iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** VIII **Month of publication:** Aug 2023

DOI: https://doi.org/10.22214/ijraset.2023.55448

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VIII Aug 2023- Available at www.ijraset.com

A Review of the National Cybercrime Law and its Attendant Impact on National Security in Nigeria

Oluwatosin Abiona[1], Abdul-Quadri Oje[2]

Abstract: ***This paper is a study on the issues in cybercrime, offences and penalties, and challenges that provoke cyber policy established in Nigeria. It seeks to define what cybersecurity and cybercrimes are from the perspective of the National cybercrime law. The focus of this study, however, is to highlight crimes or offences considered to have an impact on national security, the related issues, the effects of cybercrimes, challenges, and prospects. The study concludes that the leading causes propelling Nigerians to indulge in cybercrimes are disorientation and the rate of unemployment***

I. INTRODUCTION

The national cybercrime act of 2015 defines thirty-two different offenses and penalties that the crimes incur [1]. The crimes were explained in detail, and their various offenses were stipulated. Some of the offenses highlighted in the Act include but are not limited to;

Offenses relating to national information infrastructure are critical to national Security. Interfering with personal or official systems includes inputting, deleting, altering, damaging or other alterations to computer data on systems. Accessing data critical to national Security on unauthorized systems. Interception of electronic mail, messages or money sent electronically.

The penalties range from payment of One million naira to twenty-five million Naira and a jail term ranging from 2 years to 10 years, depending on how grave the offense is. Offenses with the highest charges are offenses related to child pornography and offenses relating to cyber bullying, kidnap, and coercion, among other cyberbullying-related offenses.

This Act proves that the impact of crimes on national Security is as grave as it can be, given the various penalties meted out for the various cybercrimes as found in the Cybercrimes Act of 2015 [1] by the Nigerian Government. As indicated in the Act, the Onus for effective implementation of the Act is on intelligence, law enforcement and security agencies, which are expected to develop the capacity required for this task.

Table 1: Summary of the cybercrime law as stated in the cybercrime act [2]

	ACT	**SUMMARY OF ACT**		
	CYBERCRIMS ACT 2015	This Act provides an effective, unified and comprehensive legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria.		
	PART 3: OFFENCES AND PENALTIES			
S/N	**SECTIONS**	**TITLE OF SECTIONS**	**SUMMARY**	**PENALTIES**
1	***Section 5***	Offences Against Critical National Information Infrastructure	Critical National Information Infrastructures are designated computer systems, programs and networks that have impact on the security and economy of Nigeria Amongst others.	A person found guilty is liable on conviction to imprisonment of term not ≥ 10years without option of fine. When offences involves bodily harm the penalty is ≥ 15 years and when it death = life imprisonment.
2	***Section 6***	Unlawful Access to a Computer	Unlawful access of computer or network for fraudulent purposes to obtain data	A person found guilty is liable on conviction to imprisonment of term not ≥ 7 years or a fine of ≥ N7 Million Naira
3	***Section 13***	Computer Related Forgery	Access of computer to delete or alter data	3 years in prison or N7 million or both
4	***Section 14***	Computer Related Fraud	Access of computer to commit fraud	3 years in prison or N7 million or both
5	***Section 16***	Unauthorized modification of Computer systems, network data and system interference.	Without lawful authority modifies or causes modification of any data held on a computer.	Not more than 7 years imprisonment or N10 Million or both
6	***Section 18***	Cyber Terrorism	Access computer for purpose of terrorism	Life imprisonment on conviction
7	***Section 22***	Identity theft and impersonation	Identity theft in financial institution or impersonation	7 years imprisonment or N5 Million Naira or both.
8	***Section 23***	Child pornography and related offences	Produces, offers, distributes or possess child porn	5-15 years in prison and N10 - N25 million in fines
9	***Section 24***	Cyber Stalking	A course of conducted directed at a specific person that would cause a reasonable person to feel fear.	3 – 10 years imprisonment and/or N7 – N25 Million Naira in Fines
10	***Section 30***	Manipulation of ATM/POS Terminals	Manipulation of ATM/POS with intention to defraud	5 years in Prison or N5 million or both
11	***Section 32***	Phishing, Spamming, Spreading of Computer Viruses	Sending of spam emails and spreading of computer viruses	3 years imprisonment or N1 Million or both
12	***Section 36***	Use of fraudulent device or attached e-mail and websites	Use of any devices, email or website with an intention to defraud.	3 years imprisonment or N1 Million or both

