# APPRAISING THE WORKABILITY OF THE NATIONAL CYBER SECURITY POLICY AND STRATEGY DOCUMENT 2021*

**Abstract**
*There is an on-going rat race between law-making bodies and tech-companies on how to effectively keep the activities of modern technologies and daily advancement in the internet within the ambits of the law. The efforts by legislative draughtsmen to make up to date, watertight laws, which encompasses the ever spreading tentacles of e-commerce, e-business, online identity, and critical issues bothering on technology cannot be over emphasized. With a deluge of policy documents, guidelines and legal frameworks and just recently, the signing by the Nigerian President of the National Cyber-Security policy document 2021, the Nigerian government like every other nation has not rested on its oars in their efforts to ensure that matters bothering on the Nation`s Cyber security are nipped on the bud. The Nigerian government once again, in a pro-active step through this 2021 policy document, takes a look into the future and addresses foreseeable challenges which may overawe the state and proffering either medium or long term solutions to these issues. The aim of this paper is to conduct a holistic review of the 2021 Cyber security policy framework, appraising several efforts of the government from 1999 till date, and critically analysing this policy document with a view to unravelling the progress made so far.*

**Keywords:** National Cyber security Policy, Strategy Document 2021, Workability, Nigeria

## 1. Introduction

The speed at which the advancement in technology changed the narrative with regards to regulatory safeguards in the spheres of Information Communications Technology cannot be overemphasized. Ranging from simple contracts metamorphosing into paperless electronic contracts, and data protection and privacy online not properly governed by the existing legislations calls for great concern. Efforts by the government either through policies, guidelines or legislation to ensure that its cyberspace remains a safe-haven for every form of transaction or activities is what is called the cyber –security architecture of every jurisdiction. Until recently, Nigeria as a country did not have any comprehensive cyber security policy or framework on ground and this got tongues wagging in the ICT world. A different approach needed to be adopted to ensure that matters bothering on securing the cyber space were thoroughly dealt with, hence the Nigeria`s President in conjunction with the Office of the National Security Adviser signing a policy document tagged the Cyber security Framework Policy document 2021.[1] Before delving into analysing this policy document, there may be the need to first trace a recital on the metamorphosis of the nation`s cyber security network, highlighting major strides in the development of our current status as a nation.

## 2. Historical Background of Nigeria's Cyber Security Framework

While it is the responsibility of the government to ensure the security of the lives of its citizens by setting regulatory structures in place to check the excesses of social vices, the advancement of technology has created a leeway for crimes to be perpetrated not only physically but in the cyberspace hence the need for a robust cyber-security framework to tackle security challenges not envisaged by our conventional security systems. The world was shocked at the extent to which the cyber space can be utilized in the perpetration of complex organized crimes when a target who was hospitalized was murdered through hacking into his online daily prescription pad, changing his daily dosage to a lethal drug which was administered unknowingly by the nurse on duty.[2] Up until the early 1990`s, the nation`s cyber-security platform or framework as the case may be was still aloof as not much activity was experienced in the areas of setting regulatory structures or safeguards in place to secure the nation`s cyber space. Whereas nations like Belgium, United Kingdom and the United States as at the time, had well laid out regulatory structures and safeguards in place to ensure a robust crime free cyber space. As at then, all matters bothering on crime in the nation was addressed using either Criminal Procedure Code (CPC)[3] or the Criminal Procedure Act (CPA)[4] as the case maybe.The above mentioned legislations that encompassed the Nigerian Criminal Law System did not pre-empt crime through other avenues like the cyber space. While these laws addressed for instance, the offence of defamation; when it occurs over the internet; these normal conventional laws would either be insufficient or inapplicable, hence the urgent need for specialized legislations that govern matters or transactions online or through the cyberspace.

