LEGALITY OR OTHERWISE FOR THE IMPOSITION OF CYBER SECURITY LEVY IN NIGERIA*,**

Abstract

The growing threats of cyber-attacks has undoubtedly, prompted the need for improved security measures to combat these issues and mitigate the resultant consequences. Thus, the cyber security levy is aimed at providing dedicated and adequate funding for the actualization of cyber security initiatives in Nigeria. However, the implementation of cybersecurity levy in Nigeria has generated unimagined public resistance. This study therefore sought to examine the Legality or otherwise of the imposition of cybersecurity levy in Nigeria. The specific objective of this research was to establish the legal basis, if any, that justifies the imposition of cybersecurity levy in Nigeria and to make salient recommendations on how to effectively surmount the challenges and concerns relating to the imposition of the levy. The research design and methodology was doctrinal approach, using analytical and descriptive research methodology. The main sources of data collection were various legal documents and materials, both from the library and the internet, and covering both the primary sources and the secondary sources, including decided cases. In this work, it was discovered among others that cybersecurity levy is the 0.5% (0.005) levy imposed on all electronic transactions by applicable businesses as provided under the Cybercrime (Prohibition, Prevention, etc) Act (as amended) 2024. It is further observed that the financial support realised through this levy will help in developing and implementing strategies to safeguard Nigeria's digital infrastructure and combat cybercrimes effectively. In the end, it was recommended among other things that a clearer provision on the implementation of the cybersecurity levy be made by the Act in order to provide a uniform implementation guideline for the levy.

Keywords: Cybercrime, Cybersecurity levy, Imposition, Nigeria

1. Introduction

The innovation of the Information and Communication Technology (ICT) which has produced the Internet to connect the whole world as a global village has been a vital aspect of our daily lives. Business organizations, Industries, government, non-profit organizations as well as individuals are now using the Internet with computer network for various activities. However, the advent and reliance on the internet as an integral part of our daily living has brought its unintended consequences which involves criminal activities, including; spamming, credit card fraud, ATM fraud, phishing, identity theft and a blossoming haven for cybercriminal miscreants to perpetrate their insidious acts.[1]

In Nigeria, the phenomenon of cyber-crime dates back to the year 2001 when Nigeria came into realization of the full potentials of the internet. Since then, the country has acquired a world-wide notoriety in criminal activities, especially financial scams, facilitated through the use of the Internet.[2] Statistical analysis from around 2013 positions Nigeria as the 43rd among EMEA (Europe, Middle East and Africa) and according to the report by the Internet Crime Complaint Centre (ICCC), Nigeria ranks third among sources of global cybercrime, trailing only the United States and the UK.[3] A report by the

* **NWABACHILI, Chioma O., PhD,** Department of Intternational Law, Faculty of Law, Nnamdi Azikiwe Univversity, Awka, Anambra State. Email: co.nwabachili@unizik.edu.ng

** **NNOYELU, Chinemelu V.,** Faculty of Law, Nnamdi Azikiwe University, Awka, Anambra State. Email:

[1] YA Makeri, "Cybersecurity issues in Nigeria and Challenges" [2017] (7) (4) *International Journal of Advanced Research in Computer Science and Software Engineering,* 315 <https://www.researchgate.net/publication/318668652_Cyber_Security_Issues_in_Nigeria_and_Challenges > accessed 22 July, 2024

[2] *ibid*

[3] JT Jack and R Ene, 'Cybercrime and The Challenges of Socio-economic Development in Nigeria' [2016] (14)(2) *Jorind,* 42-49

IC3 under the Federal Bureau of Investigation (FBI) in 2020 ranked Nigeria as the 16th among countries grappling with significant cybercrime issues.

Nigerian cyber criminals are daily devising new ways of perpetrating this form of crime and the existing methods of tracking these criminals, if any, are no longer suitable for to deal with their new tricks. The victims as well show increasing naivety and gullibility at the prospects incited by these fraudsters.[4] Therefore, building and maintaining a stronger cybersecurity network for Nigeria becomes very imperative. As a corrective measure, the then President of Nigeria, Olusegun Obasanjo set up National Cyber security Initiative (NCI) in 2003. The Nigerian Cybercrime Working Group (NCWG) is to meet the objectives of NCI; however, their effectiveness did not match up to the rate of growth of cybercrime.[5] Cyber-crime is complex and committed mostly from remote locations making it difficult to police. The absence of enabling law makes policing even more difficult.[6]

In 2014, the Federal Government of Nigeria issued the National Cybersecurity Policy and Strategy[7] encapsulating cohesive measures aimed at addressing cyber threats and attacks effectively. Furthermore, in 2015, the National Assembly enacted the Cybercrime (Prohibition and Prevention) Act, 2015, which was signed into law by the then President Goodluck Ebeleckukwu Jonathan. The objectives of the Act includes; (i) to provide an effective and unified legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria; (ii) protect critical national information infrastructure, and promote cybersecurity and cyber safety; and (iii) to promote cybersecurity and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights.[8] The Act at section 44[9] established the National Cybersecurity Fund and clearly provides that into the fund shall be paid a levy of 0.005 of all electronic transactions of businesses specified in the second schedule to the Act which are: GSM service providers and all telecommunication companies, Internet service providers, Banks and other financial institutions and Nigerian stock exchange.

However, since 2015, the provisions of this Act were never enforced due to ambiguity in certain provisions especially with respect to the amount payable as the cybersecurity levy. Thus in 2024, the law was amended and among other things the amount payable as cybersecurity levy was clearly stated to be 0.5 percent on all electronic transactions of businesses specified above.[10] Consequently, The Central Bank of Nigeria (CBN) on 6th may, 2024, issued an implementation guideline to all commercial, merchant, non-interest and payment service banks, other financial institutions, mobile money operators and payment service providers mandating the collection and remittance of the national cybersecurity levy.[11] However, the implementation of the cybersecurity levy has generated a lot of controversies among stakeholders, writers and jurists regarding the Legality of the levy. The levy was in fact termed; "government strategy to milking a dying cow."[12] It is against this background that this work seeks to assess the Legality or otherwise of the imposition of cybersecurity levy in Nigeria. The

[4] *ibid*
[5] YA Makeri (n.1)
[6] *ibid*
[7] National Cybersecurity Policy and Strategy, 2014
[8] Cybercrime (Prohibition and Prevention) Act 2015, s 1
[9] Cybercrime (Prohibition and Prevention) Act 2024 (as amended), s 44
[10] *ibid*, s 44(2)(a)
[11] W Ajayi, 'Central Bank issues Guidance on the Collection and Remittance of the National Cybersecurity Levy' KPMG (Nigeria, May 2024) <https://kpmg.com/ng/en/home/insights/2024/05/central-bank-issues-guidance-on-the-collection-and-remittance-of-the-national-cybersecurity-levy-by-financial-institutions.html> accessed 22 July 2024
[12] MS Shelleng,'Cybersecurity levy: Milking a dying cow' Daily Trust (Lagos,13 May 2024) <https://dailytrust.com/cybersecurity-levy-milking-a-dying-cow/> accessed 22 July 2024.

work examines the legal framework as well as the justification, if any, for the imposition of cybersecurity levy in Nigeria.

