

**History of Article**

Submitted: February 17, 2021

Revised: March 12, 2022

Accepted: April 23, 2022

Available Online since: April 30, 2022

VOLUME 3 ISSUE 2, APRIL 2022

Editor in Chief:

[Assoc. Prof. Dr. Indah Sri Utari, S.H., M.Hum](#)

*Universitas Negeri Semarang, Indonesia*

Associate Editors:

[Prof. Ngboawaji Daniel Nte, Ph.D.](#)

*Novena University, Nigeria*

[Assoc. Prof. Frankie Young, Ph.D.](#)

*University of Ottawa, Canada*


**How to cite:**

Nte, Ngboawaji Daniel, Brebina Kelvin Enoke, and Joda Adekunbi Omolara. "An Evaluation of the Challenges of Mainstreaming Cybersecurity Laws and Privacy Protection in Nigeria". *Journal of Law and Legal Reform* 3, No. 2 (2022): 243-266. <https://doi.org/10.15294/jllr.v3i2.56484>.

© 2022 Authors. This work is licensed under a Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0). All writings published in this journal are personal views of the authors and do not represent the views of this journal and the author's affiliated institutions. This title has been indexed by [Science & Technology Index \(SINTA 3\)](#), [Directory Open Access Journal](#), [Google Scholar](#), and [GARUDA](#)

Type: **Research Article**

# An Evaluation of the Challenges of Mainstreaming Cybersecurity Laws and Privacy Protection in Nigeria

Ngboawaji Daniel Nte<sup>1</sup>✉, Brebina Kelvin Enoke<sup>2</sup>, Joda Adekunbi Omolara<sup>3</sup>

<sup>1</sup> Department of Intelligence and Security Studies, Novena University Ogume, Delta State, Nigeria

<sup>2</sup> Faculty of Law, Niger Delta University, Wilberforce Island, Amasoma, Bayelsa State, Nigeria

<sup>3</sup> School of Postgraduate Studies, Department of Intelligence and Security Studies, Novena University, Delta State, Nigeria

✉ [profdnte@novenauniversity.edu.ng](mailto:profdnte@novenauniversity.edu.ng)

## ABSTRACT

The goal of this study is to discuss cybercrimes and review cybersecurity threats, with a focus on cybersecurity legislations in Nigeria that seek to protect the privacy and digital property of the Nigerian people and the country's institutions. The study's methodology includes a qualitative examination of Nigeria's present national cybersecurity laws. It explores how effective they are and interrogates the additional measures that may be needed-notably in cybersecurity and related national laws-to ensure that individuals, institutions are protected and that society and the national economy function well in the 21<sup>st</sup> Century. Individuals have a right to privacy, so do companies and various other institutions in post- modern societies. This right varies widely across different countries across the globe. In some countries it is minimal or non-existent, in others it is hard fought for constitutional right. In order to reap the benefits of advanced technologies in the information age, personal and institutional data have to be made available to merchants, institutions and government. The benefits of advanced technologies are immense-and vital to modern economies. However, this process involves risks. Abuse of the data is a risk, and criminal abuse has become widespread.

**Keywords:** *Cybersecurity, Data Privacy Protection, Nigerian Legal System, Law Enforcement, Criminal Law*

## INTRODUCTION

According to Wikipedia, the constitutions of over one hundred and fifty nations mention the right to privacy.<sup>1</sup> This is instructive to highlight the global interest in privacy laws as it remains one of the fundamental human

---

1. ^ "Read about "Right to privacy" on Constitute". [constituteproject.org](https://constituteproject.org). Retrieved 31 March 2018.

rights so far. Most times a country's ability to maximise the cyber benefits and protect citizens' privacy results in a trade-off. Cybersecurity laws therefore are put in place to combat cybercrime which has the potential to infringe on citizens' and institutions' privacy, and digital property.<sup>2</sup>

The threats of Cybercrimes are global in nature. They are perpetrated electronically and seriously impact the national economy and security of every nation. With the rapid growth globally of electronic platforms and communications, often replacing now vulnerable "old technology" systems, there has been a huge surge in (a) the number and (b) types of cybercrimes. Hence the need for countries to invest significantly in cybersecurity measures-and to draft and pass appropriate laws to protect privacy rights, digital property and related assets.

Experts have identified some the key issues on the subject of cyber security. Among these are the reality that technological changes are occurring at an unprecedented rapid rate. Although they benefit the global economy in many positive ways, electronically based abuses are growing at a faster rate than protective cybersecurity systems can be put in place. Private sector solutions (protections and solutions) are available, at a price, but are not available to all.