With the unbundling of the telecommunications sector and the sale and privatization of the nation`s telecommunication`s service NITEL[5], then a free and liberal market became possible hence the proliferation of several ISP (Internet Service Providers) within the market. More entrants into the sector made it possible for increased number of unaccounted or poorly accounted subscribers to have access to the cyber-space, making the nation`s cyber space a vulnerable place for different forms of unscrupulous and obnoxious practices. Offences such as online scams, cyber stalking, cyber bullying, internet phishing, website cloning, email-phishing, credit card fraud and online advance fee fraud were alien to the Nigerian criminal law system, so worldwide, Nigeria became a safe-haven for such above mentioned criminal activities. With a deluge of complaints traced down to Nigeria, there was pressure by the international community mandating countries whose laws are not in consonance with the International best practices to ensure that their domestic laws adopt the model international law.
Based on the some of the above reasons, the nation intensified efforts to ensure that it`s criminal law system was up to date bearing in mind the advancement in technology and the incidental ills associated thereto.

***By Chidiebele EZEAMA, LLM,** Lecturer, Department of Commercial and Property Law, Faculty of Law Nnamdi Azikiwe University, Awka Anambra State, Nigeria; and
***Ejike Francis OKAPHOR, PhD,** Senior Lecturer, Department of Public and Private Law, Faculty of Law, Nnamdi Azikiwe University Awka, Anambra State, Nigeria. E-mail: ef.okaphor@unizik.edu.ng

[1]National Cyber Security Framework Policy and Strategy, February 2021
[2] 'Killer nurse gets 11 life sentences' available at www.cnn.com, Friday 10th March, 2006. Accessed o 1th March 2022, at 12:25pm
[3]Criminal Procedure Code (Amendment Law) 1963
[4]Criminal Procedure Act CAP 48, 1956 L.F. N and Lagos
[5]Ministry of Communications National Policy on Telecommunications 1998.

**3. Regulatory Steps Taken by Nigeria towards Securing its Cyber-Space**

In a bid to secure its Cyber-space, Nigeria has taken some legal and regulatory steps aimed at securing the country's cyber space against attacks, proliferation and other criminal elements, they include:

**Presidential Committee to Investigate the Rising Activities of Fraudsters on the Internet Cyberspace 2003**

Based on the above mentioned pressure for the Nigerian Government to ensure that its laws are compliant with international best practices as regards the regulation on criminal activities online, the Federal government constituted a Committee to investigate into the unscrupulous activities online and their term of reference being: *'*To propose legal and policy measures to tackle online advance fraud and other forms of cyber- crime*'*. From the above term of reference it can be deduced that up until 2003, Nigeria did not have any laid down legal structure to tackle incidents of cyber-crime and other forms of online scam making the country vulnerable and a safe haven to such obnoxious practices online.[6] While the committee was foot-dragging on its mandates, a shooting incident of a Nigerian diplomat in Prague hastened the steps of the Nigerian government in ensuring that a well laid down structure is put in place to legally tackle complaints bothering on the above mentioned strategies devised by these cyber-criminals.

**Nigeria Data Protection Act 2023**[7]

The newly sworn in President of Nigeria, Bola Tinubu on the 14th of June, 2023 signed into law, the Data Protection Act, 2023. The objective of the Act, amongst others, is to safeguard the fundamental rights and freedoms and the interests of data subjects as guaranteed under the 1999 Constitution of the Federal Republic of Nigeria (as amended). The Act established the Nigeria Data Protection Commission (the Commission) and replaced the Nigeria Data Protection Bureau (NDPB) established by former President Buhari. The Act also focuses on crucial aspects such as the processing of personal data, protection of data subjects' rights, the establishment of a Data Protection Commission, data security, cross-border data transfers as well as data breach management.[8] The scope of new Act covers or applies to data controllers or data processors domiciled, ordinarily resident or ordinarily operating in Nigeria or in cases where the processing of personal data occurs within Nigeria. It also applies to data controllers or data processors not domiciled, ordinarily resident or ordinarily operating in Nigeria, in so far as they are processing personal data of data subjects in Nigeria. The Act further mandates data controllers and data processors to implement appropriate technical and organizational measures aimed at ensuring the security, integrity and confidentiality of personal data in its care. It also provides for certain measures that may be implemented towards ensuring data security like pseudonymization and de-identification of personal data, encryption etc.[9]