2. Conceptual Framework

The Conceptual Framework of this study seeks to outline the meanings and definitions of major terms of the research topic. It provides a roadmap for understanding the key components and considerations relating to cybersecurity levy in Nigeria. These major terms will hereby be conceptualized and defined seriatim;

2.1 Tax

The Black's Law Dictionary has defined tax as a charge usually monetary, imposed by the government on persons, entities, transactions or properties to yield public revenue.[13] Tax, according to M.N. Umenweke,[14] is a compulsory contribution towards a country's expenses raised by the government from peoples' salaries, properties, and from the sale of goods and services. Tax is a compulsory financial charge or some other type of levy imposed on a taxpayer by a government with a view to generating revenue to fund government expenditure. The word tax was further judicially defined in the Australian case of *Mathews v Chicory Marketing Board*[15] as 'a compulsory exaction of money by a public authority for public purpose or raising money for the purpose of government by means of contributions from individual persons.

2.2. Levy

The Black's Law Dictionary defines levy as; "to impose or collect (a tax, fine, or other payment) by authority of law, to seize or attach (property) by legal process, especially to satisfy a debt or judgment".[16] A statutory definition of levy is found under the Tax and Levies (Approved List for Collection) Act,[17] to include any fee and charge. Therefore, levies as forms of taxation are imposed to enable the government provide for or achieve a very specific purpose which might be education, cybersecurity, Agriculture etc.

2.3 Tax Imposition

Tax imposition refers to the act of a government or taxing authority requiring citizens and businesses to pay a mandatory financial obligation. This process is essential for generating revenue to fund public services, infrastructure, and various government functions. The primary purposes of tax imposition include:

- Revenue Generation: Taxes are a primary source of income for governments, enabling them to finance public goods and services such as education, healthcare, and infrastructure development.[18]
- Economic Regulation: Taxation can influence economic behavior by encouraging or discouraging certain activities. For instance, higher taxes on harmful goods can reduce their consumption, while tax incentives can promote investment in specific sectors.

[13] Garner BA, 'Black's Law Dictionary, 9th Edn. (New York, St Paul Min; West Publishing Co.)
[14] MN Umenweke, *Tax Laws and its Implications for Foreign Investments in Nigeria,* (Enugu: Nolix, Educational 2005) p.5.
[15] [1938] 60 CLR 263*; Newcomer v Coulson* [1877] 5 Ch D 133 At 142, 143, *Fearn v Tate Gallery* [2023] Uksc 4at 5, Para 9; *Onagoruwa v State* [1993] 7 NWLR (Pt 303) 49 At 100 Para D-E.
[16] BA Garner, 'Black's Law Dictionary, 9th Edition' [2009] 1594 *St. Paul Minnesota: West Publishing Co*.
[17] Tax and Levies (Approved List for Collection) Act, Cap T2, Laws of the Federation of Nigeria 2004, s 4
[18] O Aguolu, *Taxation and Tax Management in Nigeria* (3rd edn, Enugu: Meridian Associates, 2004)

- Fiscal Policy Tool: Governments use taxation as a tool to manage economic stability. For example, increasing taxes during inflation can help control excess purchasing power, while reducing taxes during economic downturns can stimulate growth.[19]

2.4 Cybercrime

The term "cybercrime" can be used to describe any criminal activity which involves the computer or the internet network.[20] Cybercrime encompasses a range of activities that exploit computers and the internet for fraudulent purposes. These activities span from identity theft to money laundering, targeting victims via diverse strategies.[21] A more comprehensive perspective classifies cybercrime as crimes committed on the internet or through computers, involving either the use of the computer as a tool or the computer's owner as a target. This classification encapsulates a wide array of offenses, including fraud, forgery, identity theft, phishing, spam, and more; thereby highlighting the intertwining of technology and victims in all cybercrimes.[22]

2.5 Cybercrimes in Nigeria

Cybercrime incidences in Nigeria grow explosively as the internet continues to penetrate every sector of our society and no one can predict its future. Dangerously, the crime usually requires a hectic task to trace. Unemployment and quest for wealth amongst others has been identified as the main causes of cybercrime in Nigeria.[23] According to Check-Point, a global network cybersecurity vendor, as at July 2024, Nigeria is ranked 19th highest country in cyber-attacks out of 112 countries.[24] The country faces a multitude of cybercrime challenges, including computer-related and internet-related fraud, hacking, identity theft, credit card fraud, DDoS attacks, ransomware, phishing, child sexual exploitation, malware attacks, and more.[25] These offenses exploit technology to compromise victims' personal and financial information, disrupt services, and spread malware.

2.6 Cybersecurity

Cybersecurity encompasses measures and practices aimed at safeguarding computer systems, networks, and data from unauthorized access, disruption, and destruction.[26] It ensures confidentiality, integrity, and availability of digital information. Continuous vigilance and adaptation to evolving threats are crucial in maintaining effective cybersecurity.[27] According to Kaspersky, cybersecurity is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It is also known as information technology security or electronic information security.[28]

---

[19] *ibid*

[20] FB Okeshola and AK Adeta A.K, 'The Nature, Causes and Consequences of Cyber-Crime in Tertiary Institutions in Zaria-Kaduna State' (2013) 3(9) *Nigeria American International Journal of Contemporary Research,* 98-114.

[21] D Halder and K Jaishankar, 'Cyber Gender Harassment and Secondary Victimization: A Comparative Analysis of the United States, the UK, and India, Victims & Offenders, (2011) 6:4 *Manonmaniam Sundaranar University [Debarati Halder],* 386-398

[22] *ibid*

[23] *ibid*

[24] A Adepetun 'Nigeria Ranks 19th in Global Cyber Attack Index' *The Guardian* (Lagos, 21 August 2024) <https://guardian.ng/technology/tech/nigeria-ranks-19th-in-global-cyber-attack-index/#:~:text=Nigeria%20has%20been%20ranked%2019th,Threat%20Index%20for%20July%202024> accessed 21 August 2024

[25] BA Omodunbi et al, 'Cybercrimes in Nigeria: Analysis, Detection and Prevention' (2016) 1(1) *FUOYE Journal of Engineering and Technology,* 37-42.

