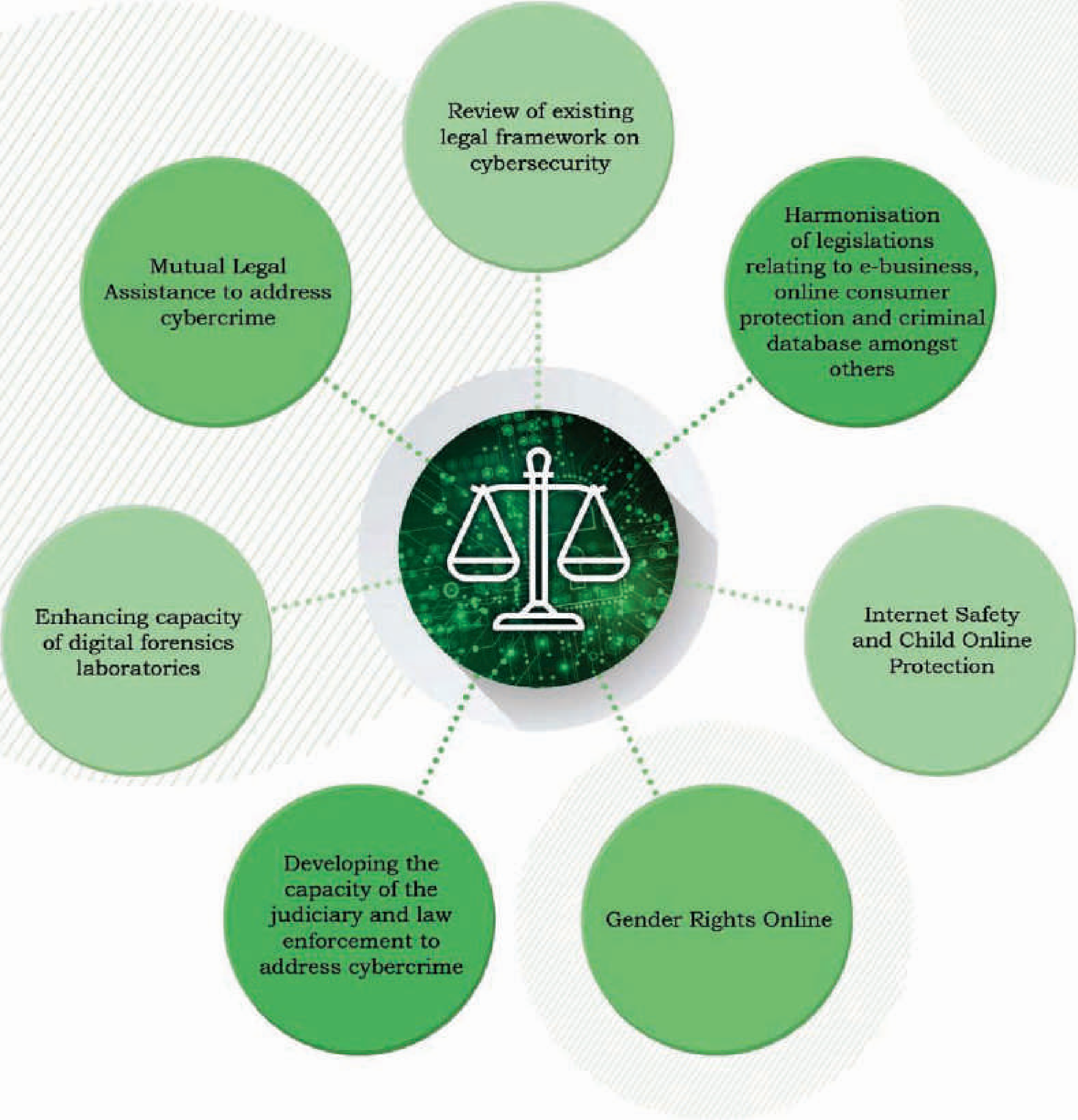
- To facilitate the development of policies to ensure that cybersecurity considerations are prioritised in the domestic development of software and infrastructure components.

- To support the development of policies to govern the cybersecurity marketplace and consider certification for both imported and local cybersecurity products and services.

- To promote discussion between the public and private sectors on cyber-insurance coverage, to identify whether there is a need for cyber-insurance products or services based on perceived cyber threats.

CHAPTER SIX

Strengthening Legal and Regulatory Framework



Review of existing legal framework on cybersecurity

Harmonisation of legislations relating to e-business, online consumer protection and criminal database amongst others

Internet Safety and Child Online Protection

Gender Rights Online

Developing the capacity of the judiciary and law enforcement to address cybercrime

Enhancing capacity of digital forensics laboratories

Mutual Legal Assistance to address cybercrime

CHAPTER 6

STRENGTHENING LEGAL AND REGULATORY FRAMEWORK

Cyber threats have become more dynamic, pervasive and detrimental to societal safety and wellbeing. Individuals, businesses, organisations, government functions, essential services and critical infrastructure across the country are now faced with sophisticated risks emanating from cyberspace. Moreover, perpetrators of cybercrime and other malicious cyber activities have demonstrated the ability to conduct attacks across the entire spectrum of cyberspace with attendant dire consequences on victims. This brings to fore the need for robust legal and regulatory framework to facilitate a proactive approach to confront and curtail these threats.

The Government is responsible for improving and updating federal and state laws to combat cybercrime and enhance the capacity of the nation to address cyber incidents and protect the Nigerian Cyberspace. To this end, this strategy shall support the amendment of our existing Cybercrimes (Prohibition, Prevention, Etc) Act, 2015. The strategy shall also ensure the harmonisation of provisions in other legislations relating to e-business, online consumer protection and criminal database amongst others. Furthermore, it will boost efforts to promote online child and gender protection while developing the capacity of the judiciary and law enforcement to enhance their effectiveness to address cybercrime.

6.1 AMENDMENT OF CYBERCRIME LEGISLATION

The foremost legal framework on cybersecurity in Nigeria is the Cybercrimes (Prohibition, Prevention, Etc) Act 2015, (hereafter the Act). The Act is well developed and addresses several aspects of cybercrime and other cybersecurity issues. However, in line with the dynamic and emergent nature of cybersecurity, the focus of this strategy is to review and amend the Act in order to address new aspects not included in the current legislation. The Cybercrime Advisory Council is charged with driving the process of amendment of the Act in consultation and collaboration with relevant stakeholders across Nigeria’s cyber ecosystem. The amendment of the Act is expected to consider, amongst others, the following areas:

- Penalties for breaches or disruption to CNII
- Timelines for cyber incident reporting
- Regulation of cybersecurity service providers
- Allotment of powers to NCCC to coordinate national cybersecurity and anchor investigation of cyber breaches
- Identity theft
- Enhanced enforcement of cybersecurity legislation
- Lawful interception
- Child and gender online protection
- Review of penalties

6.2 ENACTMENT AND HARMONISATION OF NEW AND EXISTING LEGISLATIONS

Government will ensure the enactment and harmonisation of new and existing legislations. Currently, there is no primary legislation on data protection and privacy in Nigeria. This informs the need for a national legislation providing for an independent regulator for data protection. Recent migration of businesses and interactions to the digital domain also makes it imperative to develop a unified national legislation for data protection.

We will focus on strengthening National Data Governance and Protection of Digital Intellectual Property. We will also focus on strengthening public service delivery, research, economic promotion, and security and development through National Data Governance which will ensure the safeguard of Nigeria's digital economy. The strategy will further ensure the protection and safeguard of the nation's digital content through regulations and guidelines regardless of the medium it is held on.

Additionally, the need for integration of digital identity framework as an element of national cybersecurity is also expedient. In this regard, Nigeria will adopt the following strategy options:

- Strengthen legislative, technical and policy initiatives to fulfil the goals of national cybersecurity programmes.
- National Data Governance and Protection of Digital Intellectual Property.
- Ensure harmonisation of e-business laws in line with global best practices.
- Development and enactment of Data Protection and Privacy law.

- Provision of legal protection for entities and individuals who disclose vulnerabilities.
- Provision of a legislative framework for child and gender online protection.
- Provision of a legislative framework for online consumer protection.
- Provision of a legislative framework for bug bounty.
- Integration of digital identity framework as an element of national cybersecurity strategy.
- Reduce reliance on foreign-hosted cloud services for storing personal data of Nigerian Citizens.

6.3 INTERNET SAFETY AND CHILD ONLINE PROTECTION

Increasingly, children are embracing the use of cyber resources facilitated through the availability of Internet in homes, schools and other locations. While this availability of the Internet has significant advantages for children, there are harmful social media contents and illicit materials, being distributed within cyberspace, which can exploit the innocence of minors thereby posing a risk to their well-being.

Such exposure of children to the Internet can trigger cyber abuse and online exploitation with consequences that are inimical to our national dignity. Therefore, this strategy establishes that any act against a child which is illegal in the physical environment is equally illegal online. The focus of government is to protect children from exposure to adverse online materials. To this end, our focus is the development of control mechanisms to prevent accessibility and distribution of malicious online materials, launching of a national child online safety awareness agenda, creation of a national register of convicted online child abuse offenders and establishment of channels for reporting incidents on child online abuse.

6.3.1 Mechanisms to Prevent Distribution of Illicit Content Online

Nigeria is committed to the detection, identification, removal as well as prevention of the distribution of illicit or malicious content on the Internet. We shall therefore engender the necessary synergy between service providers, law enforcement and the judiciary to combat the distribution, availability and accessibility of illicit content online. To this end:

- NCCC shall interface with service providers and relevant government agencies to promote the development of control measures to combat the distribution of malicious digital contents and materials targeted at the young population.

- Regulatory agencies shall ensure that service providers and owners of online platforms take proactive measures to prevent accessibility to malicious content that are targeted at children as well as integration of parental control measures on websites and applications on mobile devices. This shall be driven through the constitution of a Task Force on Child Online Protection.

- Stakeholders shall also ensure that all Child Abuse Materials (CAM) online are channelled into a centralised national resource. Actions shall entail outlawing any form of remote enticement of minors into inappropriate sexual contact or sexual activity, possession, production and distribution of CAM, irrespective of the intent to distribute. This will include taking additional responsive steps to disrupt the trafficking of CAM and creating awareness about the illegality of being in possession of CAM for any purpose.

- Nigeria shall engage in bilateral and multilateral collaboration and information exchanges with relevant law enforcement authorities and investigative bodies in other countries.

- We shall also develop evaluation mechanism to promote zero tolerance of online child abuse and exploitation while spearheading the development of Child Online Abuse and Exploitation Combating Strategy (COAECS).

6.3.2 National Child Online Safety Awareness Campaign

Nigeria is dedicated to promoting education and awareness about the issues of child online safety as a prerequisite for enhancing Internet safety for children. Accordingly:

- National Orientation Agency (NOA) shall interface with other relevant agencies for the development of programmes to promote awareness on child online safety. Efforts shall be directed at ensuring that child online protection awareness agenda is enshrined in all aspects of our national orientation programmes.

- We shall also develop platforms for stakeholders to partner in educating children on the need to speak out against any form of sexual harassments or molestations online.

- Government agencies and actors in the private sector shall collaborate to promote the provision of appropriate long term support for victims of online child abuse.

6.3.3 National Register of Convicted Offenders

Federal Ministry of Justice (FMOJ) shall interface with NCCC to develop a register for convicted child online abuse offenders. The register shall serve as a watch list and online database that will be accessible to relevant stakeholders that host the list of convicted sex offenders in the country.

6.3.4 Incident Reporting and Investigation

NCCC shall through ngCERT and sectoral CSIRTs develop and sustain channels for reporting incidents of child online abuse. Efforts shall focus on creating platforms to receive reports from entities around the globe on illegal behaviour or content. NCCC shall also enhance the capacity of the National Digital Forensics Laboratory to obtain details of reported incidents, and process and interpret forensic evidences from digital devices relating to online crimes against children.

6.4 GENDER RIGHTS ONLINE

We recognise the rights and importance of the active involvement of women in the use of cyberspace. We are also committed to promoting the inclusiveness and active participation of women in the complete lifecycle of activities in our cyber ecosystem. Nigeria is also up to date on the global and domestic digital gender gap and the country is dedicated to breaking the barriers hindering accessibility for women. Furthermore, combating online violence against women is a crucial priority for the Nigerian Government. We are therefore committed to the development of mechanisms to create a safe cyberspace and protect women online presence.

Against this backdrop, our approach is to prioritise the promotion of online safety awareness and education for women. We shall spearhead the development of a multi-stakeholder forum to drive the development of online gender protection and participation initiatives. Furthermore, we shall provide the necessary support for organisations anchoring gender promotion initiatives to strengthen advocacy. We shall also develop mechanisms to empower women with the requisite capacity while also creating opportunities in the cybersecurity ecosystem across government, industry and academia. In the area of online safety, NCCC in conjunction with regulatory agencies shall interface with Internet service providers and owners of online platforms towards enhancing security and privacy of women online. We shall also establish and promote mechanisms for reporting online violence against women.