The Act establishes the Nigeria Data Protection Commission otherwise referred to as 'the Commission'. It is an independent body, a body corporate with perpetual succession and a common seal. The new Act further makes transitional provisions aimed at empowering the Commission to take over all the powers and duties of the existing NDPB.[10] The Commission is tasked with the functions of promoting awareness to data controllers and data processors on their obligations under the Bill and supervising the implementation of the provisions of the Act. The Act went further to set up a Governing Council. The members of the council are all citizens of Nigeria and part-time members except for the National Commissioner. The National Commissioner shall have 10 years of cognate experience and proficiency in law, data protection, cyber security management, information and communication technology, consumer protection, management science or other relevant disciplines at a senior management level.[11]

**Economic and Financial Crimes Commission Act 2004**

The establishment of a more advanced and specialized body to augment the efforts of the conventional police in tackling sophisticated crimes was another bold step by the Nigerian government in checking the increasing rate of cyber-crimes and online scams prevalent in Nigeria as at that time. The EFCC Act[12] whose short title reads thus *'*Enforcement of all financial crimes, laws among other things*'* gave the Act a wide scope of operation inadvertently subsuming the role of the almost obsolete Special Frauds Unit (SFU) of the Nigeria Police Force. The EFCC Act charged the Commission with the mandate of investigating all financial crimes including advance fee fraud, money laundering, counterfeiting, illegal charge/transfer, future market frauds, fraudulent encashment of negotiable instruments, computer credit card frauds, contract scam etc.[13] This is the first legal instrument whose letters charged a government agency to conduct investigations and prosecute criminal activities online. The scope of operation of this Act is within the jurisdiction of Nigeria though some departments of the EFCC in collaboration with the INTERPOL and other international organizations share intelligence and information in effectively combating cyber- crime and terrorism. In 2017, the NFIU an operative arm of the EFCC was struck off the list of countries forming part of the EGMONT group. The EGMONT group is a list of 159 FIU`s (Financial Intelligence Units) of several countries which provides a platform for secure exchange of expertise and financial intelligence to combat Money Laundering and Terrorist Financing.[14] Being blacklisted by the EGMONT group gives a nation a bad image to potential investors as FDI would be minimized due to non-compliance with international best practices as regards anti-money laundering activities. The prior enactment of the EFCC Act in 2004 increased the rating of the nation among the international community as a jurisdiction that recognizes anti money laundering safeguards through existing legislations. Shortly after the coming into effect of the EFCC Act, in 2004, Nigeria was removed from the list of blacklisted nations and was termed an anti-money laundering

[6]2003 Presidential Committee To Investigate The Rising Activities Of Fraudsters On The Internet/Cyberspace

[7] The Act was recently passed into Law by President Bola Tinubu

[8]E. Odunze & B. Agbakoba-Onyejianya, 'Unveiling the Nigeria Data Protection Act, 2023: An Expert Appraisal of Key Provisions' available on https://oal.law/unveiling-the-nigeria-data-protection-act-2023-an-expert-appraisal-of-key-provisions/?utm_source=mondaq&utm_medium=syndication&utm_term=Privacy&utm_content=articleoriginal&utm_campaign=article assessed on 29th June, 2023

[9] *Ibid*

[10] S.64 of the Act

[11] S. 9(4)

[12]The Economic and Financial Crimes Commissions Act 2004

[13] S.6(b) EFCC Act, 2004

[14] This is available on www.egmontgroup.org accessed on 14th June,2023

compliant nation. With the coming into effect of the Cyber-Security Policy Document 2021, a review by this article would be conducted in the later part of this work to appraise the efforts by the Nigerian government through this framework to ensure that such blacklisting would not occur again in the near future. While it is commendable that the government has through several legal instruments achieved a fairly stable cyberspace with decreased nefarious activities which was prevalent pre-enactment of these above mentioned legislations, however with the advancement of ICT on a daily basis, the need for collaborative efforts by sister agencies of government is required in order to achieve a collective gain in securing the nation`s cyber space. Problems like duplicity of functions of government agencies, bureaucratic bottlenecks, lack of inter –agency information and intelligence sharing, and bottlenecks to cross-border collaboration, spurred the government of the day, to come up with a framework with a holistic approach towards ensuring the safety of the Nation`s Cyber-Space.