[26] ME Whitman and HJ Mattord, *Principles of Information Security* (5th edn, Boston MA: Ceenage Learning 2018) p 1-2

[27] AM Auwal, 'Cybercrime and Cyber Security in Nigeria: Overview and Rate' (2023) *Research Square Platform LLC,* <https://doi.org/10.21203/rs.3.rs-3307532/v1>accessed 8 August 2024

[28] AO Kaspersky Lab, 'What is Cybersecurity? Types, Threats and Cyber Safety Tips' *Kaspersky* (2024) <https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security> accessed 8 August 2024

2.7 Cybersecurity Levy

Cybersecurity Levy refers to a tax or fee imposed on organizations to fund cybersecurity initiatives, such as; national cybersecurity programs, cybercrime prevention and investigation, cybersecurity research and development, information sharing and threat intelligence, Incident response and disaster recovery. Cybersecurity Levies can be implemented in various ways, such as, direct tax on organizations, fee on specific industries, surcharge on online transactions, etc. In Nigeria, cybersecurity levy is the o.5% levy imposed under section 44(2) (a) of Cybercrime (Prohibition and Prevention) Act[29] on all electronic transactions by the businesses specified in the second schedule to the Act, which are; GSM Service providers and all telecommunication companies; Internet Service Providers; Banks and other Financial Institutions; Insurance Companies; and Nigerian Stock Exchange. The imposition of the cybersecurity is informed by the urgent need to address the poor funding and the disruptive impact of current and emerging existential cyber threats against national security and critical economic infrastructures.[30]

3. Brief Analysis of the key laws under Discourse

3.1. Overview of the Cybercrime (Prohibition, Prevention, etc.) Act (as amended) 2024[31]

The specific objective of the Act is to provide an effective, unified and comprehensive legal and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria. It also ensures the protection of critical national information infrastructure, and promotion of cybersecurity and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights.[32] The Act in order to achieve its objectives established the office of the National Security Adviser under section 41[33], as well as the Cybercrime Advisory Council (the Council) under section 42.[34]

Most notably under the Act is the establishment of the National Cybersecurity Fund (referred also to as the "Fund") under Section 44 of the Act.[35] According to the Act, there shall be paid and credited into the Fund and domiciled in the Central Bank of Nigeria, a levy of 0.005 of all electronic transactions by the businesses specified in the second schedule to this Act. Under the Second Schedule to the Act[36], the specified businesses are: (a) GSM Service providers and all telecommunication companies; (b) Internet Service Providers; (c) Banks and other Financial Institutions; (d) Insurance Companies; and (e) Nigeria Stock Exchange. The Act further provides other sources of funds for actualizing its objectives including; grants-in-aid and assistance from donor, bilateral and multilateral agencies; all other sums accruing to the Fund by way of gifts, endowments, bequest or other voluntary contributions by persons and organizations, and states clearly that all monies accruing to the Fund shall be exempted from income tax and all contributions to the Fund shall be tax deductible.[37]

Furthermore, the Act provides that the levy imposed under subsection 2(a)[38] shall be remitted directly by the affected businesses or organizations into the Fund domiciled in the Central Bank within a period

[29] Cybercrime (Prohibition and Prevention) Act 2007, s 44(2)(a)
[30] SB Umar, 'Cybersecurity levy, national security and economic growth' *The Cable* [Lagos, May 10, 2024] <https://www.thecable.ng/cybersecurity-levy-national-security-and-economic-growth/amp/> Accessed 2nd August, 2024
[31] The Cybercrime (Prohibition, Prevention, etc.) Act (as amended) 2024
[32] The Cybercrime (Prohibition, Prevention, etc.) Act (as amended) 2024, s 1
[33] *ibid,* s 41
[34] *ibid,* s 42
[35] The Cybercrime (Prohibition, Prevention, etc.) Act (as amended) 2024, s 44
[36] *ibid,* second schedule
[37] *ibid,* s 44(3)
[38] *ibid*, s 44(2)(a)

of 30 days. By subsection (5)[39] an amount not exceeding 40 percent of the Fund may be allocated for programs relating to countering violent extremism. Under subsection (6),[40] the Office of the National Security Adviser is mandated to keep proper records of the accounts; and the account of the Fund shall be audited in accordance with guidelines provided by the Auditor General of the Federation. On the 14th of February 2024, the Cybercrime (Prohibition, Prevention, etc.) Amendment bill was assented into Law. The amendment of the 2015 Principal Act,[41] was a response to the urgent need to address the issue of ambiguity and insufficiency inherent in the Principal Act which has culminated into its unenforceability and lack of implementation since 2015.

Key changes made by the amendment Act which are relevant to this study include: the new amendment to section 44 (2)(a) to provide that; A levy of 0.5% (0.005) equivalent to a half percent of all electronic transactions value by the businesses specified in the Second Schedule to the Act shall be paid and credited into the National Cybersecurity Fund (NCF)[42]. By this section thus, the amount payable as the cybersecurity levy is clearly defined for ease of determination. Also, the new subsection (6)[43] extends the powers of National Security Adviser by conferring on ONSA, the administration, proper record keeping of the accounts and ensuring compliance monitoring mechanism for the NCF.

Furthermore, a new subsection (8)[44] is introduced by the amendment and it provides that any business specified in the Second Schedule to the Act that fails to remit the levy under section 44 (2)(a) commits an offence and is liable on conviction to a fine of not less than 2% of the annual turnover of the defaulting business and failure to comply shall lead to closure or withdrawal of the business operational licence.

3.2. Overview of Cybersecurity Levy

The emergence of cyberspace, a virtual global domain, is increasingly impacting almost every aspect of our lives. The domain is transforming Nigerian's economy and security posture more than ever before, creating opportunities for innovations and the means to improve general welfare of the citizens.[45] However, behind this increasing dependence on cyberspace lies new risks that threaten the national economy and security. Sensitive data, networks and systems can be compromised or impaired, in a fashion that detection or defence can be hard, thus undermining confidence in a connected economy.[46] The Federal government in response, has put in place, cohesive measures aimed at addressing national risks effectively. These measures are encapsulated in the National Cybersecurity Policy issued in December 2014. By 2015, the President of the Federation signed into law, the Cybercrime (Prohibition and Prevention) Act, 2015. The Act among other things established the National Cybersecurity Fund (NCF) into which shall be paid and credited, a cybersecurity levy of 0.5% (0.005) of all electronic transactions value of businesses specified in the second schedule to the Act[47]. According to the Second Schedule to the Act, the specified businesses are: (a) GSM Service providers and all telecommunication companies; (b) Internet Service Providers; (c) Banks and other Financial Institutions; (d) Insurance