6.5 CAPACITY DEVELOPMENT FOR LAW ENFORCEMENT AND JUDICIARY

A major focus of this strategy is to enhance the capacity of the law enforcement community to investigate cybercrime and handle digital evidences, and training of the judiciary to prosecute and adjudicate on cybercrime. This will be driven through a continuous, comprehensive and specialised training program developed to educate lawyers, judges, prosecutors, law enforcement officials, forensics investigators and other specialists. For this purpose, relevant government bodies shall collaborate with NCCC, academia and industry towards capacity development to address cybercrime.

We shall also promote requisite capacity building through specialised training courses, curricular development and skills acquisition championed by universities and professional training institutions. Furthermore, we shall promote synergy between relevant stakeholders to build the capacity of law enforcement and judiciary to investigate and prosecute Internet related crimes against children and other vulnerable groups, and enhance the ability of the Courts to handle digital forensic evidence and preside over cybercrime cases.

6.6 NATIONAL DIGITAL FORENSICS LABORATORY

The National Digital Forensics Laboratory (NDFL) shall be established under the NCCC to provide the requisite facilities for digital forensics investigation and intelligence gathering on cyber related issues. The

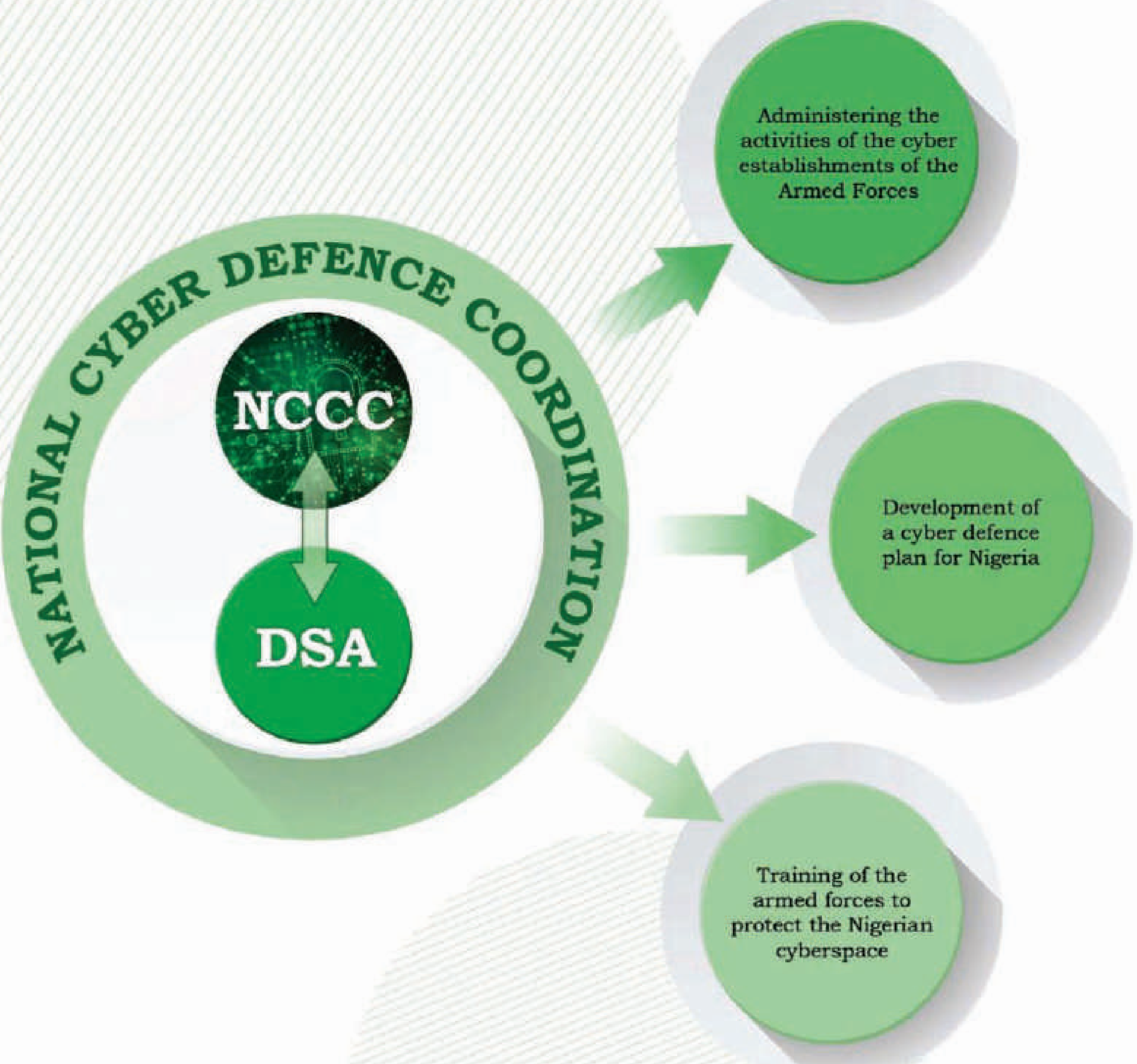
NCCC shall boost the capacity of the NDFL through deployment of adequate human resources and technology solutions to automate and facilitate rapid surfing, processing and extraction of digital information from devices which would be used as evidence for effective prosecution. NDFL shall also, where necessary, collaborate with industry and academia to provide a platform for training on cybercrime investigation skills-based courses such as malware analysis, cyber intelligence gathering and digital forensics, amongst others. Efforts shall also focus on certification, support and regulatory oversight functions to foster collaboration and development of digital forensics laboratories across the country.

6.7 MUTUAL LEGAL ASSISTANCE FOR COMBATING CYBERCRIME

As part of efforts to ensure our commitment to the protection of society from transnational cybercrime, the strategy engenders development of effective multilateral and bilateral coordination mechanisms. This includes establishment of frameworks and channels for mutual legal assistance, facilitating cross border investigation, prosecution and transfer of digital evidence as well as related cross-border processing of cybercriminals. To this end, stakeholders shall collaborate and share relevant information with global partners as well as international and multilateral organisations. We shall also promote sustainable cooperation and partnership amongst stakeholders to prosecute and combat transnational cybercrime.

CHAPTER SEVEN

Enhancing Cyber Defence Capability


NATIONAL CYBER DEFENCE COORDINATION
NCCC
DSA
Administering the activities of the cyber establishments of the Armed Forces
Development of a cyber defence plan for Nigeria
Training of the armed forces to protect the Nigerian cyberspace

CHAPTER 7

ENHANCING CYBER DEFENCE CAPABILITY

The development of our cyber defence posture and capability is crucial to national cybersecurity. The need for an enhanced cyber defence capability is even more pronounced with the increased use of cyberspace by domestic, foreign and transnational state and non-state actors to perpetrate cyber terrorism, cyber espionage and other forms of organised cyber attacks. Therefore, our strategy shall develop the capability of our military and defence establishments to identify, detect and effectively deter any form of organised cyber-attack launched on the nation. To this end, our Defence Space Administration (DSA) shall interface with NCCC for effective coordination of activities of relevant stakeholders in the armed forces, development of an effective cyber defence plan and training of our military to protect the Nigerian cyberspace.

7.1 NATIONAL CYBER DEFENCE COORDINATION

In consonance with the provisions of extant domestic and international laws, DSA shall mobilise its capabilities for cyber operations to complement Nigeria's diplomatic, information, military and economic elements of national power. Our focus is therefore to develop the necessary capabilities to effectively defend our military networks and systems, government ICT assets and the country's CNII domiciled with the private sector, against national cyber attacks. Our efforts shall also extend to the collective development of cyber capabilities to support the mandate and operations of our armed forces towards the protection of our territorial integrity. Therefore, we recognise that effective development of our cyber defence capability relies on close collaboration across government, private sector and our international partners.

Against this backdrop, DSA in line with its mandate to provide resilient and affordable space and cyberspace capabilities for the Nigerian military, will work closely with the NCCC, agencies of government and think tanks from industry and academia to implement our national cyber defence strategy. To this end, the DSA shall assign roles to and coordinate the activities of the cyber establishments of the armed forces to ensure readiness to defend the nation against cyber attacks.

The Defence CSIRT and Defence Security Operations Centre (SOC) shall be set up under the DSA. Similar to other sectoral CSIRTs across the country, the activities of the Defence CSIRT shall be coordinated by ngCERT in the areas of information sharing, protection of CNII, cyber incident management, technology and skills transfer, and conduct of cyber drills and exercises. NCCC shall also support DSA by promoting the maintenance of necessary communication channels and coordination arrangements to ensure that all stakeholders across government and the private sector mobilise in unison to protect the nation from any national cyber-attack.

7.2 NATIONAL CYBER DEFENCE PLAN

DSA shall work closely with NCCC to develop a National Cyber Defence Plan (NCDP) for the nation. The plan shall identify the relevant stakeholders and delineate their roles in the event of cyber-attack against the country. The plan shall also outline arrangements for protection of CNII and protocols for rendering or requesting for assistance from ngCERT and the Sectoral CSIRTs. Furthermore, the plan shall engender collaboration with regional and international defence CSIRTs and multinational organisations for addressing cross-border cyber attacks while embracing the requisite restraints obligated under international law.

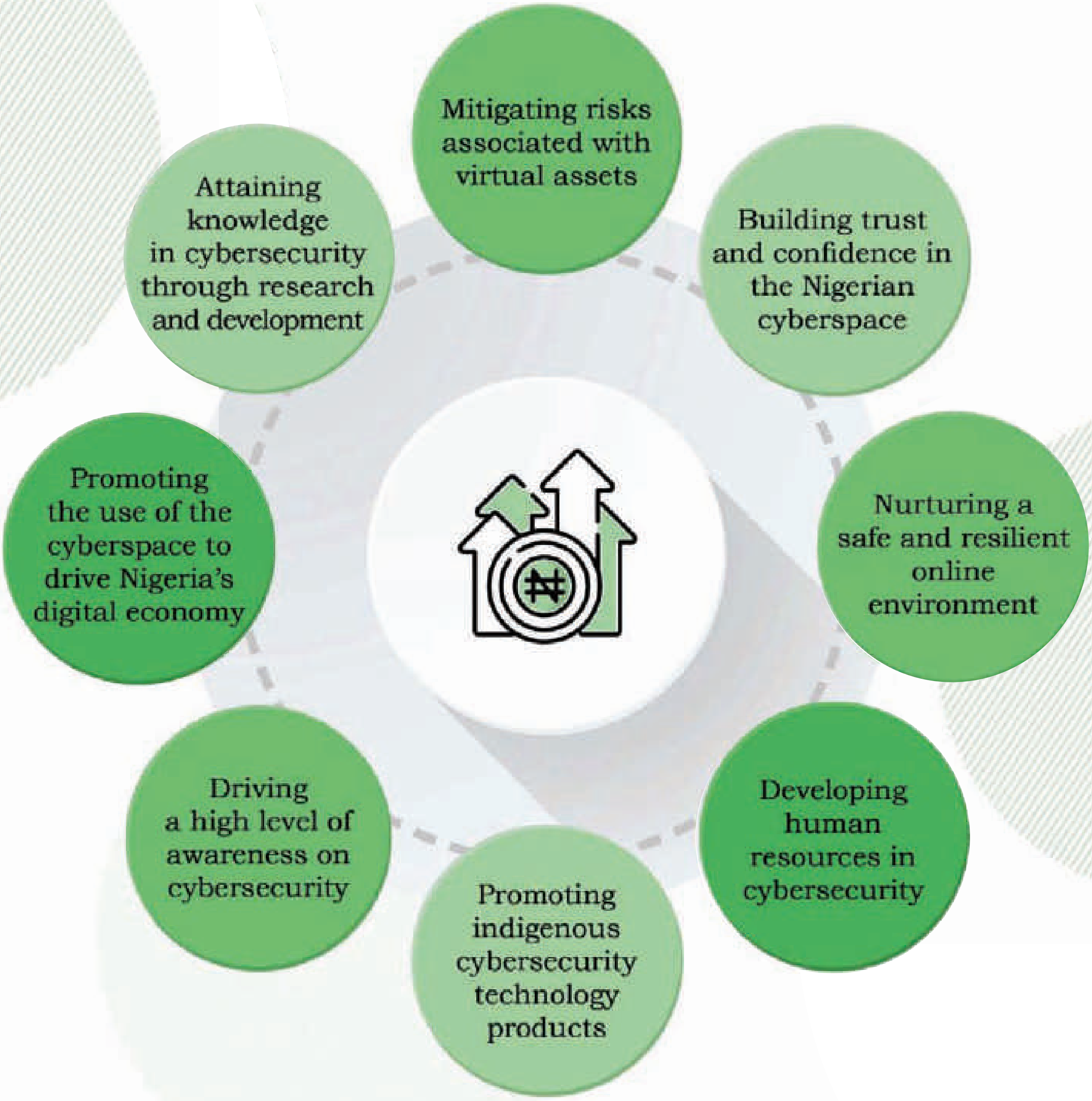
7.3 CYBER DEFENCE CAPACITY DEVELOPMENT

As a pathway for ensuring effective implementation of our NCDP, our efforts shall focus on maintaining an operations-ready Defence CSIRT. We shall also ensure that the necessary synergy is developed between our Defence CSIRT and other sectoral CSIRTs for effective cyber operations and protection of CNII across all sectors of the economy. We therefore recognise that the implementation of our NCDP relies on the availability of personnel with high standard of cybersecurity training supported with state of the art technological capabilities.