In looking at cybersecurity related institutions and policies in Nigeria in terms of cybercrime related issues, we had posed some intriguing questions such as: (a) where Nigeria stands when it comes to a national policy of ensuring data privacy and (b) the types of initiatives our national policies could be taken to improve the way we approach both the threats to our privacy as well as opportunities to improve our cybersecurity laws and their equitable implementation. The preponderance of Cyber-based technologies cannot be over emphasised as they dominate the political, social and economic space of modern society. The cyber world encompasses the world of computers and computer networks involving a wide range of electronic devices and currently rules the entire global socio-

---

<sup>2</sup> citation: Various internet sources.

economic and political spectrum. It is globally acknowledged to be a multi-trillion dollar “industry”.

Cybersecurity laws are put in place to protect privacy, data and other information that individuals and institutions (private sector firms and governments) wish to be kept private. They cover almost every aspect of modern economies and societies. They include confidential information required for the proper operation of hospitals, schools, banks, merchants, government services, private institutions as well as personal information stored by households and individuals.

The perpetrators of cybercrimes can be categorized in a number of ways. They include:

1. State-sponsored agencies (the literature often cites Russia; Iran; North Korea and China, but it is probable that all countries engage in cybercrimes to some extent). For example, alleged Russian interference in the 2016 U.S. presidential elections.
2. Entrepreneurial cybercrimes: these can be institutional (e.g. otherwise legitimate banks profiting from money laundering fees) or private individuals (e.g. random hackers and ransomware pirates) or organised crime (e.g. mafia, gangs and terrorist organizations).

Cybersecurity is put in place to combat crime in cyberspace. The use of the internet globally has grown exponentially in the past years and has become increasingly popular with each generation.

The growth of cyberspace comes with an increased risk of various types of cybercrimes being carried out. With this, it has become extremely important for the right measures to be put in place to combat these crimes and that’s where cybersecurity is relevant. The world's economy loses over 500 billion in monetary value yearly.<sup>3</sup> Thousands of jobs are lost in the United States due to perpetration by cyber criminals. A Lot of livelihoods are put at stake when private data is intercepted and used for illegal actions. A kind of cybercrime known as the “Business Email Compromise

---

<sup>3</sup> Nigeria Communications Commission - Department of New Media and Information Technology

" is one of the ways in which companies have been compromised over the years.

When an attacker gains access to a company's email account and impersonates the legitimate owner in order to dupe the firm, its customers, partners, and/or workers into sending money or sensitive data to the attacker's account, this is known as business e-mail compromise (BEC). A Nigerian scammer known as Ramon Olorunwa Abbas aka Hush Puppy received a wire transfer fraudulently of over \$922,000 through this means for which he is currently facing indictment.<sup>4</sup>

The final reports of the Nigeria Communications commission's shows that there has been no decrease in the Global Economic Crisis over the years. There has been an evolution in the sophistication of cybercrime and the volume of crime. Toolkits have been created which now help facilitate cybercrime as well as Web browsers and plugins. Attacks are now being perpetrated from the developing world such as India, Nigeria, and Ghana to the developed world like the US and UK due to the low possibility of being apprehended.<sup>5</sup> The effect of cyberterrorism has affected so many countries over the years and Nigeria is not an exception. Reports indicate that it cost Nigeria N127 Billion alone in its GDP<sup>6</sup>. Effects of cybercrime affect the bank sector, foreign direct investments, stocks, safe use of the internet without theft of personal details and harassment.

## THEORETICAL BACKGROUND & LIMITATIONS

### *A. Cybersecurity*

---

<sup>4</sup> <https://www.bloomberg.com/features/2021-hushpuppi-gucci-influencer/>

<sup>5</sup> *Ibid.*

<sup>6</sup> *Ibid.*

Cybersecurity are measures put in place to protect cyberspace from unauthorized access, cyber terrorism and extremism. This was born as a result of cybercrimes which are of various kinds. A good cybersecurity policy secures critical and sensitive data and prevents it from falling into the hands of malicious parties. One will ask that when it comes to security and privacy, which should come first. When you really think of it, how will a nation function if the citizens have lost trust and hope in their country? We tend to wonder whether or not Nigeria's cybersecurity put in place can actually protect its citizen's privacy. It is difficult for any nation to 100% guaranty the privacy of its citizens especially in the age of cyberterrorism as well as cyberwarfare. The rights to privacy deserve protection. In this respect, Nigeria has a long way to go.

### *B. Privacy*

Privacy or rather the right to privacy is an element of various legal traditions to prevent Governmental and private entities from threatening the privacy of individuals. Globally, we have over 150 national constitutions that mention the rights to privacy including the Nigerian 1999 Constitution as amended.<sup>7</sup> The United Nations General Assembly adopted the Universal declarations of human rights (UDHR) in 1948 which was originally written to guarantee individual rights of everyone globally. It states that:

*"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks"*

There have been numerous debates on whether there can be privacy in this era with the capabilities of security agencies being able to gain access to private information of individuals for one reason or another. Major

---

<sup>7</sup> [https://en.wikipedia.org/wiki/Right\\_to\\_privacy](https://en.wikipedia.org/wiki/Right_to_privacy)

arguments raised by governments in the UK and Australia to justify the increase of government surveillance hereby infringing on the digital privacy of its citizens is the need to protect its citizens from harm by preventing and responding to threats to national security more efficiently. Is it truly an infringement if the ultimate purpose is to safeguard both individuals and cyberspace? Surveillance and data collecting on individuals is necessary for cybersecurity and the prevention of cybercrime in order to ensure the security of the state, but I feel that privacy rights should also be considered at this time.