[39] *ibid,* s 44(5)
[40] *ibid*, s 44(6)
[41] The Cybercrime (Prohibition, Prevention, etc.) Act 2015
[42] Cybercrime Act, 2024 (as amended), s 44(2)(a)
[43] *Ibid,* s 44(6)
[44] The Cybercrime (Prohibition, Prevention, etc.) Act (as amended) 2024, s 44(8)
[45] MS Dasuki, 'Forward', *National Cybersecurity Policy and Strategy* (PDF, 2014) p 1-2
[46] *ibid*
[47] Cybercrimes (Prohibition and Prevention) Act 2015, s 44 (1) and (2)(a)

Companies; and (e) Nigeria Stock Exchange[48]. Furthermore, all monies accruing to the Fund shall be exempted from income tax and all contributions to the Fund shall be tax deductible.[49]

3.3. Enforcement of Cybersecurity Levy in Nigeria

It is trite that since the enactment of Cybercrime (Prohibition and Prevention) Act in 2015, and imposition of the cybersecurity levy under the Act, the cybersecurity levy has never been enforced. The reason for non-implementation of the cybersecurity levy stems from the fact that certain provisions in the Act, especially the amount payable as the levy, (0.005), the body to administer the levy, etc were vague and ambiguous.

This led to the amendment of the Act in 2024 and the outcome of the amendment were; the specification of the amount payable as cybersecurity levy to be 0.5% (0.005) equivalent to a half percent of all electronic transactions value by the businesses specified in the Second Schedule to the Act,[50] empowering the office of the National Security Adviser to administer the levy[51], imposition of penalty for failure to pay the levy[52], etc. In an attempt to ensure the implementation of the Cybersecurity levy, the Central Bank of Nigeria, on the 6th of May 2024, published and issued a circular, providing "Implementation Guidance on the Collection and Remittance of the National Cybersecurity Levy" (the "CBN Circular"). Unfortunately, this guideline generated a lot of controversies, heated debates and unimagined resistance from stakeholders, legal practitioners, investors and even lawmakers. The many arguments raised issues like; the constitutionality or otherwise of the imposed cybersecurity levy, the justification for the imposition of the levy in the light of Nigerian Economic Crisis as at the time the implementation is sought, the implication of the levy on investment in Nigeria, the actual person to bear the burden of the levy (whether businesses themselves or their customers), and the constitutional basis for the empowerment of the office of the National Security Adviser to administer the levy. The levy was criticized for being a way of milking a dying cow[53]. Others argued that no nation can tax itself to prosperity[54] and the imposition of the levy is attempt to do the impossible[55].

All these issues led to the suspension of the implementation guideline by Mr. President, His Excellency, Bola Ahmed Tinubu for adequate consultation with and review by stakeholders. Since after the suspension, and up till the time of this research, no further guideline has been issued on the enforcement of the cybersecurity levy, hence the levy has been mere letters in the statute without any lifeline.

4. Legality or Otherwise for the Imposition of Cybersecurity Levy in Nigeria

4.1 Legal Basis for the Imposition of Cybersecurity Levy

In a bid to make a dovetail analysis and assessment on the legality or otherwise of the imposition of cybersecurity levy in Nigeria, this researcher has raised certain salient issues which if properly addressed will help in ascertaining the legal foundation and justification for the imposition of cybersecurity levy. These issues are:

---

[48] Cybercrimes (Prohibition and Prevention) Act 2015, Second Schedule

[49] *ibid,* s 44(3)

[50] Cybercrimes (Prohibition and Prevention) Act 2024 (as amended), s 44(2)(a)

[51] *ibid,* s 44(6)

[52] *ibid,* s 44(8)

[53] MS Shelleng, 'Cybersecurity levy: Milking a dying cow' *Daily Trust* (Lagos,13 May 2024) <https://dailytrust.com/cybersecurity-levy-milking-a-dying-cow/> accessed 8 September, 2024.

[54] A Olayiwola, 'This is extortion: Nigerians lament CBN's new cybersecurity levy' *Punch* (Lagos, 7 May 2024) < https://punchng.com/this-is-extortion-netizens-lament-cbns-new-cybersecurity-levy/ > accessed 8 September, 2024.

[55] A Adegboyega, 'Nigerians react to new 0.5% cybersecurity levy' *Premium Times* (Lagos, 6 May 2024) < https://www.premiumtimesng.com/news/more-news/692212-nigerians-react-to-new-0-5-cybersecurity-levy.html > accessed 8 September, 2024.

1. Constitutionality or otherwise of the Cybersecurity Levy in relation to Section 162 of the Constitution.[56]
2. The legal Implications of the empowerment of the Office of the National Security Adviser (ONSA) with the administration of the Cybersecurity Levy.
3. The exact intent of the Act, with respect to the issue of who bears the burden of the Cybersecurity Levy and whether the Cybersecurity levy amounts to double taxation.
4. The derivative source of the power of the CBN to prescribe guidelines for the implementation of the cybersecurity levy and its implications.

4.2 Constitutionality or Otherwise of the Cybersecurity Levy in Relation to Section 162 of the Constitution.

The principal issue for determination here is whether or not the Federal Government of Nigeria can maintain any other account other than the Federation Account for the purposes of receiving revenue collected by it. Section 162 (1) of the Constitution[57] provides that the Federation shall maintain a special account to be called "the Federation Account" into which shall be paid all revenues collected by the Government of the Federation, except the proceeds from the personal income tax of the following;

- personnel of the armed forces of the Federation,
- the Nigeria Police Force,
- the Ministry or department of government charged with responsibility for Foreign Affairs, and
- the residents of the Federal Capital Territory, Abuja.

The principle of law is trite that in the interpretation of tax statute, where the words are clear and unambiguous, the court shall give effect to their literal meaning[58]. This rule was further given special force in the case of *Partington v Attorney-General.*[59] In relation to section 162[60] above, the question that needs an answer is whether or not the use of the word "shall" makes it mandatory that every revenue must be paid into the federation account, unless such revenue falls within the exceptions therein. In the case of *Amata v Omofuma*[61] the court established that the word "shall" in its ordinary sense is a word of command and one which has always or which must be given a compulsory meaning. It denotes an obligation...Thus, if a statute provides that a thing "shall" be done, the natural and proper meaning is that a peremptory mandate is enjoined.

However, in *Maiwada v F.B.N. Plc*[62] the court held that although, the word "shall" implies a mandatory obligation, it is sometimes construed as merely permissive or directory in cases where it's so being construed as mandatory will bestow no right or benefit on anyone. When construed as being permissive or directory, it carries the same meaning as the word "may."[63] Further, the Supreme Court in *S.P.D.C.N. v. Ekwems*[64] held that it is not in every case that the word "shall" imports a mandatory meaning into its use. It held further that the particular context in which the word "shall" is used under section 294(1) of the Constitution cannot be construed to mean compulsion for the simple reason that there could be several unforeseen occurrences or circumstances which could stall the judgment of the court from being delivered within the 90 days prescribed by that section of the Constitution.