On this premise, DSA shall ensure that all the components of the cyber defence structure are empowered with the relevant knowledge and technical capacity to defend the country against cyber attacks. Based on this, the DSA shall interface with NCCC, security and law enforcement agencies, academia and industry to ensure focused arrangements for professional training and technical skills acquisition for personnel. Capacity development shall focus on training to familiarise personnel with cyber law as it affects cross-border operations. DSA shall also make necessary arrangements to continually empower the Defence CSIRT with relevant and up-to-date technological capabilities to enhance cyber operations.

CHAPTER EIGHT

Promoting a Thriving Digital Economy


Mitigating risks associated with virtual assets
Building trust and confidence in the Nigerian cyberspace
Nurturing a safe and resilient online environment
Developing human resources in cybersecurity
Promoting indigenous cybersecurity technology products
Driving a high level of awareness on cybersecurity
Promoting the use of the cyberspace to drive Nigeria's digital economy
Attaining knowledge in cybersecurity through research and development
₦

CHAPTER 8

PROMOTING A THRIVING DIGITAL ECONOMY

Nigeria recognises the role that cyberspace plays in the propagation of an ICT-driven economy for the country. Cyberspace, especially the Internet and social media, provides the platform for connectivity, interaction and innovation, which opens up a plethora of new opportunities for businesses and commercial activities to flourish. These opportunities offered by cyberspace, if effectively harnessed, have the potential to project our economy and accelerate the country's pace towards achieving the broader socio-economic objectives.

Our focus is therefore to use cybersecurity as a catalyst to promote the use of the Internet and social media for increased commercial, financial and related government activities, thereby facilitating a thriving digital economy for Nigeria. We shall build trust and confidence in the Nigerian cyberspace, nurture a safe and resilient online environment, develop a robust cybersecurity workforce, develop and promote indigenous cybersecurity technology products, and drive a high level of awareness on cyber threats and cybersecurity practices to mitigate risks.

8.1 SAFE AND TRUSTED ONLINE ENVIRONMENT

We strive to create an online environment that is safe, resilient and trusted by society and businesses within and outside Nigeria. We envisage a transformation of our cyber ecosystem to a user-friendly digital environment where the security of personal and sensitive information is assured, safety of online activities is guaranteed, and the rights of users, businesses and service providers are protected.

Our approach is to develop processes and set actions in motion that will support and promote the use of e-business, e-transactions, and e-government platforms in the Nigerian cyberspace. Such drive requires the emplacement of mechanisms that ensure that Internet users, businesses and commercial services including facilitators of online government services, develop a responsible cybersecurity culture and behaviour and foster the security and resilience of services hosted on the Internet.

8.1.1 Responsible Cybersecurity Culture and Behaviour

- Government will lead by example through the institution of responsible cybersecurity culture and behaviour. This shall be driven by NCCC, in collaboration with heads of government departments and agencies. To this end, NCCC in conjunction with heads of government bodies, shall prioritise the development of periodic training programmes for government employees to improve understanding of responsible cybersecurity culture and encourage the adoption of cybersecurity best practices when carrying out day-to-day activities online.

- Heads of ministries, departments and agencies shall be responsible for developing, institutionalising and promoting the adoption of practices that ensure responsible cybersecurity behaviour in their respective jurisdictions, especially when handling government functions online.

- At the private sector level, the responsibility to drive good behaviour online shall be entrusted to companies and businesses under the supervision of regulatory agencies across all sectors of the Nigerian economy. By this, NCCC shall prompt regulatory agencies to encourage service providers and operators of online digital services to introduce mechanisms that protect platforms and foster cybersecurity best practices by employees. Regulatory agencies are also charged with ensuring that private sector executives prioritise the adoption of these cybersecurity work practices in their organisations.

- For users of the Internet among the general public, a whole-of-society approach would be adopted by promoting practices such as incident and cybercrime reporting and other activities to make the public proactive in ensuring their safety online. To this end, NCCC, regulatory agencies, Sectoral CSIRTs, academia and industry stakeholders shall promote incident reporting through regular provision of publicly available materials to prompt users to take collective responsibility of protecting the online community as well as their own personal presence on the Internet.

- We are conscious of the role that legislation will play in the enhancement of personal information protection online. Therefore, Government shall prioritise promulgation of Nigeria's Data Protection Act as a catalyst for privacy and protection of user and corporate information on the Internet.

8.1.2 Secure and Resilient Online Services

- Our priority is to improve the level of trust and confidence that our people and the international community have on online activities and services in the Nigerian cyberspace, especially digital financial transactions, e-government and e-business platforms. We are also conscious of a rising number of other new activities moving to the cyber domain, in the areas of e-health and online educational services, amongst others.

- As way of ensuring security, resilience and trust in e-government platforms and other public sector services hosted online, NCCC shall interface with relevant government stakeholders across the sectors of the Nigerian economy to drive adoption of digital standards that ensure security, transparency and accountability of services hosted online. This will encourage the use of platforms that provide end-to-end encryption, display indicators of authenticity on websites and applications, incorporate channels for user reviews and feedback, and adopt user privacy policies, amongst others.

- Regulatory agencies shall also tow the path of government to encourage operators of online services in the private sector to adopt similar measures to secure their Internet-based platforms and promote user trust. Stakeholders are also entrusted to make requisite effort to continually leverage social media, mainstream media and other platforms for advertisement, to promote trust, confidence and utilisation of e-government, e-business and e-transactions services.

- We shall promote the deployment of mechanisms to prevent unauthorised electronic transmission of data from establishments of stakeholders across the public and private sector. Our focus is to protect information from being stolen or compromised or disseminated illicitly across cyberspace. This shall be achieved by encouraging stakeholders to deploy templates, checklists, tools and processes to detect and prevent unauthorised access or misuse of sensitive data, in line with extant laws governing data in transit, data in use and data at rest.

- As a whole-of-government approach, NCCC shall lead the way in establishing the channel for Nigeria to work with global partners, international businesses and multinational organisations to facilitate secure cross-border data flows and online transactions built on transparency, accountability, mutual trust and confidence.

8.2 ROBUST CYBERSECURITY WORKFORCE

Cybersecurity human resources development and skills acquisition is instrumental to the creation of the enabling digital environment for online economic activities to strive. The role of Government is to set the platform for capacity development and skills acquisition in cybersecurity as a pathway for the generation of the cyber workforce required for the Nigerian cyberspace. This can only be achieved through the creation of opportunities for the Nigerian people to take up interest and amass the education, knowledge and professional skills required to meet the high demand for cybersecurity experts in the digital market. Our focus is therefore to enhance availability, uptake and quality of education in cybersecurity, encourage cybersecurity skills acquisition and professional development and promote attainment of knowledge in cybersecurity through research and development.

8.2.1 Cybersecurity Education

- Federal Ministry of Education (FMoE) shall interface with regulatory bodies in the education sector to promote uptake of cybersecurity courses and curricular at undergraduate and postgraduate levels in Nigerian universities. FMoE and regulatory bodies in the education sector shall also be entrusted with efforts to promote the uptake of cybersecurity courses and programmes by schools and institutions of learning across Nigeria.

- FMoE shall interface with regulatory agencies in the education sector and other stakeholders to map out actions to enhance cybersecurity education. Stakeholders shall also collaborate to ensure that national investments in education meet the demands of the cybersecurity environment across all sectors of the Nigerian economy. This approach is envisaged to pave way for provision of adequately trained cybersecurity academic teachers, training materials and other resources.

8.2.2 Skills Acquisition and Professional Development

- Our approach is to encourage individuals to take up professional skills acquisition in the field of cybersecurity. To this end, our strategy prioritises the establishment of a National Cybersecurity Training Institute (NCTI), under the organisational structure of NCCC, to spearhead skills acquisition and professional development through multiple streams of standardised cybersecurity certification courses, career tracks and programmes. NCCC is entrusted with the responsibility of driving this initiative as a pathway to build the necessary talent pool required for the cybersecurity market in the public and private sectors.

- NCCC shall provide the relevant guidelines for the establishment of cybersecurity training centres across the country. Furthermore, it shall promote the creation of forums where cybersecurity stakeholders from academia, industry, cybersecurity societies and associations, advocacy groups and experts can interact towards proposing initiatives to accelerate the pace of cybersecurity skills acquisition and professional development in Nigeria.

8.2.3 Research, Development and Innovation

- The attainment of knowledge and expertise in cybersecurity shall also be driven through promotion of research and development. This approach will encourage cybersecurity professionals and businesses to enhance their levels of expertise to improve service delivery while also promoting close partnership between academia and industry.

- FMoE shall interface with regulatory bodies in the education sector, stakeholders in academia and key players in industry to draw up roadmaps to encourage and harness cybersecurity research and development efforts in Nigeria.

8.3 INDIGENOUS CYBERSECURITY TECHNOLOGY

Our digital market comprises a combination of cybersecurity technologies developed indigenously as well as those imported or procured from outside Nigeria. Currently, most of the cybersecurity products and solutions used in our systems and networks across the public and private sector, as well as those in the market, are developed or manufactured overseas. We acknowledge the benefits of these imported systems and software solutions to the enhancement of our cybersecurity posture. However, we also recognise the criticality of developing and expanding our own indigenous cybersecurity technology systems and products market. Our focus is therefore to enhance the development and availability of competitive indigenous cybersecurity products and services. This requires the collaborative effort of stakeholders in industry and academia especially in the area of research and development.

Government efforts to this effect shall be anchored by NCCC in collaboration with relevant stakeholders, and it shall focus on creating the platforms for cybersecurity technology incubation in Nigeria. By this, relevant stakeholders shall promote the establishment of cybersecurity technology innovation centres and laboratories in institutions of higher learning and in the ICT industry across Nigeria. NCCC shall also drive initiatives to provide support and incentives for projects that uplift the indigenous cybersecurity technology market in Nigeria. Furthermore, we shall encourage and promote the growth of cyber insurance products and services.

8.4 RAISING AWARENESS

National efforts for raising awareness on cybersecurity shall follow a whole-of-society approach. National Orientation Agency (NOA) shall drive a coordinated national effort, in conjunction with all relevant stakeholders in the public and private sector, to continually sensitise the general public, businesses, organisations and government establishments on various pertinent cybersecurity issues. Essentially, awareness programmes shall be structured to address the various areas of interest, including, cyber threats and risks online, proliferation of cybercrime and fake news, highlight of education, training and employment opportunities available in the field of cybersecurity, and ongoing research and development as well as international and regional engagements. NOA shall also interface with NCCC and other relevant stakeholders to complement existing national and international awareness raising initiatives such as the National Cybersecurity Awareness Month (NCAM), amongst others.

Our national efforts shall include the targeted training of personnel who shall anchor the delivery of awareness activities and programs. Stakeholders shall also leverage social media and mainstream media to raise awareness and initiate public discussion. Furthermore, relevant government agencies and businesses shall interface with mass media providers to create awareness on prevailing cybersecurity issues in their sectors. As part of this, stakeholders shall take steps to provide training for media providers to improve their understanding of cybersecurity issues affecting the country.