Interestingly, Russia's cyberspace is way ahead when it comes to cybersecurity. Other nations such as the U.S, most of the European Union and others view privacy as way more important than security and continuously go back and forth on what should take importance. Due to issues of extremism, cyberterrorism and cyberwarfare, Russia perceives cyberspace as a threat to Russian security and stability.

Russia openly placed the security of the nation ahead of privacy and also changed regulations influencing their cyberspace to a more sovereign one. Yes, there has been widespread criticism about these regulations but they must be doing something right as they appear to be the leading power in terms of Security over other western powers and obviously Nigeria. In recent times, Nigeria has faced several security threats from different Extremist groups and terrorist cells with a lot of their operations happening over cyberspace and the *cyberverse* (i.e. cyber universe). It is my opinion that Nigeria has a long way to go to ensure that its citizens are not prone to privacy infringement.

We don't have to go to the extreme to deal with cybersecurity threats but we should do everything reasonably possible to combat them. There are times that while also protecting the privacy of its citizens, data could be collected hence also in a way privacy is stepped on.

When it comes to cybersecurity and privacy there are certain things to keep in mind and there are:

1. Sometimes security comes at a cost to privacy.

2. Privacy requires cybersecurity in order to limit access to Individuals personal data. So, although cybersecurity may infringe on privacy at certain times in society, it is also essential to ensure privacy in the long run.
3. Cybersecurity helps to achieve privacy and vice versa.

In aggregate, they are not necessarily contradictory, as one is required in certain cases for the other to function properly, but in the case of a significant threat to national security in connection with cyberspace, cybersecurity should take precedence over individual privacy. The reaction is determined by the level of threat.

### *C. Cybercrime*

The world as we know it now is a global village. The internet has caused a worldwide transformation since its use began. With the use of the internet becoming popular each day, so has cybercrime. Cybercrime is any form of crime that happens in cyberspace. In order for us to talk about privacy and whether or not it should be considered in this age of insecurity in Nigeria we have to look at the causes of cybercrime as well as the different types of cybercrime.

At the early stages of cybercrime in the country as well as West Africa, there were poor attitudes shown towards doing anything to put an end to these scammers. There are a number of people in recent times that have turned to cybercrime over the years. The increasing rate of this practice has become alarming and they are mostly as a result of greed, the want to get rich fast, vast unemployment and lack of interest in Education. A lot of these cybercriminals have spread to other parts of Africa due to the ECOWAS free travel protocol. The people who participate in these crimes are:

1. Smart and skilful youths who instead of pursuing an education or having a reputable career have decided that all they need to live a happy life is to make money at any cost.



2. Insiders at financial institutions that know how these institutions work and how it can be manipulated for their benefits.
3. People with connections to foreigners who can aid them in the carrying out of these crimes.
4. Insiders in security agencies.

The type of people that participate in these kinds of crimes are not limited to these few named here. Cybercrimes can be committed against persons in the form of bullying, online trafficking, child pornography and so on. It can also be committed against the government. This manifests itself mainly in the form of cyber terrorism. So, let's break down the types of cybercrime in order to understand the attacks the country faces.

1. **Cyber Terrorism:** A cyber terrorist is someone who undertakes an attack on a government or organization in order to get access to data on computers or their networks. He is also someone who intimidates a government or advances their own political or social agenda by initiating cyberattacks against computers, networks, and information stored on them. It is an act of terrorism done through cyber space (cyberverse) or a worldwide system of interconnected computers. It means that any hostile act intended to generate terror or panic by gaining access to any useful information in companies or government bodies through the use of a computer and the Internet is commonly referred to as cyber terrorism.<sup>8</sup> Cyber extortion is another type of cyber terrorism that occurs when hackers illegally gain data or sensitive information that they use to extort organizations and individuals and hold them hostage until their demands are met. Cyber extortionists are increasingly targeting corporate organizations, websites, and networks, crippling their ability to operate on a regular basis.
2. **Cyber Stalking:** This is the use of the internet to harass and intimidate people on a regular basis. In this day and age of social media, a great number of people post every detail about themselves online, and this information is easily accessible to anyone who wishes to view it. As

---

<sup>8</sup> Journal of Law, Policy and Globalization [www.iiste.org](http://www.iiste.org) ISSN 2224-3240 (Paper) ISSN 2224-3259

expected, this is accompanied by bullying, stalking, harassment, and so on. They can take the shape of sexual harassment, racism, or just plain rage.<sup>9</sup>

