OPEN ACCESS Freely available online

Global Journal of Engineering, Design & Technology

Review Article

Challenges in Regulating Emerging Cybercrimes in Nigeria

Dayo Akindipe*, Eteete Adam

Department of Engineering, Redeemer's University Ede, Osun, Nigeria

ABSTRACT

Cybercrimes are emerging crimes that are facilitated by evolving algorithms in the cyber-physical systems, which cause virtual disruption. These cyber-physical systems involve existing and new technological devices that can be utilized to perpetrate crimes through cyber-physical connections. Cybercrimes are complex universal problems that have revealed a lacuna between law and technology. These necessitate the creation of effective legal and technological solutions for the prevention of cybercrimes and related virtual disruption in Nigeria. Hence, this article examined the challenges in regulating emerging cybercrimes in Nigeria. This study adopted doctrinal analysis. Primary and secondary sources of information were relied upon. Content analysis was used to provide insight into emerging cybercrimes in Nigeria.

The study found that the extant legislation in Nigeria did not cover emerging cybercrimes and the punitive measures under the cybercrime (Prohibition and Prevention) Act 2015 are weak with outdated provisions on the definition and typology of cybercrimes. There are emerging crimes in the various types of cybercrime listed under the Act which include but are not limited to black basta, mindware, onyx, vishing, typosquatting, cloud security breaches, unstructured P2P Botnets, that are not covered in the Act. Other emerging cybercrimes include advanced persistent threat, machine learning poisoning, and artificial intelligence fuzzing. Cybercriminals use Bitcoins and other crypto-assets to execute transactions in the darknet and the Nigerian cybercrime act did not provide for the regulation of crypto-assets or the manipulation of Bitcoin ATMs. The study also found that virtual disruption has widened the gap between law and technology, leading to ineffective legal and institutional framework. The study recommended that Nigeria should accede to the various conventions on cybercrimes to align existing laws to meet global expectations.

Keywords: Cybercrime laws; Effective legislation; Emerging cybercrimes; Technological innovation; Virtual disruption

INTRODUCTION

The Nigerian Consumer Awareness and Financial Enlightenment Initiative (CAFEI) reported that by 2030, the nation would have lost $6 trillion dollars to cybercrime. Prior to this, the Nigerian Communications Commission (NCC) in 2021 reported that one of the most significant risks to the telecommunications industry is cybercrime. This concern by the NCC is derived from the information that since the deregulation of the telecommunications sector, there has been proliferation of mobile phone operators which has increased to over 197 million according to the NCC first quarterly report of 2022. There are increasing devices used to commit cybercrimes, as technology is evolving and this is a major problem for legislators [1].

At the time the cybercrime (Prohibition and Prevention) act was enacted in 2015, cybercrime was listed amongst the top ten most dangerous problems globally, including unemployment by the World Economic Forum. In the same vein, according to research conducted by Sophos, a United Kingdom security firm in 2020, found that almost 90 percent of Nigerian firms were victims of cybercrimes within that period. Nigeria depends on foreign cybersecurity technology which pose significant problem to the nation's information infrastructure and data privacy. This indicates inadequate protection against cybercrime. There are

Correspondence to: Dayo Akindipe, Department of Engineering, Redeemer's University Ede, Osun, Nigeria; E-mail: akindipedayo@gmail.com

Received: 12-Oct-2023, Manuscript No. GJEDT-23-27511; **Editor assigned:** 13-Oct-2023, PreQC No. GJEDT-23-27511 (PQ); **Reviewed:** 27-Oct-2023, QC No. GJEDT-23-27511; **Revised:** 18-Jan-2025, Manuscript No. GJEDT-23-27511 (R); **Published:** 25-Jan-2025, DOI: 10.35248/2319-7293.25.14.243

Citation: Akindipe D, Adam E (2025) Challenges in Regulating Emerging Cybercrimes in Nigeria. Global J Eng Des Technol. 14:243.

weak legal and technological framework to prevent emerging cybercrimes in Nigeria. This has also affected the national reputation from the report of international organisations. The US Federal Bureau of Investigation (FBI) in 2020 ranked Nigeria 16th amongst countries with high frequency of cybercrimes. In the Global Cybersecurity Index (GCI) 2020, Nigeria came in 47th position. In the same vein, the International Telecommunications Union (ITU) placed Mauritius, Tanzania, and Ghana above Nigeria, based on the national measures to ensure cybersecurity within the continent [2].