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VIII Aug 2023- Available at www.ijraset.com

II. CHALLENGES AND ISSUES LEADING TO CYBERCRIMES

There has been an exponential rise in the rate at which cybercrimes are perpetrated all over the globe. The rise has given birth to the promulgation of various laws and the establishment of various committees, teams, and departments in agencies, among other steps taken to ensure the safety of the member of individual citizens of a country or region. These issues are so wide that there is a high poverty rate among the populace.

Listed here are some common issues as surmised by different researchers. This paper highlighted Unemployment, insufficiency of personnel in cybersecurity and related fields, work-little-get-rich mentality, and inadequacy of laws governing cybercrimes [3] as factors promoting or leading to the prevalence of cybercrimes in Nigeria. Omodunbi et al. (2016) also followed as Obarafor claimed. As opposed to the notion posed here by the author about inadequate laws guiding cybercrimes and related offenses, the Nigeria cybercrime act of 2015 has thirty-two major crimes listed and expanded upon. This is far above the three (3) crimes highlighted by the author in the paper of reference.

The research [4] published in an international journal defines that the challenges of cybercrimes include domestic and international law enforcement boundaries, the alarming rate of Unemployment, high poverty rate, high level of corruption, non-availability of standards regulation bodies for cybercrime activities, lack of infrastructure and human resources, the porosity of the internet. The challenges raised in this paper are valid. In addition, this paper was published before the Cybercrime Act of Nigeria was established.

As highlighted in the papers reviewed earlier, it is not limited to financial-related crimes only, but it is the most rampant crime related to cyber Security. The most common are; Advance fee scams, Business Email Compromise Fraud, popularly known as BEC Scams and Romance Scams or fraud [5]. In critical analyses by Muhammad et al. (2020), it was observed that Nigeria ranks top on the list of countries affected by Scam emails. Further to this, in the research is a tabular summary that shows that the number of reported cases of BEC attacks in 2019 is almost ten times the number of reported cases in 2014. This is a 5-year gap with an exponential increase. There have been several reports of such cases worldwide, with one such recent case implicating a popular Influencer, Hushpuppi.

Table 2: Table showing a summary of BEC attacks reported in the US from 2014 to 2019 [5]

No. of cases reported	Amount lost in $	Year
2,417	$226,000,000	2014
7,837	$246,226,016	2015
12,005	$360,513,961	2016
15,690	$676,151,185	2017
20,373	$1,297,803,489	2018
23,775	$1,776,549,688	2019

The high poverty-stricken mentality and disorientation among the youth of today are posing great challenges and hence increasing the involvement of youths in cybercrimes. There is a mentality of *"it is our parent's money, or our forefathers' money, get-rich-work-less,"* among other excuses youths give to perpetrate crimes in cyberspace. This corroborates with other issues, such as the country's high unemployment rate.

The prevalence of attacks in the country and around the globe has prompted some researchers and teams to develop solutions to combat cybercrimes. One such solution is the development of heat maps to show regions more affected by cyber attacks. Kaspersky also has a website that displays the heat map and statistics of cyber attacks per month. Below is an image showing the statistical representation of the Intrusion detection scan in October 2021.

