COVID- 19 PANDEMIC AND ANTI-CYBERCRIMES CRUSADE IN NIGERIA: CHANGING THE NARRATIVES FOR A BETTER ENFORCEMENT REGIME

Miebaka Nabiebu, University of Calabar
Shishitileugiang Aniashie Akpanke, University of Calabar

ABSTRACT

Nothing has ravaged the global community in recent times like the dreaded corona virus (COVID -19). The virus, though of Chinese origin was transported into Nigeria through an Italian ship. This paper therefore appraises COVID -19 pandemic and anti-cybercrimes crusade in Nigeria: changing the narratives for a better enforcement regime. The paper trenchantly posits that, COVID -19 pandemic is a blessing in disguise as it brought to fore the underlying ineffectiveness that surrounds Nigeria's administrative, institutional and legal architecture for combating cybercrimes. It is also the position of the paper that, during the lock-down (occasioned by the pandemic), there was an exponential increase in cases of cybercrimes in the country as a result of poor enforcement mechanisms, corruption, greed, poverty, lack of expertise, unemployment and the skewed undying quest for wealth. The paper makes a case for a total overhauling of the legal and institutional regime for cybercrimes combat so as to be at par with countries such as the United States of America, United Kingdom, China and the United Arab Emirate (UAE). The paper adopts the doctrinal research approach; primary and secondary materials were sourced and used. These materials include statutes, case laws, articles published in reputable journals, reports of renowned bodies, newspapers publication amongst others.

Keywords: Corona Virus, COVID-19, Cybercrimes, Enforcement and Nigeria**.**

INTRODUCTION

The year, 2020, is the most fearful, dreadful, problematic, difficult, unpredictable and uncertain period of the 21st century. The reason for this appellation or description is not unconnected to the underlying hardship, difficulties, panic, havoc, uncertainties, and mammoth challenges occasioned to the global community as a result of the unprepared, unwarranted, unwelcomed and skewed emergence of one of the deadliest and most wide spread perils called SARS-Corona Virus. This virus has also been christened COVID-19 by the World Health Organization (WHO).Worthy of note is the fact that, the origin and etymology of the virus has generated verbal gymnastic and heated debate amongst scholars, researchers, scientists, political thinkers and stakeholders. Thus, conspiracy theorists, such as Donald J. Trump, the current president of the United States of America, Mike Pompeo (US Secretary of States) amongst others are of the succinct opinion that the virus is a biological weapon, deliberately and

Citation Information: Nabiebu, M., & Akpanke, S.A. (2021). Covid-19 pandemic and anti-cybercrimes crusade in Nigeria: Changing the narratives for a better enforcement regime. Journal of Legal, Ethical and Regulatory Issues, 24(7), 1-14

surreptitiously concocted by China in its virology laboratory in Wuhan, and unleashed either deliberately or accidently to the earth and its inhabitants. On the other hand, anti-conspiracy theorists assert that, the origin of COVID-19 is biological based, animal centric (that is, it has natural roots from animals) and not man-made or laboratory based as purportedly claimed by conspiracy theorists. Professor Richard Ebright, a renowned, eclectic, and well-acclaimed professor of Chemical Biology, Rutgers University, Camden, England posits that there is no possibility that the virus is a biological weapon (The Washington Post, February 26, 2020).This proposition has also been affirmed by the US intelligence agencies. Records point to the fact that, the novel virus was first recorded in November 2019 in Wuhan City, the capital and commercial arena of China. Due to its high mobility, potency and propensity, the virus within the shortest period spread to all regions as well as over 200 countries of the world. This prompted the World Health Organization to; on March 11, 2020 declare the virus a pandemic, (by virtue of the virus infecting more than 100,000 persons across regions of the world). As at October 13, 2020, the global number of confirmed cases of the virus is 38, 292,335 while the death toll is 1, 088, 958. Happily, a total of 28, 764, 604 persons have successfully recovered from the virus (Worldometers Report, 2020).

Nigeria, not being immune to the mobility, potency and exponential spread of the virus as well as its excruciating vicissitude recorded her index case on February 27, 2020 (Nigeria Centre for Disease Control (NCDC), Report of February 27, 2020). The index case happens to be an Italian who travelled into the country. In order to curb or contain the spread of the virus in the country, government at all levels initiated different measures, strategies and multi-sectorial policies. These measures include the issue of the COVID-19 Regulations by the Federal Government (which was later adopted by States and Local Government Areas across the country) as well as the NCDC Guidelines by the Federal Ministry of Health. Further, in consonance with the COVID-19 Regulations, 2020, NCDC Guidelines and international best practices, government also declared a lockdown in key areas of the economy such as schools, churches, mosques, markets, business enterprises, recreation centres, institutions (excepting those that provide essential services example, the Nigeria Police, Army, registered private security companies, hospitals, pharmaceutical and health care providers and companies, media and broadcast stations including their staff, etc.), seaports, air ports,(except in special circumstances such as security personnel, carriers of reliefs materials/palliatives geared towards cushioning the pandemic) amongst others. Banks and other financial institution were on partial lockdown. This is in addition to social/physical distancing policy and the wearing of face masks, face shields and personal hygiene.