These low rankings indicate weakness in the detection of cybercrime as a result of the gaps in research and development to develop a modern technological framework to ensure cybersecurity in Nigeria. The government must therefore improve on its cybersecurity measures to protect its citizens.

LITERATURE REVIEW

Challenges in regulating emerging cybercrimes in Nigeria

At every epoch in human history, innovation in technology has also resulted in a disruption through the activities of cybercriminals. Technological transformation ought to be frequently accompanied with legal modification to bridge the gap between law and technology. It is submitted that the effect of emerging cybercrimes on legislation includes but not limited to; 1) The need for legislators to specifically understand and address the growing cyber techniques and not rely on general provisions in the legislation; 2) Legislators will have to be clear in the definition and interpretation of new techniques; 3) Existing rules will not likely cover new techniques in cybercrimes depending on the research and development in the applicable area; 4) Some provisions in the existing rules will not be applicable to curb emerging threats of new techniques. It is submitted that constant changes in technology presents a difficult task for the legislators since cybercrime is facilitated by technology [3].

Some jurisdictions like the United States frequently amend statutory provisions that regulates cybercrime in response to technological innovation. In comparison, since the enactment of the Nigerian cybercrime (Prohibition and Prevention) act in 2015, the legislation has not been amended 7 years after. It is submitted that legislators cannot justify that the extant legislation cover emerging cybercrimes. The fundamental issue is the increasing gap in law and technology and further undermines the protection of its citizens from cybercrime. Some of the challenges include:

Inadequate legal framework

There are emerging crimes in the various types of cybercrime listed under the Nigerian cybercrime act which include but are not limited to black basta, mindware, onyx, vishing, typosquatting, cloud security breaches, unstructured P2P Botnets, that are not covered in the act. Other emerging cybercrimes include advanced persistent threat, machine learning poisoning, and artificial intelligence fuzzing. Cybercriminals use bitcoins and other crypto-assets to execute transactions in the darknet and the Nigerian Cybercrime Act did not provide for the regulation of crypto-assets or the manipulation of Bitcoin ATMs [4].

It is important to state that there are deeper issues when it comes to the legislative and regulatory framework in Nigeria. These issues undermine the efficacy of statutory enactments across the Nation and renders legislation inadequate. This deeper issue is the disregard for the rule of law. In assessing the rule of law in Nigeria, the nation performed poorly nationally, regionally and internationally, falling to 124th out of 139th reviewed countries with a total rating of 0.40 according to the World Justice Report in 2021. The nation also faltered regionally, falling to 26 out of 33 reviewed Sub-Saharan African nations [5].

Lack of requisite skills

There is a rising deficit of 100,000 accredited cybersecurity specialists across the continent. Several institutions, firms, and departments across the country do not implement basic cybersecurity methodologies and lack basic cybersecurity competence. Governments routinely find it hard to keep track of risks, collect digital data, and investigate cybercrime. The fact that almost 100% of cyber security attacks go undetected or unaddressed demonstrates that cyberattacks in Africa are probably severe than is commonly assumed [6].

In 2020, the Sophos report stated that corporations in Nigeria had one of the highest rates of cloud security breaches in the world. Sophos also reported that in 2022, 71% of Nigerian firms had experienced ransomware in the previous year, while some of the country's greatest security breaches are still not publicly disclosed. The defensive skills required to produce effective designs, formulate detailed applications, and integrate solutions for cloud software and networks are fundamental although underestimated when it comes to upgrading cybersecurity defenses in the cloud. This is a consequence of deficit in cybersecurity skills, which results to vulnerabilities in cloud security settings that expose corporations to intrusion. The government should create opportunities for youths and information technology workshops where they can congregate and promote their expertise, as the degree of unemployment in the country has greatly contributed to the significant rise in cybercrime in Nigeria [7].

Technological advancements

The utilisation of new technologies has become absolutely crucial in the world economic landscape. Contemporary economic development is affected by cybercrime, making it essential to protect the world economy by preventing and eliminating this emerging technology enabled crimes that has become more pervasive. Utilising a computer or other similar technological tools, such as a personal device, is valuable for perpetrating cybercrimes. This is why it is necessary for the legislators to amend the definition given to a computer under the Nigerian cybercrime (Prohibition and Prevention) act, 2015

to include portable devices. It is submitted that such omission has created challenges in the legal response to emerging cybercrimes in Nigeria from the technological standpoint [8].