3. **Malware:** These are software programs that obtain unauthorized access to your computer. Viruses and Trojan horses are examples of them. These programs are designed to harm a network or a machine.<sup>10</sup>
4. **Fraud & Identity Theft:** This entails lying on purpose in order to get information and identity illegally. This is one of the many cybercrimes that are prevalent in Nigeria, and it is referred to as Yahoo. Those engaging in cybercrime in Nigeria use the internet to deceive, defraud, and steal people's identities.
5. **Drug Trafficking:** It has become common for drug traffickers to conduct their illegal drug sales online. They have used numerous technical techniques to sell illegal narcotics via the Internet. The surge in buying and selling drugs on the Internet could also be due to the fact that most people now live on their phones. This new discovery has made it easier for introverted people to obtain these Substances.

## LAWS IMPLEMENTED TO DEFEND AGAINST CYBERCRIME

The Cybercrime (Prohibition, Prevention) Act 2015 is Nigeria's major cybercrime law. Prior to this, there was no unique legislation dealing with cybercrime hence protecting the privacy of individuals in the country, however there were other laws that were helpful in combating cybercrime, which we will go through in detail.

1. **THE EFCC Act:** Before the passage of the Cybercrimes Act of 2015, the Economic and Financial Crimes Commission (EFCC) Act was the law in place to prosecute people who committed cybercrime in the

---

<sup>9</sup> The International Journal of Engineering And Science (IJES) | Volume | 2 | Issue | 4

<sup>10</sup> *Ibid.*

country.<sup>11</sup> This was due to provisions in the Act that dealt with cybercrime. It stipulates that:

The Commission (Economic and Financial Crimes Commission) established under the EFCC Act shall be responsible for the enforcement and proper administration of the Act's provisions, as well as the investigation of all financial crimes, including advanced fee fraud, money laundering, counterfeiting, illegal charge transfers, futures market fraud, fraudulent encashment of negotiable instruments, computer fraud, and computer piracy.<sup>12</sup>

This Act established a broad range of rules covering all sorts of internet-related crime, granting it the authority to combat and prosecute individuals found guilty of committing these crimes. This made a significant contribution to cybersecurity at a period when there was no specific regulation addressing cybercrime.

2. **Money Laundering (Prohibition) Act:** This Act makes it illegal to launder proceeds from illegal funds. It specifies that no individual or corporation may accept a cash payment in excess of \$5,000,000 for individuals and \$10,000,000 for corporations unless the payment is made through a banking institution. Any such transactions must be disclosed within seven days to the CBN or the EFCC. This aims to prevent cybercriminals from using financial institutions to launder money and fuel illegal operations. When money is laundered for terrorist purposes, the transaction's bearer's identity should be made public and reported to the proper authorities. Privacy should be compromised for the benefit of security in this case.

This Act concerns cybersecurity and how cybercrime is prosecuted, notably in financial organizations. The EFCC is also in charge of enforcing the provisions of this Act.

3. **The Criminal Code Act:** This Act does not specifically address cybercrime because it predates the internet and dates back to colonial times. Under this statute, every sort of theft, as well as false pretences,

---

<sup>11</sup> Journal of Law and Criminal Justice June 2020, Vol. 8, No. 1, pp. 30-49

<sup>12</sup> Economic and Financial Crimes commission Establishment act (2004)

is a criminal offense. Because cybercrime is committed under the pretext of a legal business, those who perpetrate cybercrime under the guise of a legitimate business can be penalized under this Act. It states that any person who obtains anything capable of being stolen, or forces someone to obtain anything that could be stolen or pays for or delivers anything that is said to have been stolen or gotten with trickery or pretences is guilty of a misdemeanour.<sup>13</sup>

This part of the Criminal Code is specifically for internet fraudsters who use false pretences to swindle people. This is one of many laws that addressed cybercrime before the Cybercrime Act of 2015 made it explicit.

4. **The Penal Code Act:** Despite the fact that it does not explicitly indicate that it deals with cybercrime, this Act is used to prosecute cyber offenders and defend cybersecurity in Nigeria. Sections of the Penal Code, such as Section 362 of the Penal Code, are used to prosecute cyber criminals who engage in counterfeiting and forgery. This Act only applies to the northern area of Nigeria.

**Section 362** of the Penal Code says that a person who with the intent to be dishonest signs, seals or execute a document with the sole intent to deceive other individuals that they have the capacity to sign such document or without the proper authority alters a document to deceive others into believing that the falsified document s real commits forgery.<sup>14</sup>

**Section 320** of the Penal Code also provides that whoever by deceiving a person induces the person who has been misled to give any property to a person in a fraudulent or dishonest manner or intentionally convinces the person deceived to do or omit doing anything that he would not do or avoid doing if he were not so deceived and such act or omission causes or is likely to cause damage to that person in body, mind, reputation, or property is said to cheat<sup>15</sup>.