As part of the social/physical distancing policy, people were encouraged to prioritize and patronize electronic learning (e-learning), electronic commerce (e-commerce), electronic trade (e-trade), electronic banking (e-banking) amongst other services within the financial technology (fintech) landscape through the use of Point of Sales (POS) machines, Automated Teller Machines (ATMs), mobile phones as well as computers. This is in tandem with the WHO perspective that digital payment is a potent conduit pipe for containing the spread of the virus (Bright, 2020). To further cushion the dismal effects of the virus, government gave palliatives to the vulnerable as well as kick-back loans to households and firms. Internet scammers and cyber criminals took advantage of the lockdown to navigate their nefarious acts. They sent out

Citation Information: Nabiebu, M., & Akpanke, S.A. (2021). Covid-19 pandemic and anti-cybercrimes crusade in Nigeria: Changing the narratives for a better enforcement regime. Journal of Legal, Ethical and Regulatory Issues, 24(7), 1-14

unsolicited emails and messages on WhatsApp, Facebook, Twitter and other social media platforms to their suspected victims claiming that such messages emanate from organizations such as the Nigeria Centre for Disease Control, World Health Organization, Central Bank of Nigeria amongst other reputable organizations. Once victims click to the link(s) contained in such message (s), their accounts are often hacked and defrauded. For example, on August, 2020, Miss Veronica Bako (Late), a 100 level student of the Department of History and International Studies, University of Calabar, Calabar committed suicide as a result of the fact that she was defrauded of the sum of ₦100, 000 by cyber criminals during the COVID-19 lockdown in Nigeria (lindaikejisblog.com).

It is apposite that, COVID-19 pandemic ushered an exponential increase in cyber-crimes in Nigeria. This is more so because of lack of responsiveness from national institutions that have been saddled with the duty of combating the menace, poverty, skewed and undying quest for wealth and the ever increasing rise in unemployment/underemployment in Nigeria. This supports the findings by the Global Initiative against Transnational Organized Crimes that, COVID-19 pandemic has impacted African countries negatively leading to the increase in online crimes (Global Initiative Report, 2020). Without doubt, the COVID-19 pandemic has further uncovered the lack of effectiveness and responsiveness in Nigeria's legal, institutional and administrative architecture for cyber-crimes combat in the country. It is against this background that this paper intends to probe the legal and institutional architecture for cyber-crimes combat in Nigeria vis-à-vis the COVID-19 experience with a view to making recommendation on how to strengthen same for better regime. A comparative analysis of cyber-crimes responsiveness during the COVID-19 pandemic in other countries (United Arab Emirate, USA, and UK) vis-à-vis Nigeria shall be made.

Cybercrimes: Meaning, Nature, Scope and Effects

The word "*crime*" connotes an action or omission which the law preserve to constitute an offence and sets punishment thereof while the term "*cyber*" is used to describe that which relates to the culture of computers, information technology and virtual reality. It therefore follows that, when we talk of cybercrimes, we refer to activities which are criminal in nature and effected by means of computer or internet. In Nigeria, names such as yahoo yahoo, computer money press buttons, and excess money are seldom used to describe cybercrime. Examples of these crimes include schemes/scams on fake web sites, hacking into personal accounts (WhatsApp, Facebook, Twitter, etc.), breaking into competitor's database, hacking into work database and other facets of internet theft and fraud (Legal.Match.Com).Unemployment, urbanization undying quest for wealth, poverty, corruption, negative role models, poor enforcement of cyber laws amongst others have been identified as the main causes of cybercrime in Nigeria.

Cybercrimes have negative consequences on their victims, that is, consumers as well as business entities. A single successful cyber-attack usually have a high thundering and multiplier implications on the economy including theft of intellectual property, financial losses, and even loss of consumer confidence and trust (Rahaman, 2016). Over 1.5 million people are victims of cybercrime every year (Q.A Platform.com) .The total monetary cost and effect of cybercrime on the society is estimated to be billions of dollars per annum (Gross, 2018). The federal government also estimated the annual cost of cybercrime in Nigeria to be about 0.08% of the

Citation Information: Nabiebu, M., & Akpanke, S.A. (2021). Covid-19 pandemic and anti-cybercrimes crusade in Nigeria: Changing the narratives for a better enforcement regime. Journal of Legal, Ethical and Regulatory Issues, 24(7), 1-14

country's Gross Domestic Products (GDP), which represents about N127 billion (Deloite, 2017). It has also been reported that Nigeria lost over 250 billion naira as a result of cybercrime in the year 2019 (The Guardian of November 28, 2019).This has prompted the allocation of over $121 billion on global information security in 2019. Apart from the economic misfortune, occasioned by cybercrimes, a lot of persons have died in Nigeria as a result of cybercrimes. For instance, during the COVID-19 lockdown, a 100 level student of the University of Calabar, Calabar, who hails from Benue committed suicide because she was defrauded of the sum of ₦100, 000 being the allocated sum for her school fees by cyber criminals.

Nigeria's Legal and Institutional Architecture for Cybercrime Combat

Nigeria has a potpourri of legislation, regulations, conventions and guidelines on cybercrimes and cybersecurity. The Constitution of the Federal Republic of Nigeria, 1999 (as amend) is the most pivotal legal document in that regard. Section 1 makes the provision of the Constitution to be supreme and binding on every person and institutions thereto. Section 36 forms the stem for the fundamental principles of presumption innocence and right to fair hearing which forms the bedrock of the Nigeria criminal jurisprudence and this also applies to suspects of cybercrimes. Section 6 creates the judiciary as an unbiased umpire, institution and vehicle of justice in Nigeria. Section 214 creates the Nigeria Police, clothed with the primary responsibility of protecting the lives and property of every Nigerian.

The Economic and Financial Crimes Commission (Establishment) Act, 2000 is also a germane law on cybercrimes in Nigeria. Section 1 of the Act establishes an inter-agency body christened the Economic and Financial Crimes Commission (EFCC), with the primary mandate to combat financial and economic crimes. Apart from the duty of preventing, investigating, prosecuting and penalising economic and financial crimes in Nigeria. The Commission is also charged with the hallmark responsibility of giving effect or enforcing the provisions of other laws, legal instruments, and regulations relating to economic and financial crimes in the country (efccnigeria.org). Section 46 of the Act defines "*Economic Crime*" as "*a non-violent criminal activity committed with the objectives of earning wealth illegally"*.