The CEO of Google, in 2022 reiterated that quantum computers would breach modern encryption technologies that safeguards information infrastructure within 10 years. This innovation has been acknowledged as a potential risk that will precipitate an upsurge in emerging cybercrimes by other experts including Ilyas Khan, the CEO of quantinuum, a company that specializes in emerging technologies. To avoid detection, hackers will modify standard communications into a quantum system, making computer investigations almost impossible.

Governments should increasingly update their techniques to contend with and stop cybercriminals from exploiting the disruption of technology because the digital world is altered by rapidly emerging technologies. If legislators are to accelerate the adoption of the digital revolution, cybersecurity must be embraced across all sectors of the society.

DISCUSSION

Lack of public and private sector cooperation

National legislation must ensure public and private cooperation in the fight against cybercrime. In comparison to government-enacted laws such as the cybercrime (Prohibition and Prevention) act 2015, private regulation provides mobility, adaptability, and responsiveness to the environment, market dynamics, effectiveness, and a reduction in government regulation are all factors to consider. Conversely, it is not entirely possible to regulate the cyberspace without some degree of intervention from the government. For instance, section 7 of the cybercrime (Prohibition and Prevention) act 2015 mandates the operators of cybercafe to register with the computer professionals' registration council and also maintain records of persons that use the cybercafe for online activities. Whilst this is a form of private regulation by cybercafe operators as mandated by the government, it is reiterated that most internet activities are no longer carried out at the cybercafes as computers connected to the internet continue to rise. This has widened the gap between the public and private sector [9].

Jurisdiction

The cross-border dimension of cybercrime presents the biggest problem because countries consider their legislation as a way to demonstrate their jurisdiction. Through legislation or constitutional provisions, governments are provided a significant instrument for social order that safeguards citizens but also curbs personal freedoms, as justified exceptions under the law.

As an outcome, offenses that were once limited to one jurisdiction or nation now frequently include many nations when they are perpetrated digitally such as cybercrimes in financial transactions on a networking site. Through the online platform, cyberattacks can be readily planned and carried out from another country. To underscore this development, the office of the Director of National Intelligence in 2021, in the United States reported that the Russian government was supporting electoral interference programmes operating in other countries such as Ghana, Nigeria, and Mexico against the United States.

To further underscore these issues on jurisdiction and transnational cybercrimes, it is important to bring out some of these cybercrimes that has occurred across several jurisdictions [10].

London blue

This is cybercrime group that originated in Nigeria with affiliates in the United Kingdom and allies who facilitate the processing of financial transactions in the USA and Western Europe. The organization functions like a conventional business. London Blue utilises industrial data sources to locate victims, primarily in the USA and Western Europe, and has progressed from conventional crimes business email compromise. More than 50,000 business executives, from which more than 70% were chief executives across 82 different jurisdictions, mostly in Europe and the USA were identified as prospective targets.

From the foregoing, it is submitted that these transnational crimes will compound jurisdictions issues in the fight against cybercrimes.

Slow pace of domestication of conventions or multilateral agreements

The Federal Government should ratify treaties and adopt multilateral agreements into domestic legislation in order for these agreements, whose protocols have long been considered as being slow, to resolve cybercrimes incidents that continues to evolve rapidly. From the foregoing, it is submitted that Nigeria must ratify the provisions of the African Union Convention on Cybersecurity and Personal Data, also known as the Malabo convention. The Malabo Convention has been ratified by about eleven African countries out of all the countries in the Continent and these countries include Angola, Ghana, Guinea, Mozambique, Mauritius, Namibia, Rwanda, Senegal, and Togo. The Malabo Convention has been adopted for almost a decade but the Convention is still yet to be operative because it has not met the required number of ratifications. In the same vein, it is submitted that more countries in the African region should ratify the Budapest Convention.

Slow regional response

The legal framework on cybersecurity and data protection in Europe is attributed to the low percentage of cybercrimes compared to countries from other continents such as Africa that records high rates of cybercrime. Generally, most countries in Europe are amongst the highly ranked countries globally in the adherence to the rule of law. Germany, Finland, Sweden, Norway, and Denmark are among the top five nations with the highest rankings for compliance with the rule of law. The efficacy of cybercrime legislation in Africa is also aligned with how African nations understand and comply with the rule of law. These outcomes are inseparable.