[56] Constitution of the Federal Republic of Nigeria, 1999, s 162.
[57] Constitution of the Federal Republic of Nigeria, 1999, s 162(1).
[58] Per Bello JSC at *Mobil Oil (Nig) Ltd v FBIR* (1977) S.C 53 at 74
[59] (1869) L.R 4 H.L. 100
[60] CFRN 1999, s 162
[61] (1997) 2 NWLR (Pt. 485) 93,
[62] (1997) 4 NWLR (Pt. 500) 497 (P. 507. paras. G-H)
[63] see also *Ibrahim v. Akinrinsola* (2022) 18 NWLR (Pt. 1862) 455
[64] (2023) 4 NWLR (Pt. 1874) 213 (P. 248, paras)

Having established the above principles of law, it shall therefore be considered, whether or not the Cybercrime (Prohibition and Prevention) Act is inconsistent with the Constitution[65] by providing under section 44 (2) that the National Cybersecurity Fund shall be domiciled in the Central Bank of Nigeria, and if so, whether or not the imposed cybersecurity levy is null and void[66]

First of all, Section 162(10) of the Constitution clearly provides that for the purposes of subsection (1) of the section, "revenue" means any income or return accruing to or derived by the Government of the Federation from any source and includes: (a)any receipt, however described, arising from the operation of any law; (b)any return, however described, arising from or in respect of any property held by the Government of the Federation; (c)any return by way of interest on loans and dividends in respect of shares or interests held by the Government of the Federation in any company or statutory body.[67] Thus, the revenues collected are paid into the Federation Account which is also referred to as the distributable pool account. It is from this account that distribution is made in conformity with the provisions of section 162(2) and (3) of the Constitution[68]

On whether the Federal Government of Nigeria can maintain any other account other than the Federation Account for the purposes of receiving revenue collected by it; the Supreme Court in the case of *Attorney-General of Ogun State v. Attorney-General of the Federation*[69] held that it is not unconstitutional for the Federal Government, to maintain and keep any other account for the purpose of receiving revenues collected by the said Federal Government. BELGORE, J.S.C. reiterated the rationale for this principle thus;

> "Under s. 163(b) of the Constitution in regard to tax or duty envisaged in Part II, Second Schedule, item D is collected by the Government of the Federation or any other authority of the Government of the Federation, such money will not go into Federation Account. This is because if it is paid into Federation Account it will be subject to distribution formula envisaged in section 163(3) of the Constitution i.e. to Federal government, State Governments and Local governments. The provisions of s. 163 (b) envisage that such money should be paid to each state in the proportion of derivation from each state. Thus, such money should not go into Federation Account but a different account..."[70]

Furthermore, in *Attorney-General of Bauchi State v Attorney-General of the Federation*[71] the Supreme Court reiterated that it is not all incomes or revenues earned by the Government of the Federation that qualify to be paid into the Federation Account. The proceeds of privatization and commercialization of Federal Government enterprises, as well as capital gains taxes, custom and duties, and other income accruing to or derived by the Federal Government from any other source can be kept in dedicated accounts that are different from the Federation Account.[72] From the foregoing therefore, it follows that where a statute specifically provides a dedicated account other than the federation account into which a particular revenue of the federal Government shall be paid, then into such account shall such revenue be paid.

[65] CFRN 1999, s 162
[66] Constitution of the Federal Republic of Nigeria, s 1(3)
[67] *See Attorney-General of Abia State v Attorney-General of the Federation* (2002) 18 NWLR (Pt. 798) 232
[68] *ibid*
[69] (2002) 6 NWLR (Pt. 764) 542
[70] *Attorney-General of Ogun State v Attorney-General of the Federation (supra)* per BELGORE JSC, pages 285-286, paras. H-C:
[71] (2018) 17 NWLR (Pt. 1648) 299
[72] See *Attorney-General of Ogun State v Attorney-General of the Federation (supra)*

Thus, in the case of Cybersecurity Levy, it is not unconstitutional for the Cybercrime Act to provide that the Levy shall be paid into the NCF domiciled in the CBN. Another reason is that the cybersecurity levy is specifically for the Federal Government to provide protection for its digital infrastructures, and security (including cybersecurity) being under the exclusive Legislative list, the fund shall not be subjected to distribution in accordance with section 162 of the constitution. Hence, the levy is not null and void and the word shall under section 162(1) of the Constitution, shall not be construed as imperative.

4.3. Legal Implications of the Empowerment of the Office of the National Security Adviser (ONSA) with the Administration of the Cybersecurity Levy.

The office of the National Security Adviser (ONSA) is empowered under the 2024 amendment of the Cybercrime Act[73] to administer, keep proper records of the account and ensure compliance monitoring mechanism of the National Cybersecurity Fund. The above provision has raised the critical question as to the legitimacy of its role in overseeing the National Cybersecurity Fund (NCF) and administering funds collected through the cybersecurity levy. This stems from the fact that under the Federal Inland Revenue Service (Establishment) Act[74], the Federal Inland Revenue Services (FIRS) is established and saddled with the responsibility of controlling and administering different taxes and laws specified in the first schedule to the Act, or other laws made or to be made by the National Assembly from time to time, or other regulations made thereunder by the government of the federation and to account for all taxes collected.[75]

However, it must be clearly stated that the First Schedule to the Act[76] is not ambiguous as it unequivocally enumerates such taxes and laws which the FIRS is empowered to administer and collect which includes Companies Income Tax Act; Petroleum Profits Tax Act; Personal Income Tax Act; Capital Gains Tax Act; Value Added Tax Act; Stamp Duty Act; All regulations, proclamation, government notices or rules issued in terms of these legislations; Any other law for the assessment, collection and accounting of revenue accruable to the Government of the Federation as may be made by the National Assembly from time to time or regulation incidental to those laws, conferring any power, duty and obligation on the Service, etc. Thus, Cybersecurity Levy is not one of such taxes or laws.

Furthermore, the Taxes and Levies (Approved List of Collection) Act[77], provides that no person, other than the appropriate tax authority, shall assess or collect, on behalf of the Government, any tax or levy listed in the Schedule to the Act. By section 4 of the Act[78], tax authority" means- the Federal Board of Inland Revenue, the State Board of Internal Revenue or the Local Government Revenue Committee; or a Ministry, Government department or any other Government body charged with responsibility for assessing or collecting the particular tax.