The Advanced Fee Fraud and Related offences Act, 2006 is also an important instrument on cybercrimes in Nigeria. The Act from its wordings and expressions prohibits and punishes certain offences pertaining to advance fee fraud otherwise known as 419 scam or funds transfer scam in Nigeria. By Section 14 of the Act, the Federal Capital High Court and the State High Courts have been clothed with the jurisdiction to try cases that are within the province of the Act.

Another important legislation on cybercrime is the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 (CYPPA). The Act from its tone and tenor prohibits and punishes all aspects of cybercrimes, namely: unlawful access to a computer, cyber terrorism, unauthorized modification of computer system, data and system interference, forgery, wilful misdirection of computer messages, etc. Punishment for cybercrimes ranges from fine of ₦1, 000.000 (One Million Naira) or imprisonment for a period of 2 years, and in some cases, even death penalties depending on the gravity of the offence. This can be distilled from an in-depth reading of Part III (Sections 5-36) of the Act. The Act in Section 5 empowers the judge to in reasonable circumstances grant an order allowing any law enforcement agency to intercept any electronic communication for the purpose of giving effect to the provisions of the Act. Apart from the CYPPA, the Nigeria Data

Citation Information: Nabiebu, M., & Akpanke, S.A. (2021). Covid-19 pandemic and anti-cybercrimes crusade in Nigeria: Changing the narratives for a better enforcement regime. Journal of Legal, Ethical and Regulatory Issues, 24(7), 1-14

Protection Regulation 2019 is another piece of legislation on cybercrimes in Nigeria. Reading through the preamble to the Act, it suffices that, the regulation seeks to protect data both in motion and at rest.

The Money Laundering (Prohibition) Act, 2011 is also amongst the checklist of legislation that deals with cybercrimes in Nigeria. The Act contains laudable provisions that tends to prohibit the financing of terrorism as well as the proceed accruing thereto (Sections 15-19 and Preamble to the Act). Section 1 places a limitation on cash payment or receipt through a financial institution. The financial limit for an individual is ₦5 million Naira or its equivalent and 10 million or its equivalent in the case of a corporation. By Section 2, financial institutions are obligated to report to the Central Bank of Nigeria any international transfer of funds and securities including money service of any sum exceeding 10,000 U.S Dollars or its equivalent.

Other legal instruments include: the Central bank of Nigeria Act, Cap ----, Central Bank of Nigeria Guidelines on Mobile Lending and Money Services in Nigeria, 2015; CBN Guidelines on International Money Transfer Services in Nigeria, etc. The above pieces of legislation establish various institutions to combat cybercrimes in Nigeria. Examples of such institutions include the Economic and Financial Crimes Commission (EFCC), Independent Corrupt Practices and other Related Offences Commission (ICPC), Nigerian Financial Intelligence Unit, Nigeria, Police, Courts of competent jurisdiction etc.

Global Response to Cybercrimes during the COVID-19 Pandemic

Since the emergence of the most dreadful and largest public health disaster, corona virus in 2019, the global space has been agog and inundated with a lot of economic, socioeconomic, political, psychological, financial and criminal crisis, unrest and misfortunes. In order to contain the spread and impacts of the virus, efforts have undertaken both nationally and internationally. In China, where the virus first started, severe lockdowns were put in place. This measure has been extended to almost all countries of the world including Italy, Spain, United States of America, United Kingdom, France, Nigeria, South Africa etc. The effect of this global lockdown is that, it has led to an unprecedented decrease production as a result of decline in consumption, disruptions in the transportation, service, and manufacturing industries, with a corresponding and significant reductions in income as well as a rise in unemployment, loss of jobs as a result of poor production or closure of companies (Park, 2020). On the whole, the functioning of global supply chains has been disrupted and this has affected companies across the globe. There is also shortage of many goods in supermarkets around the world as a result of the change in consumer patterns by consumers Global financial markets have registered sharp falls, and volatility is at levels similar, or above, the financial crisis of 2008/9.

The impact of the pandemic has also manifested itself in the exchange rate of the national currency. It depreciates by over 1.0% in the formal market since mid-February 2020 and the depreciation of the Naira in the informal market is even by a larger margin. Indeed, the outbreak cause more disruptions in the financial services, labor and trade sectors. Following the pandemic, some financial institutions closed their branches and this resulted in loss of jobs for many non-staff (casual) workers. The hardship caused by the pandemic has also led to increased poaching of resources and materials available in the immediate surroundings for survival. This act is common in rural communities among daily paid workers and small scale artisans whose vocation

Citation Information: Nabiebu, M., & Akpanke, S.A. (2021). Covid-19 pandemic and anti-cybercrimes crusade in Nigeria: Changing the narratives for a better enforcement regime. Journal of Legal, Ethical and Regulatory Issues, 24(7), 1-14

and earnings have been drastically affected by the lockdown occasioned by the pandemic. In the educational sector, the private school proprietors and staff suffered the worst. The closure of schools meant no income and no wages for those concerned, since parents and guardians will not pay fees when the school is not in session.