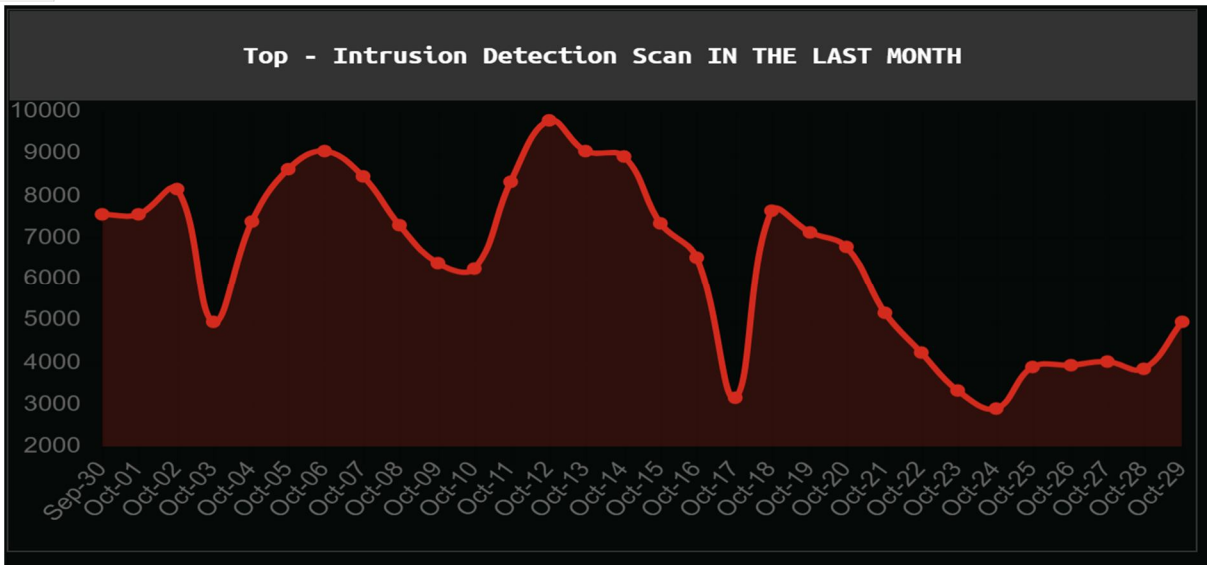


Figure 1: Image showing the frequency of intrusion detection [6].

III. IMPACTS AND EFFECTS OF CYBERCRIMES ON NATIONAL SECURITY

The impact cybercrimes have had on national Security can be positive or negative, with more inclination towards the negative in the present age. This research will highlight some positive impacts of cybercrimes on National security and the negative Impacts.
The negative impact of cybercrime on society can generally be grouped as follows;

Table 3: Table describing the negative impact of cybercrimes [2]

S/N	GROUPS TARGETED	TYPE OF CRIME
1	AGAINST INDIVIDUAL	Harassment via emails, cyber-stalking, dissemination of obscene material, defamation, hacking/cracking and indecent exposure.
2	AGAINST INDIVIDUAL PROPERTY	Computer vandalism, transmitting virus, netrespass, unauthorized control over computer system and hacking/cracking.
3	AGAINST ORGANIZATIONS	Hacking/cracking, possession of unauthorized information, cyber terrorism against the government organization and distribution of pirated software, etc.
4	AGAINST SOCIETY	Pornography (basically child pornography), corrupting the youth through indecent exposure; and trafficking

A. Positive Impact

1) Cyber Awareness and Orientation Program

The use of cyberspace for learning, orientation and fast dissemination of information must be considered. This cyberspace and the internet have proven to be a quick way of disseminating information. This enabling environment has assisted the military in relaying signals at a very quick rate. It also assists in disaster management and quick dissemination of information to the population of a particular area to avert the high impact of impending dangers. In addition, the National Orientation Agency (NOA) can use cyberspace to enlighten the country's citizens and pass on vital information that is important to national Security, as this would facilitate the easy achievement of their mandate [7].

2) Cross-country Regulation

With the advent of cyberspace and internet technologies, communication has significantly increased, thereby reducing the logical distance between countries despite the physical distances. This phenomenon is popularly regarded as a Global village. The level of international and intercontinental cooperation has expanded, and barriers to the implantation of law, though still limited to country-wise jurisdictions. Security and intelligence agencies can now collaborate to conduct investigations and research on national security matters.

B. Negative Impact

1) Cyber Mobilization and Revolution

Social media, among other electronic and digital means of communication, have enhanced relationships beyond borders. Tools such as youtube, Twitter, and Facebook, among others, have been used over the years to solicit and canvas for support. The 'Twitter revolution" of Iran and Moldova dates back as far back as 2010. Also, some North-African countries have a history of cyber mobilization [8].

About a year ago, Nigeria witnessed a large-scale protest in several states, which was facilitated by various social media avenues, with the Twitter app playing a major role in this [9]. The various cyberspace tools facilitated non-traceable fund racing such as crypto technology, easy organization and planning, among other services the cyberspace tools enhanced.