---

<sup>13</sup> Criminal Code Act

<sup>14</sup> Section 362 of the Penal Code Act

<sup>15</sup> Section 320 of the Penal Code Act

This section can be used in areas of deception in cybercrime. The area of inducement as seen in this section is seen most especially in the area of cyber terrorism.

5. **The Terrorism (Prevention) (Amendment) Act 2013:** Although this Act was not intended primarily for the purpose of cybersecurity, it can be used in certain cybersecurity situations, particularly those involving cyber terrorism and other terrorist acts committed online. This Act was abolished in 2011 to incorporate regulations for terrorist financing offenses.

**Section 1 (b)** of this Act says that any individual or company who, whether inside or outside the country, deals directly or indirectly in any act of terrorism, commits an act preparatory to or in furtherance of an act of terrorism, fails to do what is necessary to prevent terrorism, aids or facilitates the activities of individuals involved in terrorist acts, or is an accessory to any offence under this Act, helps, facilitates, or organizes any act of terrorism once convicted is punishable by death.<sup>16</sup>

Several authorities in Nigeria, including the EFCC, the Department of State Security, and the Nigerian Police Force, have the authority to pursue these offenses. With the harsh fines imposed here, it is clear that the country has zero tolerance for terrorism and that when it comes to privacy or the battle against cyber terrorism, the fight against cyber terrorism should always take precedence.

6. **The Nigerian Evidence Act 2011:** Before this Act was created, computer generated evidence were inadmissible in the Court of Law. It was unsure under the old act whether or not evidence generated via computer were primary or secondary evidence. The 2011 Evidence Act brought about the admissibility of such evidence.

Although this act came to be, a lot of cybercriminal activities online were still unchecked and this was due to the fact that the different crimes like hacking, Email hacks, pin theft and so on were

---

<sup>16</sup> Section 1 (b) of The Terrorism Act 2013

not identified and given proper penalty in the Act. There were also no designated courts or agencies put in place to prosecute cybercrime. The Cybercrime Act coming into force changed all that and was able to cover a wider range and punishment for cybercrime.

## THE NATURE OF THE PROBLEM

The security threats that the nation faces these days have drastically evolved. A lot of these threats are on the cyberspace which means that criminals have evolved hence the need for our laws and implementation to evolve alongside its threats. The country faces numerous threats from various cyber criminals. Many industries are under attack for its large amounts of data especially the banking sector. A proper cybersecurity solution and implementable laws could deal with a lot of these issues.<sup>17</sup>

The cyberspace is ever expanding which makes the prediction and the prevention of criminal activities on the cyberspace hard to deter. These activities are growing twice as much as the activities outside the cyberspace such as infiltration of banking mainframe, illegal access to password and sensitive information's, funding criminal activities.

In Nigeria's security system, cybersecurity seems to take the lowest number in the scale of preference of national security. Nigeria has failed to realize that investing in cybersecurity is as much an integral part of the nation's security. Nigeria has created laws to combat the crime but fails in the way of implementation when these laws are actually broken. Different agencies have taken upon themselves the right to implement these laws and have failed. The country lacks the preparedness to handle cybersecurity breaches and needs to work on the right way to dealing with these challenges how the effectiveness of the solutions put in place.

Organizations must also take the extra step to defend their systems and data from attack. The organizations have a somewhat careless attitude towards fortifying their security from cyber-attacks. They need to invest in

---

<sup>17</sup> <https://www.recordedfuture.com>

Information Technology (IT) and training their staff in cybersecurity practices.<sup>18</sup>

## LITERATURE REVIEW

### I. THE RISE OF PONZI SCHEMES IN THE COVID 19 PANDEMIC

Ponzi schemes have become rampant on the cyberspace since the Covid 19 pandemic began. Criminals have resorted to using the internet as a means to defraud people all over the world. In a recent case of *Isaiah vs JP Morgan Chase Bank* in the year 2020, several entities brought a claim against Chase Bank claiming that the bank aided and abetted with the Ponzi scheme.

Apparently, the bank was aware about transactions on the account suspected of fraudulent activities and did nothing to stop it. The bank only closed the account after millions of dollars had gone through the account and still allowed the Ponzi scheme to open a new account to carry on their fraudulent activities. The bank went further by allowing this fraudulent organization officially to wind down and transfer the illegally acquired funds.<sup>19</sup>

Wells Fargo Bank also had a similar case where two individuals created a company that promised great returns to people who invested and went further to pass the money through Wells Fargo bank.

A lot of people fall victim to Ponzi schemes especially since the outbreak of Covid 19 which has left a desperation for people to fend for themselves. People fell for this due to desperation to get rich quick, poverty and loss of job and finances due to the pandemic.