The pandemic has also led to an increase in the reliance and use of the internet as people trade, work and learn from home through e-commerce, e-learning and e-communication platforms (World Economic Forum Report, 2020). Majority of these people in the global space particularly in Sub-Sahara Africa Countries are unfamiliar with the operational knowledge of these technological and communication devices , thus making them vulnerable and attractive targets of cybercriminals, who exploit them through divergent means, namely: offering of fake cures for sale on the internet; online advertisement sales of non-existent hand sanitizer and medical personal protective equipment (PPEs); unsound investment advocate (e.g. cryptocurrencies); false business e-mails etc. Advanced internet criminals continue to target critical infrastructures including hospital and Vaccines Development Centers. According Belisaro Contreras, the manager of Cyber Security Programme Organization of America States and Co-Chair, Global Future Generation Cyber Security, World Economic Forum, the USA and U.K have seen an unprecedented increase in the reported cases of criminal activities during the COVID 19 Pandemic (World Economic Forum Report, 2020). Findings from the United Nations Office on Drugs and Crimes (UNODC) reveal that, cybercrime is evolving and growing exponentially in response to the COVID 19 Pandemic. There has been an unprecedented increase in online fraud, extortion and sexual abuse as a result of the comprehensive social/physical distancing mean initiated and implemented by government across the globe/community as a means of containing the spread of the dreaded monster.

The global response to cybercrimes in the COVID-19 era may be described as collective and multi-sectorial. A plethora of national, regional and international institutions are key players in the global anti-cybercrimes crusade. These institutions include the US National Security Agency; US Cyber Threat Intelligence Integration Centre; US Federal Bureau of Investigations; Organization of American States; Cyber Watch; the UK Centre for the Protection of National Infrastructure; European Network and Information Security Agency. Others include: the United Nations, EUROPOL, International Criminal Police Organization otherwise known as INTERPOL; Cooperative Cyber Defence Centre of Excellence; European Network and Information Security Agency; G8: Subgroup on High-tech Crime; United Nations Office on Drugs & Crime; the Organization for Economic Co-operation and Development, that is, OECD (which in the last three decades has developed policy options, organized conferences as well as published guidelines and best practices on cybercrimes and cyber security); the International Telecommunication Union (an autonomous, specialized agency of the UN) etc. (Choucri, 2016). These institutions played and continue to play inevitable roles and functions in the global cybercrime combat, particularly in the COVID-19 arena. These roles range from policy formulation, training of anti-cybercrime experts or personnel, mass awareness to investigation and arrest of cybercriminals amongst others. For example, on March 20, 2020, the US Federal Bureau of Investigations alerted the global space of the rise in fraud schemes as a result of the COVID-19 pandemic. Nigeria's notorious inter hacker, Raymond Igbalode popularly known as Hushpuppi and his colleagues were arrested by INTERPOL in the United Arab Emirate in

Citation Information: Nabiebu, M., & Akpanke, S.A. (2021). Covid-19 pandemic and anti-cybercrimes crusade in Nigeria: Changing the narratives for a better enforcement regime. Journal of Legal, Ethical and Regulatory Issues, 24(7), 1-14

connection to fraud and money laundering of over 100 Million US dollars meant for unemployed American citizens to cushion or water down the effects of the pandemic as well the 35 Million US dollars ventilator scam.

To further cushion the effect of the pandemic and reduce crimes including cybercrimes across the globe, most countries of the world initiated and gave out palliatives and incentives to their citizens as well as small and medium enterprises. In China, for instance, government made used of contactless lockers or machines to deliver food to her citizens particularly health workers who are the frontline in the fight against the pandemic. This was made easier due to the technological advancement of the country. In Afghanistan, on April, 2020 government initiated and implemented a free feeding programme for the vulnerable persons, that is, poor persons in Kabul and this was later extended to other cities. Government also extended this gesture to electricity and utility tariffs. In May, 2020, the government waived electricity bills of less than Af 1,000 (US$13) for all residents of Kabul and also paid utility bills of the past two months for 50 percent of households in Kabul. Over 1.5 million Kabul residents benefited from the laudable initiative. Recognizing the liquidity constraints of many taxpayers, the government extended the tax filing deadline for the first quarter by 45 days (IMF Policy Responses to COVID-19 Report, 2020). Similar palliative measures were also initiated and implemented in the UK, Spain, France, Germany, South Africa and Ghana.

Appraising Nigeria's Response to Cybercrimes during the COVID-19 Pandemic

In March 30, 2020, the President of Nigeria in exercise of his powers donated to him by the Quarantine Act, Cap. Q2 LFN 2004 issued the COVID-19 Regulations, 2020 (See Preamble to the COVID-19 Regulations, 2020). Some glaring areas of the Regulations include the restriction of movement in the country (except where such movement relates to hospitals, medical establishment, private security companies, health care related manufactures and distributors, petroleum generation and retail outlets, electronic media and broadcast stations as well as their staff, etc.); closure of airports (except in special circumstances namely, security personnel, careers of reliefs material/palliatives) amongst others. This can be gleaned from a succinct and holistic reading of Sections 1, 2, 3,4,5,6 and 8 of the Regulations.

Nigeria's response to COVID-19 pandemic is collective, dynamic, multi-sectorial and multi-structural in nature. Several institutions, bodies and parastatals are involved. The first in the list is the Presidential Task Force on COVID-19. This body was established by President Buhari on March 9, 2020. Its responsibilities include but not limited to coordinating and overseeing Nigeria's multi-facet inter-governmental architecture to combat as well as contain the spread and dismal effects of the corona virus in Nigeria. To achieve its mandate, the body made policies, directives, guidelines as well worked in collaboration with other sector bodies such as the NCDC, Central Bank of Nigeria, etc. Also, the body made recommendations leading to the direct funding and technical support to state and local government so as to rekindle their preparedness capacity to tackle the spread and effects of the virus. This led to establishment of Epidemiology and Surveillance Centres, PTF National Pandemic Response Centre (NPRC), Case Management and Isolation Centres, amongst other facilities spread across the country. It is important to state that, various States and Local Government have also established their respective task force on COVID-19. Examples are the Lagos State Task Force on COVID-19,

Citation Information: Nabiebu, M., & Akpanke, S.A. (2021). Covid-19 pandemic and anti-cybercrimes crusade in Nigeria: Changing the narratives for a better enforcement regime. Journal of Legal, Ethical and Regulatory Issues, 24(7), 1-14

Rivers State Task Force on COVID-19, and Cross River State Task Force on COVID-19. Inclusive in the list of institutions is the Federal Ministry of Health. The central function of this Ministry is the formulation as well as implementation of health policies in Nigeria (Welcome, 2011). This Ministry is the mother to the Nigerian Centre for Disease control (NCDC).