**National Cyber-Security and Policy Strategy 2021**

This Cyber Security Framework 2021, was a policy document aimed at looking into the future of the nation`s cyberspace and pre-empting challenges which the nation may encounter and seek to plugging existing legislative loopholes governing the cyber-security in the nation. It would be ideal to conduct a review of existing legal framework before this 2021 policy document which on the face of it does not have the force of law, but creates a pathway towards achieving a secure cyber space for the nation. Until 2015, the nation had not taken any drastic measures to safeguard its cyber-space, as existing laws and regulations like the Cyber Security Policy Framework of 2014 or the EFCC Act of 2004 were either not sufficient or mere policy documents without a force of law which took into consideration best practices in protection of the nation`s cyber space. This Six years between the first policy document of 2014 and this current policy framework document of 2021, was aimed at ensuring that the nation`s cyber space was formidable against cyber-attacks, threats and any action which may overawe the state as conventional security daily undergoes metamorphosis making the cyber-space a vulnerable and an important sphere which requires adequate security, hence the need for the review, overtime, of the 2014 policy document. Six years down the line, after the review of the 2014 policy document, the 2021 Cyber Security Policy Framework document was birthed, which again takes into consideration the advancement of ICT from 2014 till aimed at ensuring that policies, frameworks and regulations which came about as a result of the 2014 policy document are updated and in tune with rapid growth and advancement in the ICT sector. This study will be focusing on some pillars including but not limited to Pillar 4 in the schedule of the 2021 policy document bothering on the proposed action plan in the strengthening of the nation`s legal and security framework in the following areas:

**Cyber-Crime (Prohibition, Prevention, Etc) Act 2015**

The Act provides an effective, unified and comprehensive legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria. The Act also ensures the protection of critical national information infrastructure and at the same time promotes cyber security and the protection of computer systems and networks, electronic communications data as well as computer programs, intellectual property and privacy rights. The coming into force of the 2015 Cyber-Crimes Prohibition and Prevention Act, was a milestone in the nation`s efforts to ensure that its cyber-space was safeguarded with modern laws and regulations capable of preventing to the barest minimum, the proliferation of online criminal activities that came about as a result of government`s privatization/opening up of its telecommunication sector[15]. Unfettered access and the reduction in price of acquiring a phone line brought about increased subscriber activities online making the nation`s cyber space, which as the time was poorly regulated a safe haven for some nefarious activities online[16]. Worthy of note are the barrage of criticisms that followed the enactment of this Act which this paper will highlight. The Act in a bid to check the activities of cyber-cafes in Nigeria mandated through its S. 7[17] the compulsory registration of all operators of cyber-cafes in Nigeria with CPRC (Computer Professionals Registration Council) and the Corporate Affairs Commission (CAC), in a bid to ensuring the maintenance of a register, readily available to law enforcement agents. This is a commendable effort by the government but placing the burden of proof on the prosecutor, in its S.7 (4), when proving connivance between a person who perpetrates online fraud and a café owner according to Awhefeada and Ohwomeregwa, [18]is an onerous task which may vitiate the aim of the smooth workings of the Act. S.7 among other provisions of this Cybercrime Prohibition and Prevention Act,hence the immediate proposal for amendment to ensure the effective workability of the Act.

A commendable step by the government of the day in the 2021 Cyber-Security Policy document factored in these loopholes in the 2015 Cyber Crime Prohibition Act and proposed an amendment of the Act. Steps such as constituting a multi-stakeholder Committee to review the 2015 Act, and to develop a draft amendment bill to cover areas where the 2015 Act did not meet the required force of law were put in place. Agencies such as the Corporate Affairs Commission, the Office of the National Security Adviser, National Cyber-Security and Co-Ordination Centre, the Federal Ministry of Justice and the National Assembly were to form part of the multi-stakeholder Committee to review the 2015 Cyber-Crime Prohibition Act.[19]

It is also common knowledge that a great percentage of our police prosecutors are poorly trained on matters bothering on ICT and the workings of the cyber-space, making the effective implementation of the Cyber-Crime Prohibition Act 2015 an illusion. For instance S.7 (4) of the Act places on the prosecutor, the burden of proving connivance. To discharge such burden, the necessary training and the adequate legal tools and techniques must be readily available, hence the proposed Capacity Building for Law Enforcement Officers and the Judiciary in the 2021 Cyber-Security Policy Framework. To effectively achieve the effective workings of our cyber-security laws, there is need to strengthen the already existing cyber-security capacity for judicial officers, legal practitioners and law enforcement agents. Technical expertise, training, human resources tools, multi-stakeholder engagement and funding for capacity development are all the necessary strategies which the 2021 cyber-security