Millions of victims fall to these kinds of cyber frauds every year, especially the elderly and in recent times in hospitals. There have been cases of individuals diverting Covid 19 relief funds as well as duping hospitals. These individuals under the guise of providing equipment's to

---

<sup>18</sup> The International Journal Of Engineering And Science (IJES)

<sup>19</sup> <https://www.natlawreview.com/article/ponzi-scheme-discovery-boom-may-follow-wake-worldwide-economic-contraction-case-law>

these hospitals take large amounts of these money and defraud these hospitals.

A popular case is that of Parris and Santillo who fraudulently acquired millions of dollars from individuals from 2017 and 2018 under the ruse of return on investment via Ponzi schemes. These same individuals went as far as carrying on a huge Covid 19 scam where they gained access to hospital funds through the pretence of proving Covid 19 equipment's to hospitals.<sup>20</sup>

### *A. The Rise of Ponzi Schemes during the Covid 19 Pandemic in Nigeria*

Ponzi schemes go as far back as anyone can remember. With the internet, they have gained traction on the cyberspace. They have been able to reach a large amount of people and during the period of severe uncertainty, a lot of people are looking for the fastest ways to finance their lives and family in order to survive during the pandemic. There are several reasons why people fall prey to these illegal schemes and they are:

1. **Poverty:** Over 40% of Nigeria's population are living in poverty.<sup>21</sup> Due to this, a lot of Nigerians easily fall prey to get quick schemes that they come across on the internet. In a nation where poverty rate is so high, it is no surprise that more people will fall for these schemes hoping to become millionaires overnight. Nigeria is rich in natural resources but a lot of citizens still live below the poverty line. In the current President's second inauguration speech, he promised to lift over 100 million Nigerians from poverty but failed to do even now in 2020.
2. **Lockdown:** The lockdown played a huge role in people falling for Ponzi schemes. In 2020, for example, a 14-day lockdown was put in place in order to curb the spread of the virus. This 14-day lockdown

---

<sup>20</sup> <https://www.justice.gov/usao-dc/pr/georgia-man-pleads-guilty-charges-related-ponzi-and-covid-19-fraud-schemes>

<sup>21</sup> Pakistan Social Sciences Review



that was to end in March then ended in May.<sup>22</sup> The places affected by this lockdown included schools, churches offices and markets. In order to enforce these no movement laws, law enforcement were placed at strategic places to prevent people from moving around unless they were essential workers.

The poor were left to fend for themselves during this time which lead them to look for other means to make money while spending all their time on social media. A lot of get rich quick scheme were advertised online and lot of unsuspecting Nigerians fell prey to this.

3. **Lack of Palliatives (Covid 19):** To quote a reputable source: *“In a bid to slow the rate of spread of the virus, the Federal Government of Nigeria, on several occasions, imposed targeted lockdown measures in areas with rapid increase of Covid-19 cases. The states in which the federal government imposed the targeted lockdown included Lagos, Ogun, and the Federal Capital Territory in Abuja. Some states in the country imposed partial lockdown and closure of interstate boarders. Curfews have also been introduced in all the states nationwide. To alleviate the effects of the lockdown, the Federal Government of Nigeria rolled out **palliative measures** for targeted groups. However, lamentations have trailed the distribution of government palliatives by the masses. Citizens allege that the process of distribution of palliatives had been politicized.”*<sup>23</sup>

This is another reason why people fell prey to get rich schemes during the pandemic. A lot of people living in poverty were left without money making it impossible for them to provide for themselves during the pandemic lockdown. Other countries, such as the US and the UK, provided their citizens with palliatives during the pandemic but although palliatives were donated to Nigeria, it wasn't distributed to the citizens.

A large amount of the hoarded palliatives that were claimed to have been shared to the less privileged citizens were later discovered

---

<sup>22</sup> Pakistan Social Sciences Review

<sup>23</sup> <https://pubmed.ncbi.nlm.nih.gov/32685279/>.

in warehouses across the states. Warehouses full of palliatives were discovered in Kano, Lagos and Osun State just to name a few.<sup>24</sup>

4. **Cyberspace:** In Nigeria, the cyber space is not properly protected letting different kinds of questionable persons to infiltrate the cyber space and use it for criminal activities. Nigeria is the third country in the world of a list of ten with the highest level of Criminal activities taking place online.

With regard to victims, in Asaba Delta State more than 1000 people invested in a get rich scheme with a company called SMART Alban Investment Company SA/FX INVESTMENT GLOBAL LTD ran by a Mr. Smart Alban Ike and lost millions of Naira.<sup>25</sup> The owner of the company went on the run instantly abandoning his company premises which was later sealed off by EFCC.

## FILLING THE KNOWLEDGE GAP

One of the first and most urgent propositions to consider-in relation to closing the knowledge gap-is how Nigeria should protect its most vulnerable citizens. This proposition is not based on “equity” as such, which implies that civil rights are the dominant consideration. Rather, it is based on the need for sound public policies-to protect the economy as a whole, and our social structures.