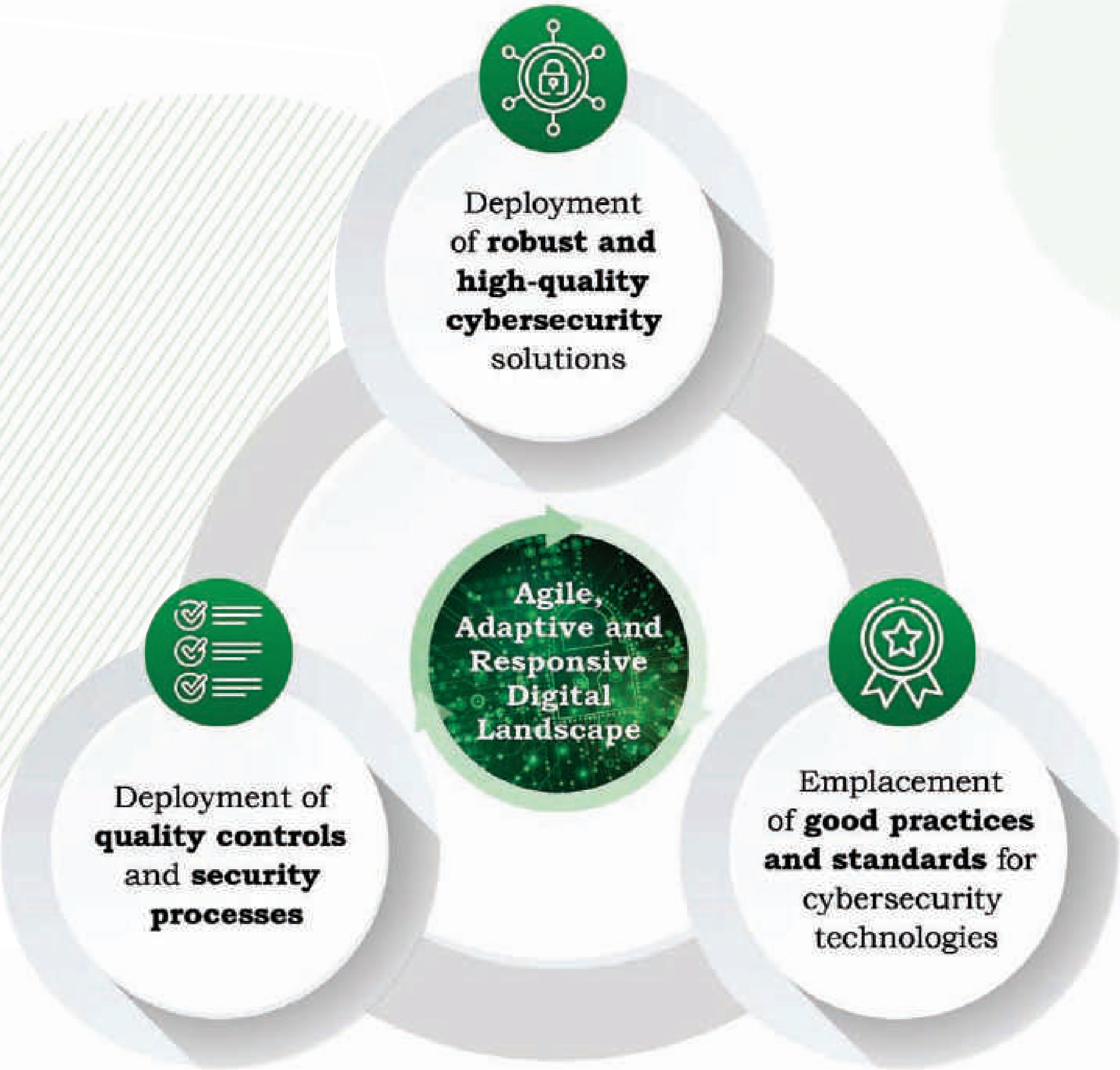
8.5 VIRTUAL ASSETS

We recognise the potential impact of virtual assets and Financial Technology (FINTECH) on our financial industry and by implication our economic security. However, considering that virtual assets create platforms for anonymity or concealment of financial transactions which could facilitate Money Laundering (ML) and Terrorist Financing (TF) amongst other illicit activities, we deem it expedient to apply risk-based approach to mitigating the threats associated with virtual assets and the activities of Virtual Assets Service Providers (VASP). Government is also aware that virtual currencies are fast becoming a currency of choice in cyber-related criminal activities across the globe.

Our approach is therefore for relevant government agencies to collaborate and advocate adoption of mechanisms to drive progressive use of virtual currency while addressing the associated risks. To this end, we shall focus on strengthening existing legal frameworks and sensitisation of stakeholders across government and the private sector. We will also leverage regional and global cooperation for mitigating the risks associated with cross-border movement of virtual assets.

CHAPTER NINE

Assurance Monitoring and Evaluation



Agile, Adaptive and Responsive Digital Landscape

Deployment of **robust and high-quality cybersecurity** solutions

Deployment of **quality controls** and **security processes**

Emplacement of **good practices and standards** for cybersecurity technologies

CHAPTER 9

ASSURANCE MONITORING AND EVALUATION

Nigeria's cyber domain is dominated by a myriad of ICT systems and related infrastructure and thus requires robust Assurance Monitoring and Evaluation (AME). These ICT assets are the bedrock of the digital environment and by implication catalysts for national development. They facilitate the operation and interconnectivity of systems in cyberspace and play a critical role in ensuring cybersecurity. With the current proliferation of cyber threats, the role of these ICT systems in ensuring cybersecurity is now more crucial. The pervasive nature of cyber threats now requires ICT systems that are agile, adaptive and responsive.

We recognise the role of these ICT systems in strengthening the security posture of our digital landscape. Hence, we envisage the widespread deployment of robust and high-quality cybersecurity technology to safeguard our presence in cyberspace. Our approach is therefore to engender the emplacement of good practices and standards for our cybersecurity technologies and the deployment of quality controls and security processes.

9.1 STANDARDS AND GOOD PRACTICES

Our focus is to strengthen ongoing efforts in the public and private sector to ensure the security of data transmission and processing systems and platforms against unauthorised access and cybersecurity threats. Therefore, our efforts shall concentrate on enhancing the design and adoption of standards and good practices related to the procurement, development, utilisation and deployment of cybersecurity hardware and software technology systems. Stakeholders in government and industry shall jointly develop and promote the adoption of ICT and cybersecurity standards across government departments and agencies and the private sector, in line with international good practices. NITDA shall interface with NCCC and other relevant stakeholders to champion this drive through promotion of guidelines as well as compliance arrangements. Accordingly, government departments and agencies have a role to ensure adherence to stipulated guidelines and standards.

Furthermore, NCCC shall provide oversight through the periodic audit of CNII and any other entity as may be determined. For the private sector, companies and businesses shall take the lead in promoting and ensuring adherence to laid out standards under the guidance of relative regulatory agencies. These efforts shall be complemented by capacity building of cybersecurity compliance officers and CNII auditors to maintain necessary oversight. Additionally, we shall promote efforts to interface with global partners to ensure continuous alignment with international standards and good practices. Our efforts shall also focus on gathering adequate cyber threat intelligence to protect our digital economic infrastructure. This shall be driven through effective identification of financial technology systems/products and development of mechanisms to enhance their resilience to mitigate financial crime.

9.2 QUALITY CONTROL AND SECURITY PROCESSES

We shall continue to support ongoing efforts in the public and private sector to enhance the quality of cybersecurity hardware and software systems deployed to support government operations, businesses and commercial and financial services in cyberspace. Our focus shall be the emplacement of oversight on procurement, development, deployment and operation of technology systems through guidelines and coordinated audit and clearance arrangements. Government shall drive the process of ensuring that businesses and organisations abstain from the use of pirated or sub-standard software and hardware systems through guidelines and adequate compliance mechanisms.

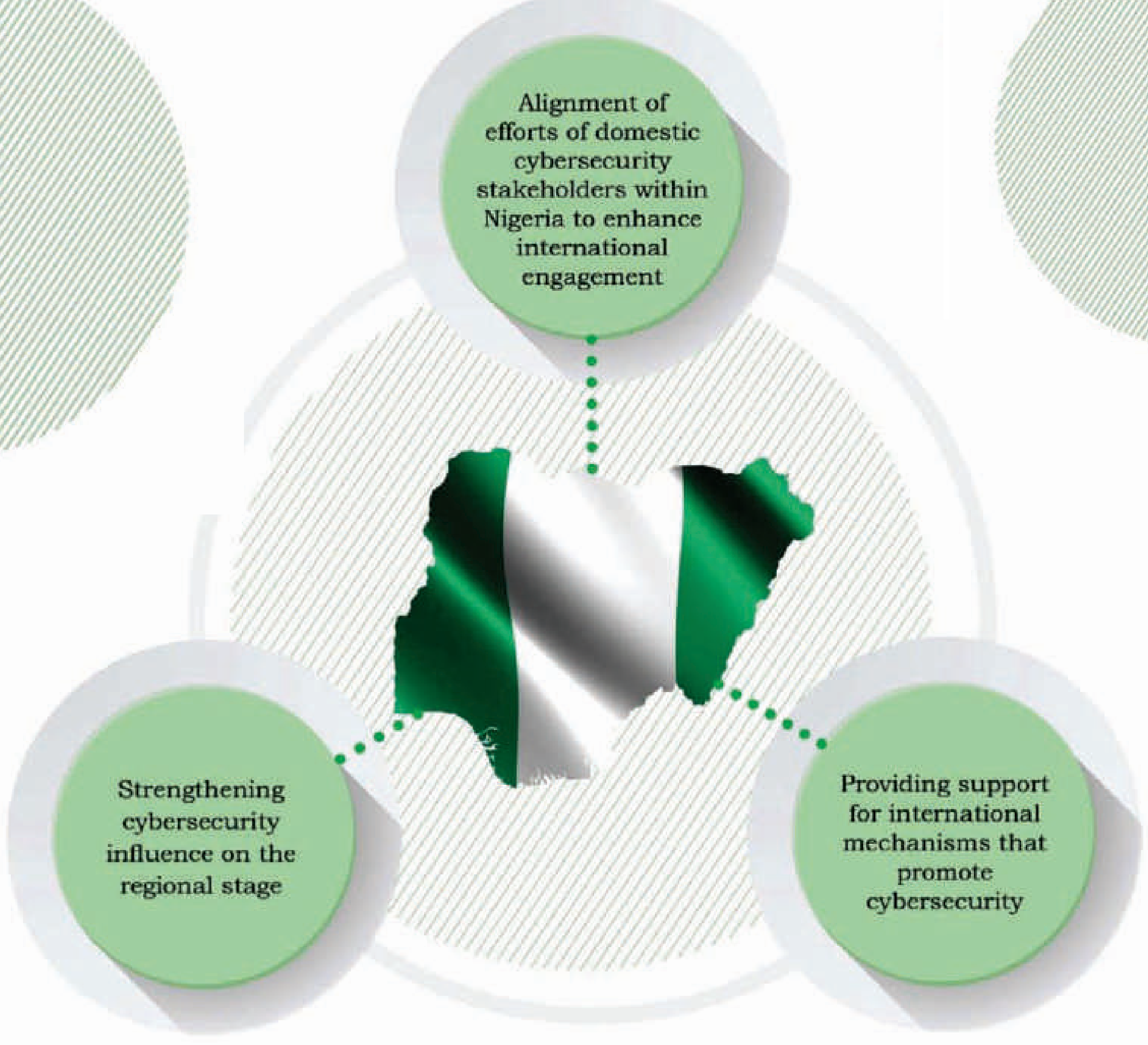
Our efforts shall also entail promoting the deployment of standardised technical security and cryptographic controls, ranging from antivirus, firewalls and intrusion detection systems, to end-to-end encryption and multi-factor authentication, amongst others, for security and data protection across government and private sector systems, especially those handling sensitive information. Efforts to promote uptake of security controls amongst general Internet users shall be driven through regular awareness campaigns, especially the promotion of security controls for mobile devices.

We are also dedicated to facilitating confidential and trusted data flow across stakeholders in government as well as the private sector. We shall therefore continue to encourage appropriate adoption of Public Key Infrastructure (PKI) to ensure the security of data flow across networks and online activities and services, such as e-government, e-business and financial transactions. We shall coordinate effective use and expansion of PKI through robust vetting mechanisms. We shall also promote mechanisms that assure the integrity of PKI elements such as certificate authorities, registration authorities, certificate databases and certificate procedures, amongst others.

Furthermore, we shall develop the necessary mechanism for annual licensing and registration of cybersecurity training centres and institutions, Managed Security Service Providers (MSSPs) and cyber cafes amongst other related services, in line with global best practices. Our approach is to ensure that all MSSPs, cyber cafes and other relevant cybersecurity vendors and practitioners are duly registered and licensed by NCCC to operate in Nigeria. In furtherance to this, NCCC shall be the sole body to license cybersecurity professionals in the country.