From the foregoing, it therefore follows that the power to collect and administer any particular tax or levy is not automatic. It must be conferred by a statute or delegated by a body on whom it is conferred upon by a statute. Where such is not the case, no person, body, ministry, department or agency of the Government, including FIRS can collect or administer any tax whether or not such tax or levy accrues

[73] The Cybercrime (Prohibition, Prevention, etc.) Act (as amended) 2024, s 44(6)(a)
[74] Federal Inland Revenue Services (Establishment) Act, 2007, s 1
[75] FIRS Act, s 2
[76] *ibid*
[77] Taxes and Levies (Approved List of Collection) Act, 1998, s 2
[78] *ibid*

to the Federal Government.[79] In the case of Cybersecurity Levy, the Act[80] unequivocally conferred on the Office of the National Security Adviser (ONSA) the power to collect and administer the Fund (NCF) and as such, it has the legitimate power to do so subject to auditing by the Auditor General of the Federation.[81]

4.4. The Exact Intent of the Act, with Respect to who bears the Burden of the Cybersecurity Levy and Whether the Cybersecurity Levy Amounts to Double Taxation.

According to the Act,[82] a levy of 0.5% of all electronic transactions by the businesses specified in the second schedule to the Act shall be paid into the Fund (NCF). The Second Schedule to the Act enumerates the specified businesses to include: (a) GSM Service providers and all telecommunication companies; (b) Internet Service Providers; (c) Banks and other Financial Institutions; (d) Insurance Companies; and (e) Nigeria Stock Exchange.

The Implementation Guidance on the Collection and Remittance of the National Cybersecurity Levy[83], among other things made a list of 16 specific transactions that is exempted from the levy. Some of these transactions include: loan disbursements and repayments, salary payments, intra-account transfers within the same bank or between different banks of the same customer, intra-bank transfers between customers of the same bank, Cheques clearing and settlements, letters of credits and transactions relating to education.

Unfortunately, the issue on who in fact bears the burden of the cybersecurity levy has been a very controversial one. According to Ajisafe Olayiwola,[84] the burden is to be borne by customers of the specified businesses. According to him;[85]

> "For example, if someone plans to send ₦20,000 to another person, 0.5% of that sum would be ₦100.The originator of the electronic transfer will cover the levy, which will be deducted by the financial institution. The deducted sum will appear in the customer's account with the narration "Cybersecurity Levy." Thereafter, financial institutions will remit the deducted levy to the National Cybersecurity Fund, administered by the Office of the National Security Adviser."

According to the President of the Nigerian Labour Congress, Joe Ajaero, "implementing a levy on electronic transactions without assessing its impact on workers and vulnerable groups is unjustifiable."[86] He emphasized that the new levy is another anti-people policy of the government in the midst of excruciating economic hardship. On the other hand, Joseph Eimunjeze and Precious David argued that the levy is only applicable to the businesses specified in the Cybercrimes Act.[87] All these controversies and misinterpretations has led this researcher to inquire into the exact audience who shall bear the burden of the Levy.

---

[79] *ibid,* s 2
[80] *ibid*
[81] *ibid,* s 44 (6)(b)
[82] *ibid*
[83] Cybercrimes (Prohibition, Prevention, etc) (amendment) Act 2024- Implementation Guidance on the Collection and Remittance of the National Cybersecurity Levy, 2024.
[84] A Olayiwola, 'This is extortion: Nigerians lament CBN's new cybersecurity levy' *Punch* (Lagos, 7 May 2024) < https://punchng.com/this-is-extortion-netizens-lament-cbns-new-cybersecurity-levy/ > accessed 8 September 2024.
[85] *ibid*
[86] M Omonigho, 'NLC differs on CBN's Cybersecurity Levy' *Daily Post* (Lagos, 7 May 2024) < https://dailypost.ng/2024/05/07/nlc-differs-on-cbns-cybersecurity-levy/ > accessed 8 September 2024.
[87] J Eimunjeze and P David, 'An Overview of The Application of The National Cybersecurity Levy' *Udo Udoma & Bello Osagie* (PDF)

The general principle of law is that an ambiguous provision in a tax statute is construed *fortissime contra preferentes,* that is strictly against the acquiring authority but sympathetically in favour of the taxpayer.[88] Thus the legislature should ensure that tax is expressly imposed on a subject and the intention to lay the burden on the subject clearly shown by the statute.[89] This principle was affirmed by Lord Cairns in *Partington V AG,*[90] where he noted that if a person sought to be taxed falls within the letter of the law, he must be taxed. On the other hand, if the crown cannot bring him within the letter of the law, the subject is free.[91] The rationale for the strict interpretation is based on the fact that taxes are pecuniary burden on citizens.

The clear provision of the Act is that the Levy shall be paid by the businesses specified in the second schedule on all their electronic transactions only. According to Senator Buba who sponsored the amendment of the Cybercrimes Act, "the Act is clear on the businesses to pay the levy and not the citizen."[92] Thus, it is not the intentions of the draftsman that the burden of the levy shall be borne by the customers of the specified businesses. To do so will amount to double taxation, because, a customer will have to pay for the levy during his electronic transactions with banks and other financial institutions and still pay the same levy during his electronic transaction with GSM Service providers and other telecommunications companies and so on. This therefore will be very absurd. Thus, the burden of the tax must be borne alone by the specified businesses and not anyone else.[93]

4.5. The Derivative Source of the Power of the CBN to Prescribe Guidelines for the Implementation of the Cybersecurity Levy and its Implications.

The law is trite that a statute which seeks to impose tax must do so in clear and precise terms so that the taxpayers and stakeholders would know who and what is being taxed.[94] The Cybercrime (Prohibition and Prevention) Act provides that the cybersecurity levy is to be collected and administered by the ONSA. The fund itself shall be domiciled in the CBN. However, the Act unlike other tax statutes,[95] failed to make provisions on the guideline for the implementation and enforcement of the cybersecurity levy. The issue to be determined therefore is, "who exactly has the power to prescribe implementation guideline for the enforcement of cybersecurity levy since the Act has failed to make provision in that respect"?

Undoubtedly, CBN on the 6th of May issued a circular on the Implementation Guidance for the Collection and Remittance of the cybersecurity levy for Banks and other Financial Institutions. But does it really have the power to make such prescription? One would ask. The Act only provided that the NCF shall be domiciled in the CBN and nothing more. It did not in any of its provisions confer on the CBN with the power to collect or administer the levy, prescribe implementation guideline or sanction default with payment of the levy.

---

[88] *FBIR v The Nigerian General Insurance Company* (1966) L.L.R 86 at 95.
[89] *Aderawos Timber Trading Co. v FBIR* (1966) L.L.R, 195 at 200
[90] *ibid*
[91] See also *Cape Brandy Syndicate v Inland Revenue Commission (1921) 12 T.C 358 at 366*
[92] SB Umar, 'Cybersecurity Levy, National Security and Economic Growth,' *Vanguard* (Lagos, May 9, 2024) <https://www.vanguardngr.com/2024/05/cybersecurity-levy-national-security-and-economic-growth/> Accessed 2 August 2024
[93] CCA 2024, Second schedule.
[94] *SA Authority v Regional Tax Board* (1970) NCLR 276.
[95] National Information Technology Development Agency Act, 2007, s 12 and Federal Inland Revenue Service (Establishment) Act.