Vulnerable citizens are those who have little money and protections. In most cases, they cannot afford to buy technological solutions. They are the most vulnerable group when it comes to safeguarding themselves against the impacts of random or targeted cyberattacks. We cannot afford to isolate and abandon some groups in society through what is sometimes regarded as the *Digital Divide*. This refers to the gap between people who have access to modern information and communications technology and those who don't.

---

<sup>24</sup> <https://www.bbc.com/pidgin/tori-54677956>

<sup>25</sup> <https://www.nairaland.com/6496590/sa-fx-ceo-mr-smart-alban>

If Nigeria does not-at a minimum-protect its most vulnerable citizens, it runs the risk of undermining the economy and the country's social structure. If people *en masse* lose confidence in the state, if they are forced to protect themselves, our institutions will be weakened. This is a road to undermining the national economy. Ordinary citizens need to have confidence in Nigeria's monetary system and its various payments systems (including banks, near-banks and entrepreneurial digital payment platforms-which Forbes estimates, globally, collectively are worth over \$19 Trillion annually). Citizens have to see fairness, and be confident in nationwide legislation that "bites", penalizing those who break the law.

Nigeria is not a wealthy country which can afford to "go it alone" in the emerging world of cybersecurity. We simply don't have the trained people or the resources. For now, we have to follow global best practices and fully use commercially available technology.

Focusing, as a priority, on our country's most vulnerable citizens still leaves a huge segment of the economy at risk-notably the private sector and government institutions. As already discussed, there are numerous private sector global companies who are providers or suppliers of protection software. These commercial products have a price but should be used to the maximum. There is a public cost if private sector firms fail to protect their customers. Saying sorry, after mega-hacks of personal data just isn't good enough. Issuing "patches" is not enough. Private sector firms, and governments, have a fiduciary duty to protect their users' privacy. To maintain consumer confidence, we need to consider punitive fines for institutions-and government officials-who are cavalier about this responsibility.

We have to recognise that all laws, anywhere in the world, inevitably lag the crimes and criminal activities which trigger the need for them. In other words, the law typically is reactive, not proactive. It would be unrealistic to imagine otherwise. In Nigeria, we already have many of the institutions necessary to close the time-gap between criminal acts and new legislation. Our challenge is to make sure they are adequately funded and that they function as intended.

We have to recognise that, as grand and well-meaning as it is, the Universal Declaration of Human Rights (UDHR) and similar declarations of citizens' rights, may at the present time be too expensive a luxury when it comes to the rigorous protection of individual privacy. Based on the age-old doctrine-and-practise-of "for the common good" citizens may have to accept some compromises to their individual liberties when it comes to individual privacy. However, this should be very selective.

Structural and political issues arise. For example, *who* decides *what* is for the common good? Who administrates? Who implements—and with what legislative powers? These are dilemmas we will be living with for perhaps many generations. There is no obvious answer. We can be sure of one thing—there will be many dissenting voices. On the other side of things, taking no action will not be excusable.

The second proposition to consider is how to protect privacy, in general, both immediately and over the longer term. In terms of the knowledge gap, this is a question of available resources, the pace at which we educate our citizens and the value we place on the protection of individual and corporate privacy. The *Panama Papers* and the *Cambridge Analytica/Facebook data* scandals have revealed significant structural weaknesses in global policing of institutional crimes, abuse of personal data and lax tax evasion laws. In much the same way as improvements in Nigeria's policing and counter-terrorism infrastructure are a very high priority, so too are vital improvements in our cybersecurity forces—and ensuring that we have cybersecurity laws with teeth.

A third proposition is worthwhile discussing. It's an opportunity. Nigeria has one of the world's youngest populations. Our demographics are both a challenge and huge resource. Despite low average income per capita, our youth is computer savvy. It is adaptable and flexible, and motivated. The technologies that today are a platform for many criminal activities can be re-orientated towards productive activities. We have to discover how, agree a strategy and implement it. It's a huge task, but the potential rewards are immense.

## RESEARCH METHOD

Our mythological thrust is rooted on qualitative approach. This provided a useful way of approaching a very complex and rapidly evolving subject. A substantial level of detailed sources is available in digital form, and we relied heavily online sources to search the literature. We found numerous sources of information on the global situation available from government reports and private sector publications. We also drew on our own experience of the subject, as this was a useful source of identifying some of the items which we enumerated earlier in the work

With regard to information on Nigeria's laws and regulations relating to cybercrime and cybersecurity, we used publicly available online sources, including government websites and several legal platforms which helped explained their purpose and operation. The latter, along with the popular media, also provided useful critiques of the system in Nigeria.