CHAPTER TEN

Enhancing International Cooperation



Alignment of efforts of domestic cybersecurity stakeholders within Nigeria to enhance international engagement

Strengthening cybersecurity influence on the regional stage

Providing support for international mechanisms that promote cybersecurity

CHAPTER 10

ENHANCING INTERNATIONAL COOPERATION

Noting the borderless nature of cyberspace, Nigeria would seek collaboration with other countries to ensure effective implementation of this strategy. To this end, the country will deepen its relationship with regional and global partners, set conditions for favourable outcomes in bilateral and multilateral relations, while also promoting her regional influence and cybersecurity interests. Combating cyber terrorism and other forms of cybercrime is important to our national interest. We recognise that this can be effectively achieved through bilateral and multilateral collaboration.

Therefore, we will continue to participate in international forums dedicated to combating cybercrime and addressing cybersecurity. The NCCC shall serve as our national point of contact for cybersecurity issues that require urgent assistance from other countries. We anticipate that our commitment to international partnerships will give us the best chances of preventing or addressing cyber attacks. Additionally, we recognise that the security and resilience of our regional and other international partners is vital to ensuring our national security and prosperity. Against this backdrop, our strategy will focus on coordinating the responsibilities of domestic cybersecurity stakeholders within the country to enhance international engagement, strengthening cybersecurity consensus and influence on the regional stage and providing support for international mechanisms that promote cybersecurity.

10.1 COORDINATION FRAMEWORK FOR INTERNATIONAL ENGAGEMENT

We will align the responsibilities of all stakeholders in government and the private sector including academia towards enhancing cybersecurity collaboration on the international stage. To this end, we will focus on the development of requisite organisational structures and protocols for international engagement. This effort shall emanate from the NCCC as the international focal point and cascade down to all stakeholders across our cyber ecosystem.

This will enable us to clearly harmonise the focus of all key stakeholders for international cooperation and for cybersecurity dialogue on the international arena. It will also pave way for synchronisation of our legal framework with the priorities of the international community. As part of efforts to support our coordination framework, we shall facilitate capacity development and skills acquisition for personnel in the areas of international cyber law and cyber diplomacy. This effort will also support our drive to promote mutual trust, confidence, transparency and joint establishment as well as adoption of international cybersecurity norms. Furthermore, it will promote multilateral and bilateral partnerships in the areas of incident response, cybercrime prevention, child online safety, cyber defence and best practices, amongst others.

10.2 REGIONAL CYBERSECURITY DEVELOPMENT

We shall increase our involvement and influence on cybersecurity developmental issues in Africa and the West African sub-region. By this, we will spearhead the creation of new initiatives, forums and mechanisms to enhance regional cooperation in cybersecurity while strengthening existing Economic Community of West African States (ECOWAS) and African Union (AU) arrangements and instruments.

We shall also promote capacity development to improve cross-border law enforcement, judicial and other mechanism of cooperation to combat cybercrime, promote cross-border knowledge and technology transfer, support the establishment of regional coordination frameworks, enhance information sharing on cyber threats and drive regional cybersecurity market growth. We recognise that these actions are reliant on our continuous interfacing with relevant regional and sub-regional cybersecurity establishments.

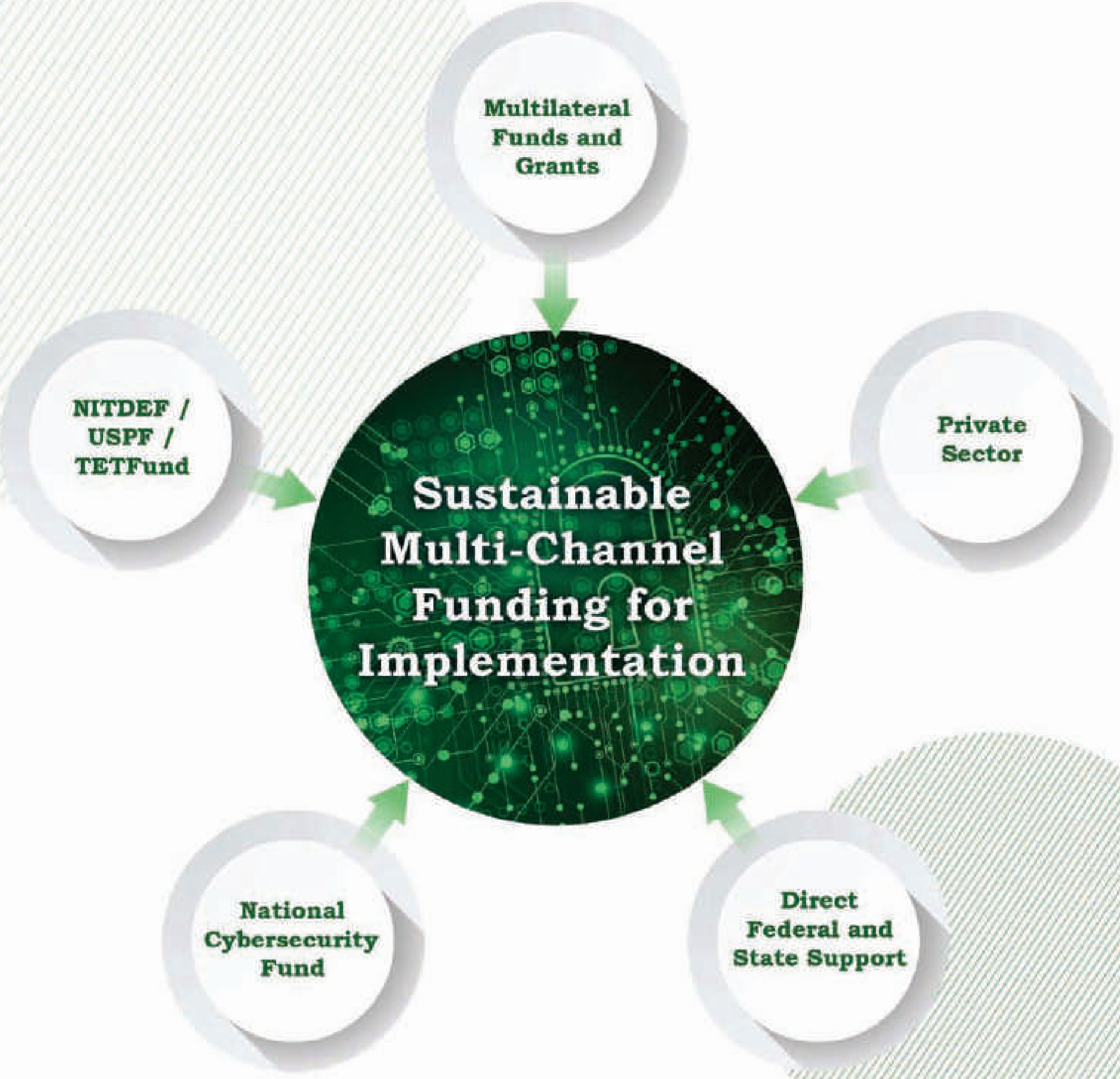
10.3 INTERNATIONAL COOPERATION

Nigeria is committed to strong international cooperation in cybersecurity as part of our shared responsibility to promote global economic development and international security. To this end, our priority is to work closely with other countries and multinational organisations such as the Global Forum on Cyber Expertise (GFCE) to garner consensus in cyber law enforcement, threat intelligence sharing, adoption of collective cyber norms and cybersecurity best practices, policy and strategy formulation and implementation, technology exchange and capacity development, including cyber defence.

We will accelerate our efforts to cooperate and combat transnational cyber threats and cybercrime. We will also further our participation and influence through dialogue on the global forum, promoting ratification of cybersecurity conventions and engendering embracement of the tenets of international cyber laws. Furthermore, we shall strengthen information sharing with our global partners through established regional and international arrangements and mechanisms.

CHAPTER ELEVEN

Funding and Sustainability


Multilateral Funds and Grants
NITDEF / USPF / TETFund
Private Sector
Sustainable Multi-Channel Funding for Implementation
National Cybersecurity Fund
Direct Federal and State Support

CHAPTER 11

FUNDING AND SUSTAINABILITY

We recognise the importance of availability of substantial financial resources to facilitate the actualisation of our national cybersecurity programme. Our focus is therefore to identify potential sources of funding relevant to the development of Nigeria's national cybersecurity. We also recognise the criticality of assessing the funding requirement of our proffered cybersecurity activities, initiatives and programmes while prescribing mechanisms to ensure availability and sustainability of identified funding streams.

11.1 FUNDING AND SUSTAINABILITY IMPERATIVES

We will adopt a multi-channel funding approach for sustaining and improving our national cybersecurity program by avoiding over-reliance on funding from government programs. Therefore, we will harness relevant financial incentives, fiscal policy, economic and other funding options that will enhance successful commitment to our national cybersecurity program. Nigeria shall also continue to sustain efforts in cybersecurity through the National Cybersecurity Fund (NCF) mechanism as stipulated in extant laws and regulations, in addition to other appropriate funding mechanisms. Furthermore, we shall enhance existing provisions for national cybersecurity funding, through the following options:

- Provision of institutional fund for the establishment of NCCC
- Provision and prioritisation of national cybersecurity budget framework
- Reformation and alignment of cybersecurity budget with implementation assessment
- Empowerment of NCCC to employ appropriate collaborative funding mechanisms including the remittance of 0.005 levy on charges of all electronic transaction in line with extant laws

11.1.1 Financial Incentives

We shall develop procedures to incentivise investment in indigenous cybersecurity related activities such as tax holidays. We shall also set up Cybersecurity Innovation Grants through public-private sector equity funding to encourage investment in cybersecurity research, innovation and development of new technologies. Furthermore, we shall encourage funding for broad base multi-sectoral capacity development.

11.1.2 Fiscal Policy Initiatives

We shall focus on identifying and selecting targeted cybersecurity solutions for time-based competition by different categories of innovators and with support fund to encourage innovation and development of new technologies. We shall also promote the grant of pioneer status (tax holidays) to interested cybersecurity investors for the development and production of cybersecurity related products, applications and equipment. We will also encourage fiscal policy that supports development of cybersecurity. To this end, Government shall explore the following funding options, amongst others:

- National Cybersecurity Program Research, Innovation and Development will access extra-budgetary funding sources and leverage extant institutional funds such as NCF, National Information Technology Development Fund (NITDEF), Universal Service Provision Fund (USPF) and Tertiary Education Trust Fund (TETFund)
- Direct federal and state budgetary allocation for cybersecurity funding – with emphasis on local content solutions
- Facilitation of requisite financial sustainability for NCCC by an Act of the National Assembly for annual government budgetary allocation to cater for core capital and recurrent expenditure
- Encourage private sector organisations to fund the protection of (people/ecosystem) network endpoints particularly individual customer endpoints as they enhance the integrity of the core national network infrastructure.

11.2 MULTILATERAL FUNDING AND GRANTS

We recognise the role of multi-lateral funding for enhancing our national cybersecurity development. We shall therefore ensure adequate coordination of the channels and protocols through which states, organisations and establishments amongst others make financial and other resources available to Nigeria for implementation and fulfilment of our national cybersecurity commitments. To this end, NCCC shall be responsible for developing necessary protocols to guide how stakeholders in the Nigerian cybersecurity ecosystem can engage with funding bodies, donors and other relative arrangements, for the acquisition of multilateral funds and grants. Government shall also continue to facilitate cooperation of state and local governments, in the area of national cybersecurity funding aspirations, to ensure adequate harmonisation of efforts of all stakeholders.

CHAPTER TWELVE

Conclusion

CHAPTER 12

CONCLUSION

The National Cybersecurity Policy and Strategy shall have 5 years life span with annual performance reporting. Throughout the period, there shall be continuous policy guidance, monitoring and review of the implementation plan. The responsibility for effective implementation of the initiatives lies with every stakeholder across the entire cyber ecosystem.

Achieving a national cyber security program requires strong commitment from Government to galvanise the much-needed Specific, Measurable, Achievable, Realistic and Timely (SMART) implementation of proffered strategic actions. Stakeholders across the private sector must also exhibit necessary commitment by working closely with Government within the proffered scope. We recognise that there are multiple competing considerations within each stakeholder's approach to addressing cybersecurity. Nonetheless, the responsibility lies on all stakeholders to ensure concerted, shared and unified efforts towards realistic implementation of the initiatives proffered in this national document.

As the country sets out to implement the strategic measures and unlock national potentials for ensuring progressive use of the nation's cyberspace, all stakeholders have a mandate to make conscious effort to balance the security, social and economic imperatives of cyberspace with the cybersecurity needs of Government, industry, academia and the international community.

APPENDIX

IMPLEMENTATION PLAN

PREAMBLE

We recognise the need to develop a plan for the implementation of our proffered initiatives, programs and activities, amongst others. Our implementation plan therefore outlines the details of our express and implied tasks, deliverables, implementation requirements, timelines and key performance indicators (KPIs) amongst others. It is the roadmap for driving success, measuring progress and transforming our prescribed strategic actions into reality.