Another important institutional architecture on anti-COVID-19 is the Federal Ministry of Humanitarian Affairs and Social Development. This Ministry is the brain child of the Muhamadu Buhari's administration and established on August 21st, 2019, with the pivotal responsibility of initiating, developing human policies, providing effective disaster management, mitigation, preparedness as well as creating and implementing social programmes that are fair and inclusive in nature (Federal Ministry of Disaster Management and Social Development). Due to the timing and circumstances that surrounds its creation; one may strongly surmise that the Ministry was divinely and futuristically established in response to COVID-19 pandemic. As earlier stated in the introducing part of this paper, as a way of cushioning the pitiable effect of the COVID-19 lockdown, the federal government of Nigeria gave out palliatives to special group of persons, otherwise known as the vulnerable. These palliative where in form of distribution of food items, tradersmoni, marketmoni, kick-back loans. The parameters for the distribution of these palliative was left to the exclusive preserve of Federal Ministry of Disaster Management and Social Development. Billions of naira was used to affect the purpose. While rendering its stewardship, the Minister, Hajiya Sadiya Umar Farouq stated that the palliatives were evenly distributed to the intended beneficiaries, and all the tribes in Nigeria.

Apart from the afore-discussed institutions, the underlying role played by the NCDC in the wake of the pandemic cannot be underrated. It is the country's national health institute commissioned with the hallmark responsibility of championing the preparedness, detection including the response disease outbreaks and public health emergencies in Nigeria. Though established in 2011, the agency was given a legislative backing in November, 2018 courtesy of the NCDC Act, 2018. Undoubtedly, the agency has been active and has performed excellently in response to the COVID-19 outbreak in Nigeria. It has set up laboratories and epidemiological centres across the country. As at October 13, 2020, the total number of accredited NCDC laboratories and epidemiological centres is pegged at 69. The centre has engaged and is engaging in samples collection, testing as well as treatment of COVID-19 patients in Nigeria. As at October 13, 2020, the total number of samples tested in Nigeria is estimated at 558, 313 with 60, 430 samples returning positive. A total of 1,115 persons have died as a result of the virus, while a total of 51,943 persons have recovered from the virus.

In order to ensure that Nigerians do not fall victims to activities of cyber criminals during the lockdown, the agency sent messages via Twitter, Facebook, WhatsApp among other social media and communication platforms sensitizing, educating and warning Nigerians not to fall prey to cyber scammers. However, a lot of criticisms and accusations have been levied against the agency. Many persons claim that the figures reported by the NCDC are not real but manipulated in order to satisfy the egoistic quest of the ruling cabals who perceive the pandemic as an avenue to amass wealth.

The Central Bank of Nigeria has also been instrumental in the fight against COVID-19 pandemic in Nigeria. The Bank has initiated and to some extent, implemented a quit number of measures and policies to tackle the impact of the virus in the country. Examples of these

Citation Information: Nabiebu, M., & Akpanke, S.A. (2021). Covid-19 pandemic and anti-cybercrimes crusade in Nigeria: Changing the narratives for a better enforcement regime. Journal of Legal, Ethical and Regulatory Issues, 24(7), 1-14

measures include the establishment of a 50 billion naira fund to revive and support the country's economy. The primary beneficiaries of the fund are households and micro and small enterprises. In the vein, on March 16, 2020, Nigeria's apex bank of Nigeria announced new measures to wit: a 1 year extension of a moratorium on principal repayments for CBN intervention facilities; the reduction of the interest rate on intervention loans from 9 percent to 5 percent; strengthening of the Loan to Deposit ratio policy (i.e. stepped up enforcement of directive to extend more credit to the private sector); creation of NGN50 billion target credit facility for affected households and small and medium enterprises; granting regulatory forbearance to banks to restructure terms of facilities in affected sectors; provision of an additional NGN100 billion intervention fund in healthcare loans to pharmaceutical companies and healthcare practitioners intending to expand/build capacity, provision of credit assistance for the health industry to meet the potential increase in demand for health services and products *"by facilitating borrowing conditions for pharmaceutical companies, hospitals and practitioners";* Commencement of a three month repayment moratorium for all TraderMoni, MarketMoni and FarmerMoni loans, similar moratorium to be given to all Federal Government funded loans issued by the Bank of Industry, Bank of Agriculture and the Nigeria Export-Import Bank (CBN, 2020). In addition, on April 7, 2020, CBN, issued a fraud alert, apprising the general public about the unscrupulous activities of cyber-criminals, who are taking advantage of the current COVID-19 pandemic to navigate their criminal activities as well as defrauding the populace through electronic devices and different techniques.