[15]I. Frank, and E. Odunayo, *'*Approach to Cyber-Security Issues in Nigeria: Challenges and Solutions*' International Journal of Cognitive Research in Science, Engineering and Education.* Vol 1. No.1, 2013 pg.1

[16]Ibid

[17] S.7 Cyber Crime Prohibition and Prevention Act, 2015

[18] U.V Awhefeada and O.B Ohwomeregwa, *'*Appraising the Laws Governing the Control of Cybercrime in Nigeria*'*: *Journal of Criminal Law and Justice* , Volume 8, No. 1 , pp 30-49, June 2020.

[19]Cybercrime (Prohibition and Prevention, Etc) Act, 2015

Policy Framework projects to achieve. It projects to train a minimum of 50 judges, 200 lawyers and 500 prosecutors per-annum on the above mentioned areas.[20]

**4. Enactment of a National Data Protection Law (Act) to Substitute the NDPR Regulations 2019**

The NDPR 2019[21] still remains the most comprehensive data protection policy document which takes a holistic approach in matters bothering on protection of consumers on the nation`s cyber-space. A review of the 2019 NDPR reveals that online data protection and privacy remains paramount in ensuring the security of persons online and this regulation mandates organizations to ensure that privileged information within the database of every organization complies with the laid down guidelines as enshrined in this 2019 NDPR regulation. While the NDPR incorporated the provisions of the General Data Protection Regulation (GDPR) into its mandates, there are however, some slight differences between both regulations as countries are encouraged to model their laws and guidelines after the GDPR which is a model law. One of the major shortcomings of this regulation is on the definition or the meaning of *'*Database*'* under the regulation, which several proponents finds limiting with a major loophole. The NDPR while defining *'*Database*'* failed to give data in its broad meaning aimed at preventing smart Data Protection Controllers from hiding under the guise of the draughtsman`s deficiency in perpetrating online fraud. Whereas both the Black Laws Dictionary and the GDPR in their definition of the meaning of *'*Database*'* used the word *'*information*'* to depict data either in its raw or organized form, the NDPR simply defined *'*database*'* to mean a collection of data organized in a manner that allows access, retrieval, deletion and processing of that data…. *'*[22]

Another area where the NDPR regulations has been criticized by scholars is in the area of penalties for non-compliance and whether a regulation can be conferred the same force of law with an Act of the National Assembly. Though a subsidiary legislation, deriving its authority from the NITDA Act, can the NDPR regulations be said to have the same force of law with its enabling Act? This is an administrative Law issue but it has since been settled in the Supreme Court`s decision in NNPC *v* Famfa Oil,[23]which held that the provisions of a subsidiary legislation cannot override the provisions of a substantive Act of the National Assembly, hence the clamour for the quick passage of a Data Protection Act rather than a Data Protection Regulation which derives its authority from the NITDA Act. Commendably, the 2021 Cyber-security Policy Framework document factors this clamour for the enactment of a Data Protection Act into their projections. In Chapter 6.2 of its schedule under the 4th pillar bothering on Strengthening Legal and Regulatory Framework, a proposed National Data Protection Legislative Framework was amongst the strategies adopted to ensure a robust cyber security network in Nigeria. To achieve this, the policy document projects to harmonize all existing legal frameworks on data protection through a multi-sectorial approach, comprising of Office of the National Security Adviser, National Cyber-Security Co-ordination Centre, Federal Ministry of Communications and Digital Economy, Federal Ministry of Information Technology and Innovation, and Federal Competition and Consumer Protection Commission.