MONITORING AND EVALUATION

The policy shall mainstream frameworks for measuring accountability and performance of outlined national cybersecurity initiatives and programmes. The objective is to ensure continuous monitoring of the implementation program and to provide assurance that the program continues to meet stakeholders' expectations within the cybersecurity ecosystem.

Appropriate mechanisms shall be emplaced for accountability and performance measurement of the strategy implementation. To this end, the Cybercrime Advisory Council (CAC) shall establish a National Steering Committee on Performance Monitoring and Evaluation (NSC-PME), as a multi-stakeholder steering committee which shall monitor overall progress and performance and report to the CAC. An annual performance report on Nigeria's national cybersecurity, in line with the direction and provisions of the National Cybersecurity Policy and Strategy shall be submitted to the CAC by the NSC-PME. Furthermore, the overall policy direction, relevant approvals and accountability of all subsequent activities, including the strategy implementation shall be anchored by the CAC.

Our efforts shall also entail the monitoring and review of cybersecurity capabilities and level of preparedness of stakeholders at the national, state, sectoral and private sector levels to ensure continuous improvement and development of relevant capabilities, skills and proficiencies. Additionally, we shall continue to conduct information security audits and process audits for government entities while also coordinating and validating security audits and process audits of self-assessment entities. Our focus will also be directed to the development of benchmarks for regular statistical data and situational reports on Nigeria's cybersecurity status.

ACTION PLAN FOR STRATEGY IMPLEMENTATION

The objective of the Action Plan for implementing our national cybersecurity strategy is to articulate our priorities and outline the direction through which they will be effectively implemented. The Action Plan outlines our priority activities and highlights the stakeholders that are entrusted with driving the process towards their actualisation. All stakeholders are therefore enjoined to utilise the action plan as a compass to align, focus and consolidate their efforts towards progressive and successful implementation of our national cybersecurity strategy.

ACTION PLAN FOR STRATEGY IMPLEMENTATION

PILLAR 1: STRENGTHENING CYBERSECURITY GOVERNANCE AND COORDINATION

Ser	Reference	Express/Implied Task	Further Actions Required	Responsible Agency	Implementation Requirements	Estimated Budget (₦)[1]	Timeframe[2]	Performance Metrics	
								Rational Outcomes	KPI
(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)	(i)	(j)
1.	Chapter 3.1	**Establishment and Operationalisation of the National Cybersecurity Coordination Centre (NCCC)**	Development and approval of framework for the establishment of NCCC Allocation/development of physical structure and facilities for NCCC Generation of manpower for NCCC Allocation of operational budget for day-to-day running of NCCC	ONSA (CAC) ONSA (CAC) Relevant Agencies ONSA (CAC) FMoF	Approval of framework for establishment of NCCC Funding for upgrade of existing infrastructure or construction of new facility for NCCC Human resources and inter-agency engagements for NCCC manpower generation		Short Term Short Term Short Term Short Term	Framework for establishment of NCCC developed and approved Physical structure for NCCC available Adequate manpower from relevant agencies deployed or seconded to NCCC Budgetary allocation for day-to-day running of NCCC approved	NCCC operational Enhanced governance and coordination of cybersecurity in Nigeria Improvement in inclusiveness of all relevant stakeholders Stipulated mandates of NCCC effectively delivered
2.	Chapter 3.2	**Establishment of National Cybersecurity Dialogue Platform**	Design and installation of a platform for secured dialogue and information sharing between all relevant cyber stakeholders	ONSA (NCCC) FMoCDE (NITDA NCC)	Funding for design, commissioning and installation of the Dialogue Platform across terminals of all stakeholders		Short Term	Cybersecurity Dialogue Platform established	Improved synergy and enhanced information sharing across stakeholders

PILLAR 2: FOSTERING PROTECTION OF CRITICAL NATIONAL INFORMATION INFRASTRUCTURE

Ser	Reference	Express/Implied Task	Further Actions Required	Responsible Agency	Implementation Requirements	Estimated Budget (₦)[1]	Timeframe[2]	Performance Metrics	
								Rational Outcomes	KPI
(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)	(i)	(j)
1.	Chapter 4.1 to 4.5	**Identification, Designation and Protection of Critical National Information Infrastructure (CNII)**	Development of framework and guidelines to administer the identification, designation, protection and periodic audit of CNII in the public and private sectors Establishment of Trusted Information Sharing Network (TISN) made up of owners and operators of CNII and government stakeholders	ONSA (NCCC) Relevant Stakeholders Security and LEAs TISN	Human resources, technical expertise and inter-agency engagements for effective coordination of activities related to CNII protection Human resources, technical expertise and funding for technical design, administration and day-to-day functioning of TISN		Short Term Short Term	Framework and guidelines for identification, designation, audit, management and protection of CNII developed and operational TISN established and functional, and collaboration activities commenced	Improvement in coordination of activities related to CNII protection Enhanced information sharing and synergy between relevant stakeholders and owners/operators of CNII
			Development and Execution of CNII Protection Plan	ONSA (NCCC) Security and LEAs FMoCDE (NITDA, NCC) Regulatory Agencies TISN	Human resources, inter-agency engagements and funding for development and implementation of CNII Protection Plan		Medium Term	CNII Protection Plan developed and operational	Effective risk mitigation and reduction in scale and impact of physical and cyber attacks on CNII

2.	Chapter 4.3 to 4.5	**Security of Internet and Telecoms Gateways**	Arrangements to secure the nation's Internet and telecommunications gateways from, disruption or destruction	ONSA (NCCC/ ngCERT) Regulatory Agencies, TISN	Human resources, technical expertise, tools, inter-agency engagements as well as funding for development of arrangements to continually secure Internet and telecoms gateways		Short Term	Internet and telecoms gateways secured	Reduction in security risks and attacks on Internet and telecoms gateways
3.	Chapter 4.3 to 4.5	**Disaster Recovery Plan for CNII**	Develop and employ effective mechanisms to ensure business continuity and rapid recovery of essential services from cyber attacks Disaster recovery and business continuity mechanisms inspected as part of CNII audit	ONSA (NCCC) FMoCDE (NITDA) NEMA Relevant SLEAs TISN	Human resources, technical facilities, inter-agency engagements as well as funding for development of disaster recovery mechanisms		Medium Term	Disaster recovery mechanisms emplaced	Enhanced recovery and seamless continuity in the operation of CNII in the event of attacks, disaster or technical failure
4.	Chapter 4.3 to 4.5	**Development of Budget for CNII Protection**	Creation of annual list of eligible CNII under protection Budget allocation for protection of designated CNII in the public and private sectors	FMoF (BNP) ONSA (NCCC)	Inter-agency and inter-ministerial engagements for development, appropriation and continuous update of annual budget for CNII protection		Short Term (Annual)	CNII protection budget appropriated	Availability of requisite funding for activities related to CNII protection

PILLAR 3: ENHANCING CYBERSECURITY INCIDENT MANAGEMENT

Ser	Reference	Express/Implied Task	Further Actions Required	Responsible Agency	Implementation Requirements	Estimated Budget (₦)[1]	Timeframe[2]	Performance Metrics	
								Rational Outcomes	KPI
(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)	(i)	(j)
1.	Chapter 5.1 to 5.6	**Development of National Cybersecurity Crisis Response Mechanism**	Development of frameworks and regulations for establishment of CSIRTs Development of ACIS System for information sharing on cyber incidents Development of National Cybersecurity Crisis Response Plan (NCCRP)	ONSA (NCCC) ngCERT Sectoral CSIRTs Regulatory Agencies Relevant Stakeholders	Human resources, technical expertise, tools, inter-agency engagements and funding for establishment of CSIRTs, and development of ACIS platform, NCCRP as well as operationalisation of other activities towards enhancing cyber crisis response		Short to Medium Term	Relevant Sectoral CSIRTs established and operational ACIS installed and commissioned across terminals of all relevant agencies NCCRP developed and executed when required	Improved incident detection and response across all identified sectors of the economy Enhanced information sharing and prompt incident reporting Effective response to cyber incidents
2.	Chapter 5.4	**National Cybersecurity Readiness Exercises and Drills**	Organise and conduct periodic exercises and drills to assess national preparedness against cyber threat for timely mitigation and recovery in the event of attacks	ONSA (NCCC) ngCERT Sectoral CSIRTs Relevant MDAs CSIRTs (Private), Academia, Industry and International Partners	Human resources, multi-stakeholder engagement, tools and materials as well as funding for planning, conduct and evaluation of cyber exercises and drills		Short Term (quarterly drills and annual exercises)	Regular cyber drills organised and executed Quarterly evaluation reports developed with lessons learned	Improved synergy and enhanced cybersecurity readiness, protection and incidents response capabilities

3.	Chapter 5.5	**Development of Cyber Emergency Monitoring System (CEMS)**	Design and installation of CEMS for effective detection and interception of cyber threats and associated information sharing	ONSA (NCCC) ngCERT Sectoral CSIRTs ISPs and IXPs	Human resources expertise, inter-agency engagement and funding for design, commissioning and installation of CEMs across terminals of ngCERT and CSIRTs		Medium Term	CEMS commissioned and operational	Improved detection and interception of cyber threats Enhanced information dissemination on imminent cyber threats
4.	Chapter 5.7	**Human Resources and Technological Capacity Development for ngCERT, Sectoral and other CSIRTs**	Institutionalisation of technical capacity building, provision of technological capabilities and regular system maintenance, upgrades and support services Development of training programmes and provision of support services	ONSA (NCCC) ngCERT Regulatory Agencies Sectoral CSIRTs, Private Sector CSIRTs	Funding and inter-agency engagements for human and technological capacity development		Medium Term (Continuous Annually thereafter)	Human and-technological capacity developed and sustained Periodic conduct of training and provision of routine technical maintenance and support services for ngCERT and CSIRTs facilities	Enhanced ability of ngCERT and CSIRTs to carry out mandate of cyber incident monitoring, prevention and response
5.	Chapter 5.8	**Establishment of National Technical Working Group (NTWG) for Public Private Partnership (PPP)**	Establishment of NTWG of multi-stakeholder setup with representation from the international community	ONSA (NCCC) NTWG	Human resources, multi-stakeholder engagement and administration requirements for day-to-day functioning of NTWG		Medium Term	NTWG established and collaboration activities commenced	Improved synergy and enhanced information sharing between stakeholders

6.	Chapter 5.8	**Development and Implementation of PPP Cybersecure Framework for Security of National Digital Infrastructures**	Develop draft PPP Cybersecure Framework for consideration Develop modalities for implementation of approved PPP Cybersecure Framework	ONSA (NCCC) NTWG	Human resources expertise, inter-agency engagement and funding for development of Cybersecure Framework		Medium Term	NTWG, in collaboration with relevant stakeholders, to develop a PPP Cybersecure Framework to assure the security of the nation's digital infrastructures Continuous registration and renewal of licenses for: Cybersecurity Organizations, Cyber Cafes, Managed Security Service Providers, etc	PPP Cybersecure Framework approved and implementation activities commenced Number of cybersecurity organisations and related entities registered and licensed

PILLAR 4: STRENGTHENING LEGAL AND REGULATORY FRAMEWORK

Ser	Reference	Express/Implied Task	Further Actions Required	Responsible Agency	Implementation Requirements	Estimated Budget (₦)[1]	Timeframe[2]	Performance Metrics	
								Rational Outcomes	KPI
(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)	(i)	(j)
1.	Chapter 6.1	**Amendment of the Cybercrimes (Prohibition, Prevention Etc) Act 2015**	Constitute multi-stakeholder committee to review the Cybercrimes Act 2015 to accommodate establishment of NCCC and other areas as listed in the strategy document Development of draft Cybersecurity Act to cover cybercrime and other aspects of cybersecurity	CAC ONSA (NCCC) FMOJ NASS	Human resources, multi-stakeholder engagement, materials and funding for review of existing Cybercrimes Act towards development of new cybersecurity legislation Inter-agency arrangements for promulgation of new cybersecurity legislation		Short to Medium Term	Cybercrimes Act 2015 amended	Improved legislative framework for administration of cybersecurity in Nigeria
2.	Chapter 6.2	**Provision of Cybersecurity Framework for Strengthening National Data Governance and Protection of Digital Intellectual Property (IP)**	Development of national data framework for public service delivery, research, economy and security. Development of measures to ensure the safeguard of the digital content of intellectual property	ONSA (NCCC) CAC FMoCDE (NIMC) FMoE NOTAP Nigeria Copyright Commission NIRA	Human resources, inter-agency engagement and funding for development and security of national data framework Technical expertise and funding for development of IP protection frameworks		Long Term Medium Term	Frameworks for National Data Governance and IP Protection developed	Enhanced security of national data