Examples of global best practices and solutions to the conflicts between cybersecurity laws and rights to privacy were found on various platforms, including NGO studies, private sector and government reports. An important source was the Nigerian and global media, which provides a type of "watchdog" role in identifying examples of cybersecurity abuses and failings. These sources were also a valuable source of my discussion of possible solutions that Nigeria could consider adapting and adopting.

## RESULTS & CONCLUDING REMARKS

Our study and analyses found that the benefits of full participation in digital technologies associated with the information age certainly outweigh the costs. They help make our lives easier, they allow economies to function and they provide jobs and numerous social benefits, including better healthcare and improved levels of education.

At the same time, government and the private sector have (a) fiduciary duties and (b) legal responsibilities to protect their citizens and

institutions from abuses of privacy and the protection of data and digital property. Like all laws, the regulatory framework vital to curbing abuses, and penalizing the perpetrators of cybercrimes, typically “lag” behind the crimes themselves. In addition, people and institutions have a responsibility to protect themselves. Cybercrimes such phishing and various other types of fraud have grown rapidly in number and sophistication. Again, with a “lag”, citizens have become more digitally savvy-and this has to continue, as part of closing the knowledge gap.

Nigeria has many of the institutions already in place to provide cybersecurity regulations and to develop appropriate new laws, where required. Not everything can be regulated, thus consumer and institutional education has to be a high priority for our country. Our findings are that the literature shows, however, that not all of the laws that Nigeria has put in place to achieve cybersecurity are managed well. Often, they are policed inadequately-when it comes to enforcement and prosecutions. We can do better.

Closing, and ultimately filling, the knowledge gap between the rapid escalation of cybercrimes and Nigeria’s cybersecurity measures and supporting laws, is a fundamental necessity. Otherwise, our national economy will suffer; social structures will deteriorate and the forces of political instability will grow. Looked at positively, filling the gap will allow our country to attain more of its full potential-as a modern, secure and prosperous digitally-based nation within the global economy.

## REFERENCES

- BBC News: Covid Palliative looting <https://www.bbc.com/pidgin/tori-54677956>
- Blogpost: Naira Land Forum <https://www.nairaland.com/6496590/sa-fx-ceo-mr-smart-alban>

- Bloomberg [2021]: The fall of the Billionaire Gucci Master  
(<https://www.bloomberg.com/features/2021-hushpuppi-gucci-influencer/>)
- Department of Justice [2021]: United States Attorney General’s Office  
(<https://www.justice.gov/usao-dc/pr/georgia-man-pleads-guilty-charges-related-ponzi-and-covid-19-fraud-schemes>)
- Economic and Financial Crimes Commission: The EFCC Act [2004]  
Federal Republic of Nigeria.
- Journal of Law Policy & Globalization [2015] <http://www.iiiste.org> ISSN  
2224-3240
- Maitami.O, Ogunlere.S, Ayinde.S, Adekunle.Y [2013]: The International  
Journal of Engineering and Science-Impact of Cybercrime on Nigeria  
Economy ISSN 2319-1813 VOL 2/Issue 4
- National Law Review [2020]: Ponzi Scheme Discovery boom
- National Library of Medicine: National Centre for Biotechnology  
Information [<https://pubmed.ncbi.nlm.nih.gov/32685279/>]
- Network Security systems LTD: NCC, Effects of Cybercrime on Foreign  
Direct Investment & National Development .Page 11, 12
- Pakistan Social Sciences Review : ISSN (Print)2664-0422  
<https://pssr.org.pk/>
- Penal Code Act: Section 320,362., Federal Republic of Nigeria
- Recorded Future Team [2020]: 2019 Vulnerability Reports
- Terrorism Act [2013]: Sec 1(b), Federal Republic of Nigeria.
- The Nigerian Criminal Code Act , Federal Republic of Nigeria.
- Ufuoma.V.A, Ohwomeregwa.O [2020]: Journal of Law and Criminal  
Justice, Appraising the Laws Governing the control of Cybercrime
- Wikipedia (2021): The right to privacy  
[https://en.wikipedia.org/wiki/Right\\_to\\_privacy](https://en.wikipedia.org/wiki/Right_to_privacy)

### *Acknowledgment*

None

### *Funding Information*

None

### *Conflicting Interest Statement*

The authors states that there is no conflict of interest in the publication of this article.

### *Publishing Ethical and Originality Statement*

All authors declared that this work is original and has never been published in any form and in any media, nor is it under consideration for publication in any journal, and all sources cited in this work refer to the basic standards of scientific citation.

### *About Author(s)*

**Ngboawaji Daniel Nte** is a Professor at the Department of Intelligence and Security Studies, Novena University Ogume, Delta State, Nigeria.

**Brebina Kelvin Enoke** is a faculty member at the Faculty of Law, Niger Delta University, Wilberforce Island, Amasoma, Bayelsa State, Nigeria.

**Joda Adekunbi Omolara** is a researcher at the School of Postgraduate Studies, Department of Intelligence and Security Studies, Novena University, Delta State, Nigeria.