The nations that are least and most disrupted by cybercrime are identified in the report of the 2020 Cybersecurity Exposure Index (CEI), which routinely assesses 108 nations on all Continents. Africa is the region that is mostly plagued by cyberattacks, whereas Europe is the region least susceptible to attacks. The countries that are least vulnerable to cybercrimes are Finland, Denmark, Luxembourg, Australia, and Estonia. However, no government on the continent of Africa is included on the list of the nations that are least vulnerable to cybercrimes. In the cybersecurity exposure index 2020, Ethiopia has a considerable rate of cybercrime, trailed by Tanzania, Zimbabwe, Algeria, and Cameroon. Namibia recorded the lowest cybersecurity risk. Mauritius is at the top of the list of African nations with a deep commitment to cybersecurity, trailed by South Africa, Egypt, and Kenya. Nigeria and other countries in the continent should scale up commitment to cybersecurity to increase regional and international rankings on cybersecurity.

Cybercrime has considerably weakened the already precarious African economy. African countries have not made significant progress against the growing problem of cybercrime.

CONCLUSION

As a result of the shortage of qualified labour and limited resources on cybersecurity, African countries tend to be especially susceptible to cyberthreats. The budgetary allocation to cybersecurity should improve. To address cybercrime and enhance cybersecurity, the public and private sectors should work together. African nations collaborating together will enable the development of a solid cybersecurity framework. Cybersecurity initiatives must be outlined across the region if cybercrime is to be addressed. The implementation of the security regulations and interaction is the core linchpin in addressing cybercrime across the region. Cybercrime is still not regulated by any unified regional legislation in Africa.

According to a study by the economic commission for Africa in 2022, only 52% of the total number of countries in Africa have enacted statutory provisions on data protection. The national assembly enacted a data protection act in Nigeria in 2023 which was long overdue.

RECOMMENDATIONS

It is recommended that the National Assembly must ratify multilateral agreements and conventions on cybercrime so as to align the national legislation with international best practices.

The legislators must recognise emerging technologies used in facilitating cybercrimes and the legislation must cover offenses facilitated by these technologies. This is necessary to avoid provisions being outdated or obsolete which is arguably the case in the extant legislation.

Countries like the United States have enacted legislation to ensure research in quantum computing and how such innovation might be tailored to protect cybersecurity. The Quantum Initiative Act of 2018 in the United States is an example of such legislation.

It is therefore imperative that Nigeria understand the need to adopt similar approach to ensure cybersecurity. Relevant stakeholders and agencies must protect the critical information infrastructure by investing in advanced technology and developing a competent technological framework that will prevent theft of classified information protected by encryptions that can be decrypted by quantum computers.

REFERENCES

1. Sherman J. Changing the Kremlin's election interference calculus. The Washington Quart. 2022;45(1):112-131.
2. Mphatheni MR, Maluleke W. Cybersecurity as a response to combating cybercrime: Demystifying the prevailing threats and offering recommendations to the African regions. Int J Res Bus Soc Sci. 2022;11(4):384-396.
3. Oni S, Berepubo KA, Oni AA, Joshua S. E-government and the challenge of cybercrime in Nigeria. In2019 sixth international conference on eDemocracy & eGovernment (ICEDEG), IEEE, 2019;pp. 137-142).
4. Mohammed KH, Mohammed YD, Solanke AA. Cybercrime and digital forensics: Bridging the gap in legislation, investigation and prosecution of cybercrime in Nigeria. Inter J Cybersecur intell Cybercrime. 2019;2(1):56-63.
5. Osuji E. Cybercrime in Nigeria: issues and challenges. Nigerian J Legal Stud. 2023;11.
6. Tsado L, Raufu A, Ben-Edet E, Krakrafaa-Bestman D. Combatting the Threat of Cybercrime in Nigeria: Examining Current Laws and Policies. J Appl Theor Soc Sci. 2023;5(4):413-430.
7. Viko IJ. Analysis of the legal and institutional framework for fighting cybercrime in Nigeria. IJOCLLEP. 2021;3:153.
8. Adomi EE, Igun SE. Combating cybercrime in Nigeria. Electronic Library. 2008;26(5):716-725.
9. Frank I, Odunayo E. Approach to cyber security issues in Nigeria: challenges and solution. Int J Cogn Res Sci Eng Educ. 2013;1(1): 100-110.
10. Nte ND, Enoke BK, Omolara JA. An Evaluation of the Challenges of Mainstreaming Cybersecurity Laws and Privacy Protection in Nigeria. Journal of Law and Legal Reform. 2022;3(2):243-266.