3.	Chapter 6.2	**Harmonization of E-Business Legislative Framework**	Identifying existing laws related to e-business in Nigeria with a view to harmonising them	ONSA (NCCC) FMoJ FMoCDE FMoITI FCCPC	Human resources, multi-stakeholder engagement and materials for working group to harmonise e-business laws		Medium Term	Legislative Framework for Online Consumer Protection Developed	Harmonised provisions across all identified laws
4.	Chapter 6.2	**Enactment of Data Protection and Privacy law**	Enactment of a law regulating the storage, processing, transmission and access to personal data, which provides the necessary protection against unlawful access, usage and lawful dissemination	OSGF FMoJ FMoCDE (NITDA, NIMC -ID4D PSC) ONSA (NCCC) NSS	Human resources, multi-stakeholder engagement, materials and funding for development and enactment of legislative framework		Short Term	National Data Protection Legislative Framework enacted	Improvement in data protection and privacy Reduction in number of cases of data breaches
			Establish an independent and effective regulatory authority to coordinate data protection and privacy issues in Nigeria Develop Guidelines for Data protection procedures to include steps to be taken for customer consent, record retention, secure data disposal, international data transfer and complaint handling	OSGF FMoCDE (NIMC - ID4D PSC) ONSA (NCCC)	Inter-agency arrangements, human resources, materials and funding for establishment of regulatory authority and development of data protection guidelines		Short Term	Independent national regulator/body established and operational Guidelines developed and enforced	Improved coordination, administration and enforcement of data protection related activities

5.	Chapter 6.3	**Establishment of Mechanism for Filtering and Preventing the Spread of Online Child Abuse Materials (CAM) and Prosecution of Suspects within Nigeria's Jurisdiction**	Establish technology platform/mechanism involving ngCERT/ Internet Providers, Content Operators for reporting and removing or blocking access to illegal content or CAM	ONSA(NCCC) FMoJ FMoCDE (NITDA, NCC) FMoST LEAs NGOs	Technical expertise, training, human resources, tools, multi-stakeholder engagement and funding for development and operationalisation of mechanisms to combat CAM		Medium to Long Term	Technology platform/ mechanism deployed and operational	Reduction in Child Abuse Materials (CAM) on the Internet and social media in Nigeria's cyberspace
6.	Chapter 6.3	**Launching of National Child Online Safety Awareness Campaign and other related initiatives**	Constitution of Law Enforcement Task Force on Child Online Protection Development of programs and activities to promote awareness and education on child online safety Creation of National Register of Convicted Offenders	ONSA (NCCC) FMoJ FMoE FMoWASD NITDA LEAs NOA NGOs	Programmes, inter-agency engagements, human resources and funding for constitution and operationalisation of Task Force and launching of activities to enhance child online safety		Medium Term (Annually)	Awareness campaign launched and sustained Task force established National register created Cases of abuse reduced	Sustained channels for improving sensitization and mechanism for combating online child exploitation and abuse Reduction in number of cases of online child exploitation
7.	Chapter 6.4	**Launching of Online Safety Awareness and Education for Women and Breaking Barriers to Digital Gender Gap**	Development of multi-stakeholder forum to drive online gender protection and creation of opportunities to improve the participation of women in cybersecurity activities and engagements	ONSA (NCCC) FMoJ FMoE FMoWASD FMoCDE (NITDA) LEAs NOA NGOs	Programmes, inter-agency engagements, human resources and funding for running activities to enhance women online safety and promote digital gender equality		Medium Term (Annually)	Mechanisms to combat online gender exploitation developed Initiatives to drive women empowerment created	Reduction in number of cases of online exploitation of women Increase in the number of women engaged in cybersecurity

8.	Chapter 6.5	**Capacity Building for Law Enforcement and Judiciary**	Strengthening Cybersecurity capacity building for the judicial officers, legal practitioners and law enforcement officers	ONSA (NCCC) FMoJ LEAs NCTI NGOs	Technical expertise, training, human resources, tools, multi-stakeholder engagement and funding for capacity development		Medium Term (Recurrent)	Training program, Seminars, Workshops and Conferences organised and conducted	Capacity building for Judges and lawyers on cybercrime laws - Minimum of 50 judges and 200 lawyers per annum Capacity building for prosecutors and law enforcement agencies on digital forensics, cybercrime investigation and prosecution - minimum of 500 per annum
9.	Chapter 6.6	**Establishment of a Specialised Division for Cybercrime Related Cases in the Federal High Court**	Develop and implement modalities for the establishment of a division that will have the mandate to adjudicate exclusively on cybersecurity and related cases	ONSA (NCCC) FMoJ CJ of the Federal High Court	Human resources and expertise for establishment and operationalisation of specialised division		Medium Term	Establishment of a division at the Federal High Court on cybersecurity and related matters	Improvement in ability of courts to handle digital evidence and successfully prosecute cybercriminals

10.	Chapter 6.6	**Development of Digital Forensics Capacity and Provision of Regulatory Oversight Functions**	Establish a National Framework for the regulation, certification, technical support and collaboration of digital forensic laboratories across the country Develop modalities for human and technological capacity development for National Digital Forensic Laboratory	ONSA (NCCC) LEAs	Human resources, funding and inter-agency engagements for human and technological capacity development for digital forensic laboratories		Medium Term (Continuous Annually thereafter)	Framework developed and implemented Human and-technological capacity developed and sustained Periodic conduct of training and provision of routine technical maintenance and support services for laboratories	Number of successful digital forensics investigations

PILLAR 5: ENHANCING CYBER DEFENCE CAPABILITY

Ser	Reference	Express/Implied Task	Further Actions Required	Responsible Agency	Implementation Requirements	Estimated Budget (₦)[1]	Timeframe[2]	Performance Metrics	
								Rational Outcomes	KPI
(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)	(i)	(j)
1.	Chapter 7.1	**Establishment and Operationalisation of Defence Computer Security Incident Response Team (CSIRT) and Security Operations Centre (SOC)**	Setting up of Defence CSIRT and SOC to monitor and protect the Nigerian cyberspace and respond in event of escalating cyber-attack	MoD (DSA) ONSA (NCCC) FMoST(NASRDA) Sectoral CSIRTs	Technical expertise, training, human resources, tools, hardware and software systems, multi-stakeholder engagement and funding for establishment and operationalisation of CSIRT/SOC		Short Term	Defence CSIRT operational to Interface with ngCERT and other Sectoral CSIRTs for cyber incident management, technology and skills transfer and joint conduct of drills and exercises	Operational Defence SOC with agile Defence CSIRT Number of successful cyber drills and exercises Number of successful cyber attacks prevented
2.	Chapter 7.2	**Development of National Cyber Defence Plan (NCDP)**	Development of NCDP outlining arrangements for protection of the Nigerian cyberspace in the event of escalated national cyber-attack	MoD (DSA) ONSA (NCCC) FMoST(NASRDA) Relevant Stakeholders	Human resources, technical expertise, inter-agency engagements and funding for development and implementation of NCDP		Medium Term (Continuous Thereafter)	NCDP formulated and operational	Effective response to national cyber attacks on CNII and impact prevention

3.	Chapter 7.3	**Human Resources and Technological Capacity Development for Defence CSIRT**	Institutionalisation of technical capacity building, provision of technological capabilities and regular system maintenance, upgrades and support services	MoD (DSA) ONSA (NCCC)	Funding, tools and inter-agency engagements for human and technological capacity development		Medium Term (Continuous Annually thereafter)	Human and-technological capacity developed and sustained Periodic conduct of training and provision of routine technical maintenance and support services for Defence CSIRT facilities	Enhanced ability of Defence CSIRT to carry out mandate of cyber defence Reduction in the number of successful cyber attacks and increase in the number of quelled cyber attacks

PILLAR 6: PROMOTING A THRIVING DIGITAL ECONOMY

Ser	Reference	Express/Implied Task	Further Actions Required	Responsible Agency	Implementation Requirements	Estimated Budget (₦)[1]	Timeframe[2]	Performance Metrics	
								Rational Outcomes	KPI
(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)	(i)	(j)
1.	Chapter 8.1	**Activities to Develop Responsible Cybersecurity Culture and Behaviour to Engender a Safe and Trusted Internet and Digital Environment**	Develop programs and activities to promote the confidence and use of e-government, e-business and e-transactions platforms in the Nigerian cyberspace Conduct of activities to ensure that individuals and organisations are aware of their responsibilities within the cyberspace	ONSA (NCCC) FMoCDE (NITDA, NCC) FMoI&C(NBC) NOA NGOs Private Sector	Human resources, technical expertise, tools and systems, trainings, inter-agency engagements and funding for launch of activities to promote cybersecurity culture		Medium Term (Continuous Annually thereafter)	Periodic training programmes for government employees conducted Mechanisms delivered for service providers and other operators of online digital services to protect online platforms Provision of free publicly available materials on online safety for users of the Internet among the general public and conduct of surveys	Number of training programmes conducted by government agencies Online protection measures implemented by private sector service providers General improvement in safety and confidence of online environment

2.	Chapter 8.2	**Cybersecurity Human Resources and Workforce Development**	Development, promotion and accreditation of cybersecurity courses/ curriculum in academic institutions Integrate cybersecurity awareness efforts into ICT courses at the school, academic and vocational levels	FMoE (NUC, NBTE, UBEC) FMoCDE (NITDA, NCC) ONSA (NCCC)	Funding, tools and multi-stakeholder engagements for human resources and workforce capacity development		Long Term (Continuous Annually thereafter)	Developed curriculum for Cybersecurity Adequate training materials and resources Capacity development of cybersecurity academic teachers Framework to incentivise skills and talents in cybersecurity such as award of grants to institutions for cybersecurity research and traineeship in cybersecurity	Rate of enrolment and successful completion of quality cybersecurity education in universities and other educational institutions
			Establish National Cybersecurity Training Institute (NCTI) Skills acquisition and professional development in cybersecurity	ONSA (NCCC, NCTI) Relevant Stakeholders	Funding, tools and multi-stakeholder engagements for professional development		Long Term (Continuous Annually thereafter)	NCTI established Standardised certification courses created	Number of certified cybersecurity professionals in the private sector and Government
			Research and Development (R&D) in Cybersecurity	FMoE Academia and Industry ONSA (NCCC)	Funding, tools and multi-stakeholder engagements for research and development		Long Term	Roadmap to harness cybersecurity R&D efforts developed	Number of successful quality cybersecurity R&D projects

3.	Chapter 8.3	**Indigenous Cybersecurity Technology Development**	Development of competitive indigenous cybersecurity products and services in the market Funding of cybersecurity R&D projects	FMST (NOTAP) FMoCDE (NITDA) FMoE (NUC) Academia & Industry ONSA (NCCC) TETFund NGOs	Technical expertise, multi-stakeholder engagement, funding and organisations to drive indigenous technology development		Long Term (Continuous thereafter)	Establishment of cybersecurity technology innovation centres and laboratories in institutions of learning and industry	Increase in number of quality indigenous cybersecurity software and hardware deployed
4.	Chapter 8.3	**Development of a Cyber Insurance Sector**	Promotion of cyber insurance products and services Alleviating potential consequences of cyber incidents	NAICOM ONSA(NCCC)	Human resources, multi-stakeholder engagement, technical expertise, funding and training to develop cyber insurance sector		Long Term	Increased coverage for risks associated with cyber incidents	Increase in cyber liability coverage
5.	Chapter 8.4	**Cybersecurity Awareness and Sensitisation Campaign**	Develop Cybersecurity Awareness programs in Local Languages Encourage the National Cybersecurity Awareness Month (NCAM) Private Sector Partnership for Awareness and Capacity Building	NOA ONSA (NCCC) FMoCDE LEAs NGOs NAN NIRA ATCON CSEAN ISPAN CPN NCS	Human resources, technical expertise, tools and systems, trainings, inter-agency engagements and funding for launch of sensitisation campaign		Short Term (Continuous)	Cybersecurity Information Portal launched Awareness Activities on Cybersecurity commenced Private Sector Awareness Forum created Forum created for cybersecurity professionals including the ones in Diaspora	Awareness in Local Languages Number of NCAM activities General improvement in cybersecurity awareness through conduct of surveys

6.	Chapter 8.5	**Mechanisms to Mitigate Risks Associated with Virtual Assets**	Adoption of mechanisms to drive progressive use of virtual currencies while addressing associated risks	FMoF (CBN, NFIU) ONSA (NCCC) Other relevant stakeholders	Human resources, technical expertise, tools and systems, inter-agency engagement and funding for risk mitigation measures		Medium Term	Strengthening frameworks for managing virtual assets Driving Sensitization and Collaboration on Virtual Assets	Risk Management Framework for Virtual Assets Developed
7.	Chapter 8.5	**Protection of Digital Economic Infrastructure**	Identification and protection of FINTECH, innovation sectors and financial platforms	ONSA (NCCC) FMoF (BNP, CBN) FMoCDE NDIC NBC (Banking Sector) NFIU SEC	Technical expertise, tools and systems, multi-stakeholder engagement, human resources, training and funding to emplace activities to protect digital economic infrastructure		Long Term	Integrated threat intelligent System for the financial industry	Mitigating financial crime and improved resilience of FINTECH products