If however, CBN derived its power to prescribe such guideline statutorily from the CBN Act[96] and other legislations[97], then the implication is that the guideline shall not be binding on other specified businesses to whom the levy applies which are not under the regulation of the CBN. Thus, by implication, the various regulatory body for such other businesses such as National insurance Commission (NAICOM), Nigeria Communication Commission (NCC), etc will by default be empowered to prescribe implementation guidelines for those other businesses[98]. This will lead to diverse implementation guideline for different businesses, for the same cybersecurity levy and this is as good as irrational. This is because, one of the characteristics of a good tax system is certainty and uniformity in application.[99]
It is however, imperative to note that the Cybersecurity Advisory Council (the Council) is also established under the Act[100] to formulate and provide general policy guidelines for the implementation of the provisions of the Act[101] which by extension, includes Cybersecurity Levy which is a substantial provision of the Act.[102]

Thus, it will be more appropriate if the Council is the body formulating implementation guideline for the Cybersecurity levy. This will help provide a uniform implementation guideline for all businesses affected by the levy.

5. Prospects and Challenges to the Imposition of Cybersecurity Levy in Nigeria

Cybersecurity Levy undeniably offers numerous benefits for individuals, businesses, industries and the government. While the potential benefits of Cybersecurity Levy are significant, there are also challenges and concerns regarding the Levy which must be addressed.

5.1 Prospects to imposition of Cyber security Levy

The cybersecurity levy aims at generating funds to improve and strengthen the nation's cyber defenses against cyber threats and attacks. According to Senator Buba, Cybersecurity is very expensive and Nigeria must fund its cybersecurity and counter-terrorism programme independently and not through foreign aid[103]. The cybersecurity levy is even of higher necessity to Nigeria considering the incidence of deficit budget and economic instability in the country making it unreasonable for the government to include cybersecurity funding in its appropriation bill.[104] Therefore, government by imposing the levy aims to bolster its cybersecurity capacities and combat cybercrimes effectively by allocating resources for various purposes, including but not limited to:

1. Ensuring the Protection of Critical National Information Infrastructure:[105] The National Critical Infrastructure means systems and assets which are so vital to the country that the destruction of such systems and assets will have an impact on the society, national economic security, national public health and safety of the country.[106] This will involve modernizing technology, enhancing data security

[96] Central Bank of Nigeria Act, 2007, s 33(1) (a) and (b)
[97] Bank and Other Financial Institutions Act, Cap B3, Laws of the Federation of Nigeria, 2004.
[98] W Ajayi, 'Central Bank issues Guidance on the Collection and Remittance of the National Cybersecurity Levy' *KPMG* (Nigeria, May 2024) <https://kpmg.com/ng/en/home/insights/2024/05/central-bank-issues-guidance-on-the-collection-and-remittance-of-the-national-cybersecurity-levy-by-financial-institutions.html> accessed 8 September, 2024.
[99] MN Umenweke, Tax Laws and its Implications for Foreign Investments in Nigeria, (Enugu: Nolix, Educational 2005) p.5.
[100] Cybercrime (Provision and Prevention) Act 2024 (as amended), s 42
[101] *ibid,* s 43(2)(b)
[102] *ibid,* s 42 and 43
[103] SB Umar, 'Cybersecurity Levy, National Security and Economic Growth,' *Vanguard* (Lagos, May 9, 2024) <https://www.vanguardngr.com/2024/05/cybersecurity-levy-national-security-and-economic-growth/> accessed 2 August 2024.
[104] National Bureau of Statistics, *'Nigerian Domestic & Foreign Debt Q2 2023'* (Nigeria; 2024) <https://nigerianstat.gov.ng/elibrary/read/1241381> accessed 11 September 2024.
[105] Cybercrimes (Prohibition and Prevention) Act, 2007, s 1
[106] *ibid,* s 58

protocols, and investing in cyber defense tools across Government agencies such as Ministries, Departments, and Agencies.[107]

2. Promotion of Cybersecurity Awareness and Research: Another function of the funds received by the Government from the Cybersecurity levy will be to sensitize the public on how to identify cyber threats and the importance of cybersecurity. Educational initiatives and training courses can assist Nigerians in recognizing and mitigating cyber threats.[108]

3. Punishment of Cybercrimes and Deterrent to Cybercriminals: A portion of the revenue generated from the levy can be designated for law enforcement agencies for prohibition, prevention, detection, prosecution, investigation and punishment of cybercriminals. The allocation of resources dedicated to fighting cybercrime can also deter potential attackers.[109]

4. Promotion of Cybersecurity and protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights.[110]

5. Training of cybersecurity professionals and procurement of cybersecurity experts to help in fostering cybersecurity through research, expert advice, training, policy development, etc.

5.2 Challenges to imposition of Cybersecurity Levy

While there are potential advantages of the cybersecurity levy, there are challenges associated with the implementation timeline, compliance risks, and diplomatic discussions surrounding the cybersecurity levy. The concerns and challenges are:

1. Inability of the Act[111] to Provide Implementation Guideline and Procedure for Administration of the Cybersecurity Levy or Specify Clearly, the Person or Body who shall be Responsible to Prescribe Guidelines for the Implementation and Collection of the Levy: Although this lacuna or inadequacy in the Act cannot be said to have rendered the imposed Cybersecurity Levy unlawful, illegal or void, it must be noted that this is the main reason the implementation of the levy has been almost impossible. As a matter of fact, the many controversies and displeasures relating to the cybersecurity levy arose immediately after the issuance of the implementation guideline by the CBN.

2. Transparency and Corruption Concerns: Concerns regarding transparency arise regarding the allocation of the levy funds, particularly given the fact that the administration of the cybersecurity levy is conferred on the ONSA without any concrete and clear supervision other than that the account of the fund shall be audited by the Auditor General of the Federation[112]. Any suspicion of mishandling or misappropriation could erode confidence in the levy and Nigeria's cybersecurity endeavors[113].

---

[107] U Farouk, 'The Cybersecurity Levy from the CBN: What You Need to Know' *Medium* (7th May 2024,)< https://medium.com/@umarfarouk037/the-cybersecurity-levy-from-the-cbn-what-you-need-to-know-bff41666d902 > accessed 11 September 2024.