Other key institutions in the COVID-19 debacle in Nigeria are the Nigeria police and other sister agencies such as the Army, Air force etc. Apart from their general function of protecting lives and properties of all citizens. These institutions have also assisted in enforcing the COVID-19 Regulations, through the mounting of road blocks, ensuring that people wear facemasks and other protective equipment, and in the same vein, arrest violators of such directive and ensure that they are charged to mobile courts established for such purpose. As part of the effort to curb cybercrimes during the pandemic, Nigeria's Inspector General of Police (IGP) Mr. Mohammed Adamu issued a circular informing Nigerians to be vigilant against criminal elements as well as the unscrupulous activities of cyber criminals which has exponentially increased sequel to the emergence of the COVID-19 pandemic. In a press release, signed by his spokesman, Frank Mba, the IGP advised Nigerians to avoid patronizing suspicious emails and clicking on links in unrecognized emails and attachments. He further advised that citizens should ensure that they manage their social media settings; use strong passwords to secure their emails as well as other social media handle (channelstv.com). This is in addition to the earlier warning of the global police body known as Interpol. According to Interpol, between January 2020 and April 2020, over 907, 000 spam messages, 737 incidents dealing with malware and 48,000 malicious URLS, (all having bearing with COVID 19) were detected by the agency (The Guardian, August 4,2020).In the same vein, during the lockdown, particularly, on June 10, 2020, Nigeria's notorious inter hacker, Raymond Igbalode popularly known as Hushpuppi and his colleagues were arrested by Interpol in the United Arab Emirate in connection to fraud and money laundering of over 100 Million US dollars meant for unemployed American citizens to cushion or ameliorate the effect of the pandemic as well the 35 Million US dollars ventilator scam.

Citation Information: Nabiebu, M., & Akpanke, S.A. (2021). Covid-19 pandemic and anti-cybercrimes crusade in Nigeria: Changing the narratives for a better enforcement regime. Journal of Legal, Ethical and Regulatory Issues, 24(7), 1-14

Factors that Inhibit Nigeria's Response to Cybercrimes Combat during COVID-19 Pandemic

It is not in doubt that COVID-19 has ravaged the global space, leading to exponential increase in cybercrimes across the universe without exception to Nigeria (Europol's Cybercrime Report of October 5, 2020). Just like other countries of the world, Nigeria responded to this new normal via a multi-sectorial approach. On October 8, 2020, the Economic and Financial Crimes Commission secured the conviction of four cybercriminals before Justice Simon Amobeda of the Federal High Court, Calabar Division, Cross River State (efccnigeria.org).However, much have not been achieved in the fight against cybercrimes particularly in the COVID-19 milieu as a result of certain factors. Firstly, it is not polemical that, cybercrime is a contemporary, dynamic and sophisticated criminal activity which usually involves very smart and intelligent people who possess an unfettered mastery and understanding of their devious game. It therefore requires a skilled, eclectic and dauntless investigator or expert with a better and potent understanding of the tools and techniques to track them down and prove their guilt (Saraki, 2020). Nigeria has been appellate as the largest and most populated Black Country in the world with a population estimated to be over 207 million people (Worldometers Report, 2020). Recent study shows that Nigeria is the hotspot of cyber cybercriminals, without a corresponding number of cybercrimes experts in the country (Mordi, 2019). It is trite that while the number of cybercriminals in the country increases geometrically every year, the number of counter-cybercrime enforcement personnel (specialists) increases arithmetically thus leading to an in balance in the ratio of cybercriminals Vis a Vis counter-cybercrimes experts. The COVID-19 pandemic has further compounded the situation because a large number of these personnel have been diverted from investigating cybercrime offence to supporting the government in her quest of containing the spread of the virus. They have been redeployed to other sectors such as quarantine enforcement, isolation centers, contact tracing, state and communication borders etc. To worsen the whole situation, a lot of the personnel have either died as a result of the virus or even contacted same and ipso facto, ill. This has affected negatively, the capability of states to counter new and increasing cybercrimes threat.

An appendage of the challenge of absence or inadequate counter-cybercrimes experts or personnel is inadequate or absence of sophisticated machines or instruments to combat cybercrimes in Nigeria. This is as a result of poor funding or inadequate budget on counter-cybercrimes and artificial intelligence. The Nigerian government considers cybersecurity as a luxury rather than a necessity and its importance is far from being recognised and appreciated. It has also been reported that, cybersecurity budgets in many organizations are less than 1% and some instances, zero allocation. The inadequacy or absence of these modern technological tools makes it difficult or impossible to track down, arrest, prosecute and convict cybercriminals in the country while the same criminal nuisance are easily track down in other countries that have modern and sophisticated gadgets. For instance, a few months ago, some Nigerians (cybercriminals) who engage in the habit of targeting U.S businesses and individuals in wire frauds were sanctioned by the U.S Treasury Department over allegations of cybercrimes. In the same week, a young Nigerian celebrity, who was recently featured in one of the world's famous known as Forbes Magazine's "*30 under 30*" pleaded guilty to cyber fraud involving over $11m

Citation Information: Nabiebu, M., & Akpanke, S.A. (2021). Covid-19 pandemic and anti-cybercrimes crusade in Nigeria: Changing the narratives for a better enforcement regime. Journal of Legal, Ethical and Regulatory Issues, 24(7), 1-14

USD in Virginia. Also, some Nigerians, including Huspuppi were reported to have been arrested in the United Arab Emirates for allegedly committing cyber fraud in excess of $35m USD, by allegedly illegally diverting money from a fund set up to combat the negative effects of Covid-19 (Saraki, 2020). These reported cases have further brought to fore the inherent inadequacies that characterize Nigeria's institutional architecture for cybercrimes combat.