PILLAR 7: ASSURANCE MONITORING AND EVALUATION

Ser	Reference	Express/Implied Task	Further Actions Required	Responsible Agency	Implementation Requirements	Estimated Budget (₦)[1]	Timeframe[2]	Performance Metrics	
								Rational Outcomes	KPI
(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)	(i)	(j)
1.	Chapter 9.1	**Development and Adherence to Cybersecurity Technology Standards**	Design and adoption of technical standards and good practices Mechanism to ensure adherence to technical standards and good practices Periodic audit of CNII, and Government and private sector ICT and cybersecurity system Capacity building for auditors and compliance officers	FMoCDE (NITDA) Regulatory Agencies ONSA (NCCC)	Human resources, training, tools and systems, inter-agency engagements and funding for development and enforcement of standards as well as capacity building for compliance officers		Medium Term	Cybersecurity Technical Standards and Good Practices Guidelines developed Activities launched to publicise and promote guidelines Interface with global partners to ensure alignment with international standards	Reduction in use of sub-standard software and systems Number of successful audits conducted
2.	Chapter 9.2	**Improvement of Cybersecurity Quality Control and Security Processes**	Enhancement of quality of cybersecurity systems deployed for government operations, businesses, commercial and financial services Promotion of standardised technical security and cryptographic controls	FMoCDE (NITDA) Regulatory Agencies ONSA (NCCC**)**	Technical expertise, tools, inter-agency engagements and funding for promotion of quality control and security processes		Medium Term (Continuous Thereafter)	Audit on procurement, deployment and development of technology systems Quality antivirus, IDS, IPS, E2E encryption, multifactor authentication etc	Quality of cybersecurity software and technical systems enhanced based on feedback and audit reports

3.	Chapter 9.2	**Coordinate and secure effective use and expansion of Public Key Infrastructure (PKI) through robust vetting** **Development of National Framework for Cybersecurity Regulations and Compliance**	Certification of registration authorities Ensure management system and policy of central directories Develop modalities to ensure conformity and enforcement of national cybersecurity regulation standards and guidelines of PKI value chain	FMoCDE (NITDA,NIMC, Galaxy Backbone) ONSA (NCCC)	Technical expertise, tools, inter-agency engagements and funding for development and enforcement of guidelines for PKI		Medium Term Long Term	A trustworthy digital communication and transaction environment Framework for Cybersecurity regulations and compliance developed and enforced	Developed framework for cybersecurity regulations and compliance

PILLAR 8: ENHANCING INTERNATIONAL COOPERATION

Ser	Reference	Express/Implied Task	Further Actions Required	Responsible Agency	Implementation Requirements	Estimated Budget (₦)[1]	Timeframe[2]	Performance Metrics	
								Rational Outcomes	KPI
(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)	(i)	(j)
1.	Chapter 10.1	**Capacity Development in International Cyber Law and Cyber Diplomacy**	Development of capacity to harmonise the responsibilities of stakeholders across government, academia and industry for enhanced regional and international engagement	FMoJ FMoFA NIIA ONSA (NCCC)	Funding, tools, expertise and multi-stakeholder engagements for capacity development in cyber law and diplomacy		Medium Term (Continuous Thereafter)	Training programmes and related activities on cyber diplomacy and international cyber law launched	Number of trained professionals in cyber diplomacy and international cyber law Improvements in dialogue and discussions on the global stage
2.	Chapter 6.7 and Chapter 10.2	**Cross Border Cybersecurity Law Enforcement to Combat Cybercrime**	Development of mechanisms to enhance bilateral and multi-lateral collaboration towards combating cybercrime	FMoJ FMoFA ONSA (NCCC) SLEAs	Multilateral engagement, technical expertise, human resources, training and funding to develop capacity and drive synergy		Medium Term (Continuous Thereafter)	Improved collaboration between law enforcement and judiciary for cross-border investigation, prosecution and transfer of digital evidence	Increase in successful number of cross-border processing of cybercrime cases
3.	Chapter 10.3	**International cooperation**	Review membership of recognised International bodies Facilitate cybersecurity cooperation among stakeholders, international bodies	FMoFA FMoJ ONSA (NCCC) NIIA	Multilateral engagement, expertise, training and funding to enhance international synergy		Long Term	Enhanced International Cooperation	Improved participation in global cybersecurity activities, dialogue, programs and initiatives

4.	Chapter 10.3	**Acceding to International Cybersecurity Conventions**	International cooperation mechanisms to enhance synergy in global cybersecurity concerns and improve access to technical support, influence and outreach	ONSA(NCCC) FMoJ FMoFA	Expertise, multi-stakeholder engagements and multilateral engagements to enhance consultation towards endorsing identified cybersecurity conventions		Medium Term	Consultation and accession to International Conventions on Cybercrime and other multi-lateral instruments	international conventions endorsed

[1] Relevant stakeholders are to develop budgetary requirements for implementation of express/implied tasks. Budgetary requirements would be subject to validation by the Cybercrime Advisory Council (CAC).

[2] **Short Term** (First and Second Quarter 2021), **Medium Term** (Third 2021 to Second Quarter 2022) **Long Term** (Third Quarter 2022 – Fourth Quarter 2025)

FEDERAL REPUBLIC OF NIGERIA

NATIONAL CYBERSECURITY POLICY AND STRATEGY 2021
Summary

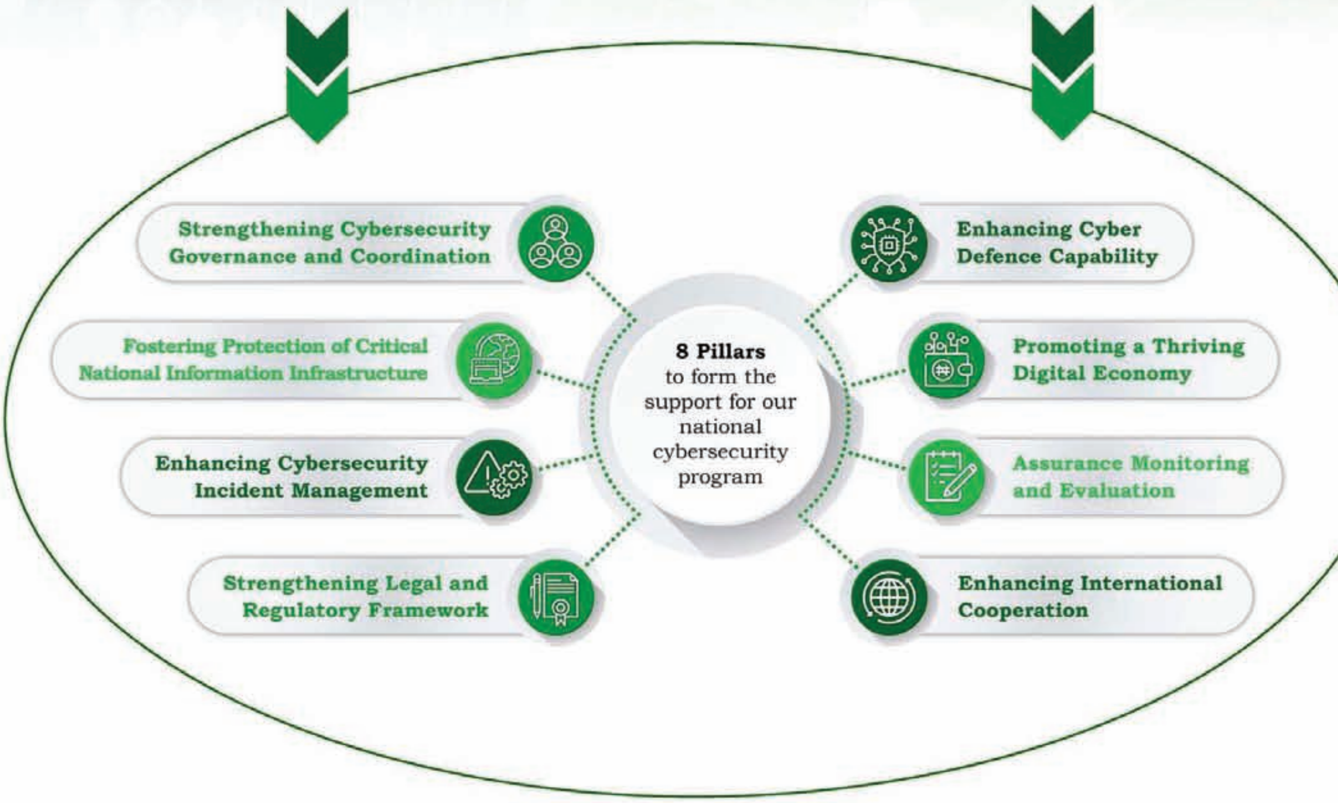
VISION

A safe and secure digital community that provides opportunities for its citizenry and promotes peaceful and proactive engagements in cyberspace for enhanced national prosperity

MISSION

To foster a trusted cyber environment that optimises Nigeria's cybersecurity readiness and coordination capacities towards addressing the nation's cyber risk exposure

The National Cybersecurity Policy and Strategy 2021 is a purposeful and living document which outlines the roadmap for realisation of our cybersecurity Vision and Mission. The document is a confluence of ends, ways and means which articulates the efforts of all stakeholders and emplaces our National Cybersecurity Programme on 8 critical pillars



8 Pillars to form the support for our national cybersecurity program

- **Strengthening Cybersecurity Governance and Coordination**
- **Fostering Protection of Critical National Information Infrastructure**
- **Enhancing Cybersecurity Incident Management**
- **Strengthening Legal and Regulatory Framework**
- **Enhancing Cyber Defence Capability**
- **Promoting a Thriving Digital Economy**
- **Assurance Monitoring and Evaluation**
- **Enhancing International Cooperation**

In line with the provisions of Section 41 of the Cybercrimes (Prohibition, Prevention, Etc) Act 2015 which empowers the Office of the National Security Adviser to be the coordinating body for national cybersecurity, the National Cybersecurity Coordination Centre (NCCC) is entrusted with the responsibility of aligning and harmonising the efforts of all stakeholders towards the delivery of our National Cybersecurity Programme

To deliver the objectives of our National Cybersecurity Programme, we have an Implementation Plan that is our roadmap for driving success, measuring progress and transforming our prescribed strategic actions into reality. The key actions are:

Strengthening Cybersecurity Governance and Coordination

- Establishment of National Cybersecurity Coordination Centre
- Driving Awareness of Cybersecurity Stakeholders' Responsibilities

Fostering Protection of Critical National Information Infrastructure (CNII)

- Comprehensive approach to CNII Protection and Resilience
- Identifying and Coordinating CNII Sectors and Dependencies
- Developing CNII Protection Plan

Enhancing Cybersecurity Incident Management

- Coordination of national cybersecurity incident management
- Establishment of Sectoral CSIRTs
- National Crisis Response Plan

Strengthening Legal and Regulatory Framework

- Review and harmonisation of existing legal framework on cybersecurity (including e-business and online consumer protection).
- Internet Safety and Protection of Children and Gender Rights Online
- Developing the capacity of the judiciary and law enforcement to address cybercrime

Enhancing Cyber Defence Capability

- Administering the activities of the cyber establishments of the armed forces and law enforcement agencies
- Development of a cyber defence plan for Nigeria
- Training of the armed forces to protect the Nigerian cyberspace

Promoting a Thriving Digital Economy

- Promoting the use of the cyberspace to drive Nigeria's digital economy
- Building trust and confidence in a safe and resilient Nigerian cyberspace
- Promoting an indigenous cyber workforce
- Driving a high level of awareness on cybersecurity

Assurance Monitoring and Evaluation

- Deployment of robust and high-quality cybersecurity technology to safeguard our cyberspace
- Strengthening Standards and Good Practices in Public and Private Sectors
- Deployment of Quality Controls and Security Processes

Enhancing International Cooperation

- Alignment of efforts of domestic cybersecurity stakeholders within Nigeria to enhance international engagement
- Strengthening cybersecurity influence on the regional stage
- Providing support for international mechanisms that promote cybersecurity

As the country sets out to implement the strategic measures and unlock national potentials for ensuring progressive use of the nation's cyberspace, all stakeholders have a mandate to make conscious effort to balance the security, social and economic imperatives of cyberspace with the cybersecurity needs of government, industry, academia and the international community.

UNITY AND FAITH, PEACE AND PROGRESS