[108] *ibid*

[109] M Ekpeke, 'Cybersecurity levy: expert provides pros and cons of 0.5% deductions' *IT Pulse* (7 May 2024) < https://itpulse.com.ng/2024/05/07/cybersecurity-levy-expert-provides-pros-and-cons-of-0-5-deductions/ > accessed 8 September 2024.

[110] Cybercrime (Prohibition and Prevention) Act, 2024 (as amended), s 1

[111] *ibid*

[112] Cybercrime (Prohibition and Prevention) Act, 2024 (as amended), s 44(6)(a) and (b)

[113] *ibid*

3. Compliance Errors: The complexity relating to the classification of transactions and implementing exemptions to the cybersecurity levy as contained in the CBN implementation circular,[114] increases the potential for compliance mistakes. Erroneously applying the levy to transactions that should be exempted, or vice versa, may lead to financial penalties, regulatory investigation, and harm to banks' reputations. This situation could also spark disagreements and misunderstandings with international partners and investors.[115]

4. Burden on Businesses and Consumers: The levy has the potential to raise the cost of electronic transactions for both consumers and businesses. Despite being a small percentage, it can accumulate over time, particularly for those who frequently use electronic payment systems. This increase may discourage the use of electronic transactions and impede efforts to promote financial inclusion.

5. Economic instability, gallop inflation and extreme hardship on the citizens at the time of this research is another impediment to the implementation of the levy.[116]

6. Conclusion

The imposition of cybersecurity levy in Nigeria represents a pivotal and necessary strategy by the Government aimed at providing funding for the government to bolster its critical information infrastructure and protect sensitive data, networks and systems from all forms of cyber risks and attacks. This study has delved into an inquiry into the legality or otherwise of the imposed cybersecurity levy and having analysed different legal and institutional frameworks relating to the levy, the findings revealed essentially that the cybersecurity levy is legal, constitutional and valid.

The examination of the current state of cyber threats and attack in Nigeria showed an exponential increase in Nigeria exposure to those risks and attacks; and coupled with the significant revenue challenges the country is facing, resulting in borrowing and indebtedness, the imposition and implementation of cybersecurity levy becomes very imperative since the government must raise funds for its cybersecurity initiatives and programs. It is even more important considering the fact that the government must finance its cybersecurity and counter-terrorism programme by itself without borrowing from other countries, and as this study has shown, the government cannot however do so through its appropriation bill.

Furthermore, this research revealed that both individuals, businesses, industries and government are all victims of cyber threat and attack from both state and non-state actors. Such attacks compromise sensitive data, networks and systems in a fashion that detection or defence can be hard, thus cybersecurity levy provides increased funding for the government to enhance cybersecurity awareness and education; training and hiring of cybersecurity experts; and dedicated funds to Investigate, prosecute and punish cybercrimes and cybercriminals. Despite the obvious benefits of the cybersecurity levy, it must be understood that the imposition of the cybersecurity levy is not short of challenges which must be addressed adequately in order to ensure smooth implementation of the levy in Nigeria.

---

[114] Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act 2024- Implementation Guidance on the Collection and Remittance of the National Cybersecurity Levy, 2024.

[115] *ibid*

[116] W Ajayi, 'Central Bank issues Guidance on the Collection and Remittance of the National Cybersecurity Levy' *KPMG* (Nigeria, May 2024) <https://kpmg.com/ng/en/home/insights/2024/05/central-bank-issues-guidance-on-the-collection-and-remittance-of-the-national-cybersecurity-levy-by-financial-institutions.html> accessed 8 September, 2024.

7. Recommendations

The benefits which the cybersecurity levy offers cannot be overemphasized. Thus, the recommendations below shall provide a strategic roadmap for the government to harness these benefits inherent with cybersecurity levy. This research further made recommendations for other funding mechanisms which will help Nigeria appropriately finance its cybersecurity initiatives and programs and eventually join the ranks of nations, such as UK with a well-established cybersecurity strategy and policy. Discussed below are the recommendations by the researchers:

I. Provision of clear and Adequate Implementation Guidelines: There should be a review of the Cybercrimes Act to clearly provide for implementation guideline for the collection and remittance of the cybersecurity levy. In the absence of such, the Cybersecurity Advisory Council (the Council) shall be authorised to prescribe guidelines for the implementation of the levy since under the Cybercrimes Act, the council is empowered to formulate and provide general policy guidelines for the implementation of the provisions of the Act. Otherwise, the Act should be reviewed to make provision, specifying clearly, the person, body or agency authorised to prescribe guidelines for the implementation of the levy. This will help provide a uniform implementation framework for the cybersecurity levy by all the businesses affected by the levy; define clearly, the subject of the levy and eliminate the unending controversies and misinterpretations relating to the levy.

II. Supervision of the Office of the ONSA in the Administration of the Levy: It is also very important that while the ONSA administers the levy, his activities should not just be left without supervision. Subjecting the account of the NCF to audit by the Auditor General of the Federation is not enough to guarantee transparency and accountability. Thus, the Act should be reviewed to include an adequate provision for supervision and accountability in the administration of the Levy. It is the candid recommendation of this Researcher that the Act establishes a supervisory body such as the Minister of Finance to monitor the activities of the ONSA in the administration of the levy, just as the FIRS under the Federal Inland Revenue Act, 2007, in exercise of their functions is subjected to the general direction of the Minister. Otherwise, the Cybersecurity Advisory Council shall be conferred with the power to monitor and scrutinize the activities of ONSA with respect to the NCF. This will help reinforce the confidence that the fund is being appropriated to the purpose, for which it was established.

III. More importantly, adequate regulations should be provided to ensure that the burden of the levy is not transferred on the citizens or customers of the businesses affected by the levy. The customers of those businesses are not the subject of the levy and should not be made one by any sharp practice by any of the affected businesses.

IV. Provision of Complementary Funding Mechanisms for Cybersecurity: The need for an alternative funding mechanism for Nigeria's cybersecurity initiative is very essential considering the high cyber threat and attack to which the country is being exposed. Other reasons that make the need for alternative funding mechanism very imperative includes: economic uncertainties; the fact that the Fund generated through the levy will not always be available to cater for the cybersecurity initiatives and programs of the government because cybersecurity is very expensive; and the fact that at the time of this research, the implementation of the levy is on suspension. Such other funding sources include:
    a) Establishment and investment in cybersecurity firms in the country which shall be dedicated to developing and selling of cutting-edge cyber tools and products to other countries, thereby generating revenue for the government to bolster its cybersecurity
    b) Partnership and collaboration with other countries including private establishments and international security agencies so as to secure the best cybersecurity for the country.
    c) Subscription to cybersecurity schemes, cybersecurity funding and grants provided by international organizations such as World Bank, International Monetary Fund (IMF), etc. A good example of such funding is the World Bank's Cybersecurity Multi-Donor Trust Fund.