**Establishment of Special Courts to Handle Cyber-Crime Matters and Training of Judicial Officers of the Specialized Courts**

The Federal High Court established under S. 251 of the 1999 Constitution of the Federal Republic of Nigeria (CFRN) as amended was formerly the Federal Revenue Court of Nigeria empowered by the Constitution to handle all matters bothering on the revenue of the Federal Government. However being a court of limited jurisdiction, and it`s scope of jurisdiction is listed in the said S. 251 of the CFRN, matters outside its scope or mandate would not be entertained by it. A proposed creation of a special court in the Federal High Court to handle matters bothering on ICT related matters was another projection by the 2021 Cyber-Security Policy Framework Document. The intricacies of ICT related matters requires specialized legal officers in that aspect who are capable of implementing legislations and giving true meaning to the legislative draughtsman's intent. Since the advent of the Cyber Crime Prohibition and Prevention Act 2015, there has been an increase of lawsuits bothering on related matters the legal framework still grapples with the challenges of giving the Act its true interpretation.

For instance S. 19(3) of the Cyber Crime Prohibition, Prevention Act 2015, mandates Financial institutions as a duty to their customers, to put in place, counter-fraud measures to safeguard their sensitive information, however, where a security breach occurs, the proof of negligence lies on the customer to prove the financial institution could have done more to safeguard its information integrity. This section in my opinion is lopsided, and places an organizational burden on a mere customer or client of a bank with little or no access to information to discharge the burden of proof placed on him by the Act. A retinue of decided cases[24] has it as proof that once the burden of proof shifts to the customer, discharging such evidential burden becomes almost impossible and their complaints of fraudulent withdrawals from their accounts are thrown out by the courts.[25]To tackle the above, the 2021 Cyber-Security Policy Framework document proposes the establishment of specialized courts under the arm of the Federal High Court with adequate skillset and expertise to handle matters bothering on ICT related matters. To achieve this, the policy document proposes the deployment of human resources and expertise for the establishment of a specialized court or judicial division for cyber-crime related cases in the Federal High Court. The 2021 Cyber- Security Policy Framework Document amongst other aspects was intentionally pre-emptive in the areas of Digital forensics, Development of a National Cyber Defence Plan, Cyber Insurance and Cyber awareness. All these factors are where our cyber security framework may be lagging behind and it is commendable that the 2021 policy framework in its foresight factors into consideration, some of these challenges and proffer implementable solutions with timelines.

**5. Conclusion**

As earlier stated, the aim of the paper is to conduct an appraisal of the cyber-security architecture of Nigeria and determine to what extent Nigeria's legislations on the subject matter provide adequate protection of the nation`s Cyber space and secondly,

[20]Schedule to the Cyber Security Policy Document on the Judiciary.
[21] NITDA, Nigeria Data Protection Regulation 2019
[22]Meaning of *'*Data*'* In the definition part of the NITDA Act
[23] (2012) 17 NWLR pt. 148
[24]*Victor Eje Uba v UBA Plc*. Suit Number MHC/323/2010
[25] *Victor Eje supra*

if indeed there is needed effort to ensure the beefing up of the cyber security architecture. The 2021 Cyber Security Policy Framework Document cannot be said to have the force of law, since it proposed to amend the NITDA Act of 2015, which was the only primary existing legislation that govern activities over the internet in Nigeria. The implementation of the key performance indexes of the 2021 policy document becomes somewhat an illusion. With the rapid growth and advancement in ICT, there is need for speedy implementation of the KPI`s in the schedule of the 2021 policy document. For instance when the decision of *Victor Eje v UBA Plc*. was given, the card technology prevalent and commonly used by most banks as at then was the chip and pin technology card type with more susceptibility to fraud as against the current technology of magnetic stripe cards being used today. There is need for these KPI`s to be speedily implemented so that our laws are in tune with technology. With the passing into law of the Nigeria Data Protection Act 2023, it is seen as welcome development not minding the several flaws or uncertainty against the new Act. And a careful reading of the new Act and from all indications, there is indeed no specific provision in the Act that mentioned the repeal of the NDPR. Thus, on a careful reading of the transitional provisions in Section 64 of the new Act which mandates all orders and regulations made or issued by NITDA and the NDPB to continue to be in force until they expire or they are repealed. One therefore can assume that the NDPR is not repealed by the Act, thus both Act and, the NITDA guidelines of 2019, can co-exist to secure the cyber space of Nigeria and further strengthen the existing cyber security architecture.