In addition, Nigeria's anti-crime architecture has over the years been bedeviled with high level of corruption and greed. Bribery in the country has not only become a routine practice but also an integral part of the DNA of her citizens including her institutions. Many persons perceive it as the shortest and surest way of accumulating wealth. Most often, the statutory allocations for cybercrime combats are either syphoned by the ruling class for their personal gains or used to buy little or inferior gadgets with little or no use. For example, in July 10, 2020, the Chairman of Nigeria's anti-graft agency, the Economic and Financial Crimes Commission was suspended by President Muhammadu Buhari on grounds of corruption, re-looting of recovered funds and breach of public. This finds solace in the unanswered question, who watches the watch dog? In some instances where cybercriminals are arrested, they pay huge sums of money to administrative institutions in order to ensure their release and acquittal. This practice became more prominent in the wake of COVID-19 pandemic. For example, on August 7, 2020, the Economic and Financial Crimes Commission arrested 32 suspected cybercriminals (mostly NYSC members and undergraduates) at Ibadan, Oyo State capital (This Day Newspaper of August 12, 2020). Till date, nothing progressive has been done about the arrested suspects thus leading to the conclusion that money has changed hands. During the lockdown occasioned by the pandemic, the federal government through the Central Bank of Nigeria injected into the economy billions of naira to cushion the effect of the economy. These monies were budgeted for the provisions of palliatives to the vulnerable, small and medium enterprises and revamp the health sector. It is quite pathetic that the palliatives did not get to the vulnerable persons but ended up in the hands of a microscopic few, namely politicians and their cronies. Thus, on September 29, 2020, the Independent Corrupt Practices and other Related Offences Commission discovered that the sum 2.6 billion naira being monies meant for school feeding programed during the COVID-19 lockdown were diverted into personal accounts(The Vanguard of September 29, 2020)

Poverty, unemployment and undying quest for wealth also negate Nigeria's efforts to tackle cybercrimes. The 2020 report of the National Bureau of Statistics (NBS) is to the effect that, 40 percent of the Nigerian population, that is, 82.9 million people live below its poverty line of 137,430 naira ($381.75) a year (NBS Report, 2020). This finding is in consonance with the 2019 reports of United Nations Development Programmed (UNDP) and the Oxford Poverty and Human Development Initiative (OPHI) that Nigerians are multi-dimensionally poor. It has also been reported that Nigeria's unemployment and underemployment rate as at second quarter of 2020 is 27.1% and 28.6% respectively (NBS Report, 2020). In effect, 57.7% of the country's populations, that is, over 100million people are either unemployed or underemployed in Nigeria. Underemployment refers to an employment relationship where one's job does not truly reflect his or her actual training or financial needs. A lot of people graduate from universities and other institutions without being employed by the government. They are allowed to room the streets and cannot carter for their families. This serves as a disincentive to the younger generation who no longer sees education as a viable instrument

Citation Information: Nabiebu, M., & Akpanke, S.A. (2021). Covid-19 pandemic and anti-cybercrimes crusade in Nigeria: Changing the narratives for a better enforcement regime. Journal of Legal, Ethical and Regulatory Issues, 24(7), 1-14

for changing the world but patronize cybercrimes as a better platform for survival and accumulation of wealth. The combine implication of this gross poverty and unemployment/underemployment is that it has led to an exponential increase in crimes and cybercrimes in the country. Thus, people strive to make a living or better their standard of living.

Another factor that accounts for the Nigeria's dismal response to cybercrimes in the COVID-19 arena is the skewed nature of her justice system. By justice system, we mean, the police, courts and prisons (Shehu et al., 2017).The roles of these three pillars of justice system cannot be overemphasized. It is elementary law that, the police are responsible for the protection of the lives and property of all individuals in the country. It receives complaints, call for help or redress against any injustice. Courts which are creatures of statutes and made of judges, magistrates, registrars etc are saddled with the responsibility of interpreting laws, settlement of disputes as well as the last hope of the common. The Nigerian justice system has been clouded by several problems as delay in police investigations, overuse of prison sentences by the courts, non-adherence to the complainant, accused and prisoner rights, prisons congestions, and shortages of funds to the components of the system. The system has the over years, suffered a refuting neglect leading to near total decay and culminating into several other linked problems, while there is a geometric increase in the population of the country without a commensurate increase in related facilities/infrastructures and services. Nigeria's criminal/civil justice system is, therefore, not up to the reality in relation to the enormity of its dynamic and institutional roles alongside the endemic problems it is facing. For example, up to this moment, issues of forensic investigations, tests and analysis are either not or poorly conducted, which are a great material for the justice system to rely on. The system upholds technicalities rather than substantial justice. This has led to delay in the trial and implied abandonment of cases. There is also lack of modernity or digitalization in the conduct of judicial proceedings. Nigeria still upholds analogue judicial proceedings despite that the world is in a digital age. This absence of digitalization hindered the effective conduct of judicial proceedings as well as cybercrimes trials in the wake of the pandemic as courts could not sit physically as a result of the physical distance whereas in other climbs, recourse was made to virtual proceedings without hitches.

CONCLUSION AND RECOMMENDATION

The COVID-19 pandemic took the world by storm with high thundering consequences. It has threatened and altered man's existence and lifestyle. There is a paradigm shift or migration from analogue to digital way of life as a way of containing the spread of the virus. A quite number of people whose figure reads in millions have been confined to their homes and forcefully subjected to school, work and trade online through various digital platforms within the fintech landscape. Although this has led to a decline in street crimes but it has led to an unwarranted increase in cybercrimes across the globe. In Nigeria, the situation became worst as a result of the inherent and systemic corruption that runs in her DNA, absence or inadequate counter-cybercrimes experts and instruments, greed and undying quest for wealth, unemployment and poverty. These factors have led to poor performance and enforcement of anti-cybercrimes policies in the country. Indeed, the pandemic has scientifically and mathematically exposed the lapses and skewed nature of Nigeria's legal and administrative framework for

Citation Information: Nabiebu, M., & Akpanke, S.A. (2021). Covid-19 pandemic and anti-cybercrimes crusade in Nigeria: Changing the narratives for a better enforcement regime. Journal of Legal, Ethical and Regulatory Issues, 24(7), 1-14

cybercrimes combat. As a panacea to these menaces, we must individually and collectively rekindle and totally restructure our education system to be more pragmatic, realistic and in tandem with global reality. This pragmatic system of education should be anchored on the proper use of skills to the betterment of the society rather than emphasis on mere possession of certificates. This overhauling of the education system must be inclusive; the private sector must work in pari pasu with educationists and policy makers for a needs assessment so as to create an enabling environment where institutions will produce graduates that fit into the industry. Youths should be encouraged and financially supported by the government, private individuals as well as non-governmental organisations to venture and invest in agriculture, mining, creative industry, tourism and information technology sectors. By doing, they become self-dependant rather than clamour for white collar jobs, which the government hardly provides. This is the best antidote to the high level of unemployment, underemployment and poverty that characterises Nigeria's economic system.

Also, our law enforcement agencies should be holistically reformed. Thus, more cybercrimes experts should be employed by the government. Apart from employment of cybercrimes personnel, government should ensure that they are trained regularly on the use on modern machines and technology on counter-cybercrimes. The expenses and welfare packages for the training are to be borne by the government. Government should also partner with foreign countries and non-governmental organisations for a free exchange of flow of artificial intelligence and revamp of the legal and regulatory frameworks on counter-cybercrimes in the country. Government should ensure that sufficient funds are budgeted towards cybercrimes combat and modalities must also be put in place to ensure the proper utilization of the budgeted funds. Any person who misuses such funds should be brought to face the wrath of the law. Law enforcement agencies and the judiciary should change the narratives by ensuring that there is a fast track process and procedure for effective and timely determination of cases involving cybercrime as obtained in other climes. This will change the international perception about Nigeria as a country that lacks a transparent, efficient and prompt justice system.

Finally, it is our collective responsibility that persons with questionable wealth should not be given recognition in the society. This will encourage hard work, responsiveness amongst youths and make them not to take cybercriminals as their role models.

REFERENCES

CBN. (2020). *Circular on policy measures in response to COVID-19 outbreak and spill* overs. Retrieved from https://www.cbn.gov.ng/Out/2020/FPRD/CBN%20POLICY%20MEASURES%20IN%20RESPONSE%20TO%20COVID-19%20OUTBREAK%20AND%20SPILLOVERS.pdf

Choucri, N. (2016). *Institutions for cyber security: International responses and data sharing initiatives.* Retrieved from http://web.mit.edu/smadnick/www/wp/2016-10.pdf

Deloite. (2017). 2017 Nigeria cyber security outlook. Retrieved from https://www2.deloitte.com/ng/en/pages/risk/articles/2017-nigeria-cybersecurity-outlook.html#:~:text=In%20Nigeria%2C%20several%20organizations%20suffered,which%20represents%20about%20N127%20billion

Europol's Cybercrime Report. (2020). Retrieved from https://www.europol.europa.eu/newsroom/news/covid-19-sparks-upward-trend-in-cybercrime

Gross, G. (2018). *The cost of cybercrime.* Retrieved from https://www.internetsociety.org/blog/2018/02/the-cost-of-cybercrime/

Citation Information: Nabiebu, M., & Akpanke, S.A. (2021). Covid-19 pandemic and anti-cybercrimes crusade in Nigeria: Changing the narratives for a better enforcement regime. Journal of Legal, Ethical and Regulatory Issues, 24(7), 1-14

Mordi, M. (2019). *Is Nigeria really the headquarters of cybercrime in the world?* Retrieved from https://guardian.ng/news/is-nigeria-really-the-headquarters-of-cybercrime-in-the-world/#:~:text=Nigeria%20has%20an%20international%20reputation,world%2C%20if%20not%20the%20biggest.&text=And%20as%20of%202013%2C%20according,fraudulent%20transactions%20in%20the%20world.> accessed 8th October, 2020 NBS Report, 2020

Park, A. (2020). *Economic consequences of the COVID-19 outbreak: The need for epidemic preparedness*. Retrieved from https://www.frontiersin.org/articles/10.3389/fpubh.2020.00241/full

Rahaman, M.A. (2016). *Cybercrime affects society in different ways*. Retrieved from https://thefinancialexpress.com.bd/views/reviews/cyber-crime-affects-society-in-different-ways

Saraki, B.A. (2020). *Nigeria: Cyber criminals-Confronting the few who dent many*. Retrieved from https://allafrica.com/stories/202007010079.html

Shehu, M.I., Othman, F.M.B., & Osman, N.B. (2017). Nigerian judicial system: The ideal, hope and reality. *Journal of Management Sciences, 15*(3), 105-120.

Welcome, M.O. (2011). The Nigerian health care system: Need for integrating adequate medical intelligence and surveillance systems. *Journal of Pharmacy a Bio Alied Sciences, 3*(4), 470-478.

World Economic Forum Report. (2020). Retrieved from https://www.weforum.org/agenda/2020/06/3-ways-governments-can-address-cyber-threats-cyberattacks-cybersecurity-crime-post-pandemic-covid-19-world/

Worldometers Report. (2020). Retrieved from https://www.worldometers.info/world-population/nigeria-population/

Citation Information: Nabiebu, M., & Akpanke, S.A. (2021). Covid-19 pandemic and anti-cybercrimes crusade in Nigeria: Changing the narratives for a better enforcement regime. Journal of Legal, Ethical and Regulatory Issues, 24(7), 1-14