2) Cyber Impersonation and Defamation

Impersonation and defamation are two completely different entities when looking at cyber threats, yet interrelated. The relationship is that they are both referring to an attack on personality. Impersonation implies taking on another person's identity, while defamation implies spoiling the outward presentation of a person or group of persons [10].

Impersonation threat in cyberspace is the most used when looking at financial-related cybercrimes. It ranges from posing to being a business associate when you are not or as a person of the opposite gender to dupe a person through romance, scams, or fraud. Another aspect of impersonation is website impersonation, where businesses are duplicated to carry out transactions on behalf of the genuine business.

Defamation comes in two, which are libel and slander. Libel involves defamation carried out through written documents which in most cases are permanent. Slander, on the other hand, involves defamation through speech. In [8] described defamation through one of the social media tools – Twitter as Twibel. This further shows that cyberspace is a small world that needs to be regulated by laws as well.

3) Cyber Malware

Malware which in full means malicious software, is one of the main attacks on a computer system, network or device. It includes viruses, trojans and worms. This software sometimes replicates itself or inhibits activities on the network or device they find themselves. They are introduced to functional sabotage systems to extract sensitive information, disrupt service or hold a company ransom so that they pay a given amount and their systems are thence free from attack.

One attack that took down major systems in the world is the Ransomware virus of 2017. Business owners are encouraged to have daily systems backups to avoid repercussion effect when malware attacks.

4) Cyber Spying, Jacking and Espionage

Cyber Spying refers to the impact of spying on people through the web as in traditional spying to access or intercept vital information from the owner or company's system. Large-scale spying on people and businesses is referred to as cyber espionage.

Cyber jacking is closely related to the above-defined term. In this case, it is defined as the hijacking of a website, or server, among other IT infrastructure, to extract vital information or interception of information being transmitted [11].

5) Illicit Business Transactions in Cyberspace

This is the implied use of cyberspace to establish communication to transfer information, such as meeting points, exchange of funds, and laundering of funds, among other illegal activities that can be carried out within cyberspace. A typical example is the 'Dark web,' which is hidden away from the general web. This is a vulnerable place to access the web as unauthorized tracking can be initiated from the dark web.

6) Cyber Terrorism and Warfare

This is becoming rampant as more and more devices are connected over the web, especially with the growing implementation of smart home systems and IoT technologies. Extensive research is ongoing to ensure maximum Security for services and infrastructures. Cyberterrorism involves hijacking internet-controlled amenities such as gas distribution, power service subscriptions, telecommunications, and transport systems, among other cyberspace-related services. It implies that any targeted system will cease functioning efficiently, and efforts will be poured into ensuring that such systems are recovered from the hijackers. Warfare, on the other hand, does not involve basic amenities only; it can encompass all forms of an attack earlier highlighted in this paper review, taking up any form of two or more of the above-highlighted threats.

IV. PROSPECTS AND RECOMMENDATIONS FOR TACKLING OF CYBER CRIMES IN NIGERIA

1) *Enlightenment and Awareness:* It is essential for the NOA, among other agencies saddled with the responsibility of educating the public so that they do not fall victim to cybercrimes. In addition, the disorientation among youths and the public, in general, should be corrected as this is not done the perpetrators any good but exposes them to the ills of cyberspace. The notion 'it is our ancestral right to get back our money' should be cast out of the mind of the public citizens [12].
2) *Enforcement of Established Laws:* As described in the sections above, laws are already in place to tackle the ills. These laws should be made known to the public, as noticed in some papers reviewed in this research [12]. Some researchers are still unaware of this Act's availability and how grave certain offenses often overlooked as minor offenses are. As the popular saying goes, "Ignorance of the law is not an excuse. "
3) *Training and Capacity Building to Tackle Cybercrimes:* As observed in some papers reviewed, the capacity of the available hands could be better with the rate at which cybercrimes is growing worldwide. Additionally, existing staff are not skilled enough to handle tasks. In that case, there need not be any reason to employ new hands but rather train those that are available so that they can safeguard the country and maintain the National Security of the country.

V. CONCLUSIONS

This paper examined the impact of cybercrime and its threat on Nigeria's national Security, examine the issues and challenges of cybercrime in national Security and propose strategies for mitigating Cybercrime for National Security.

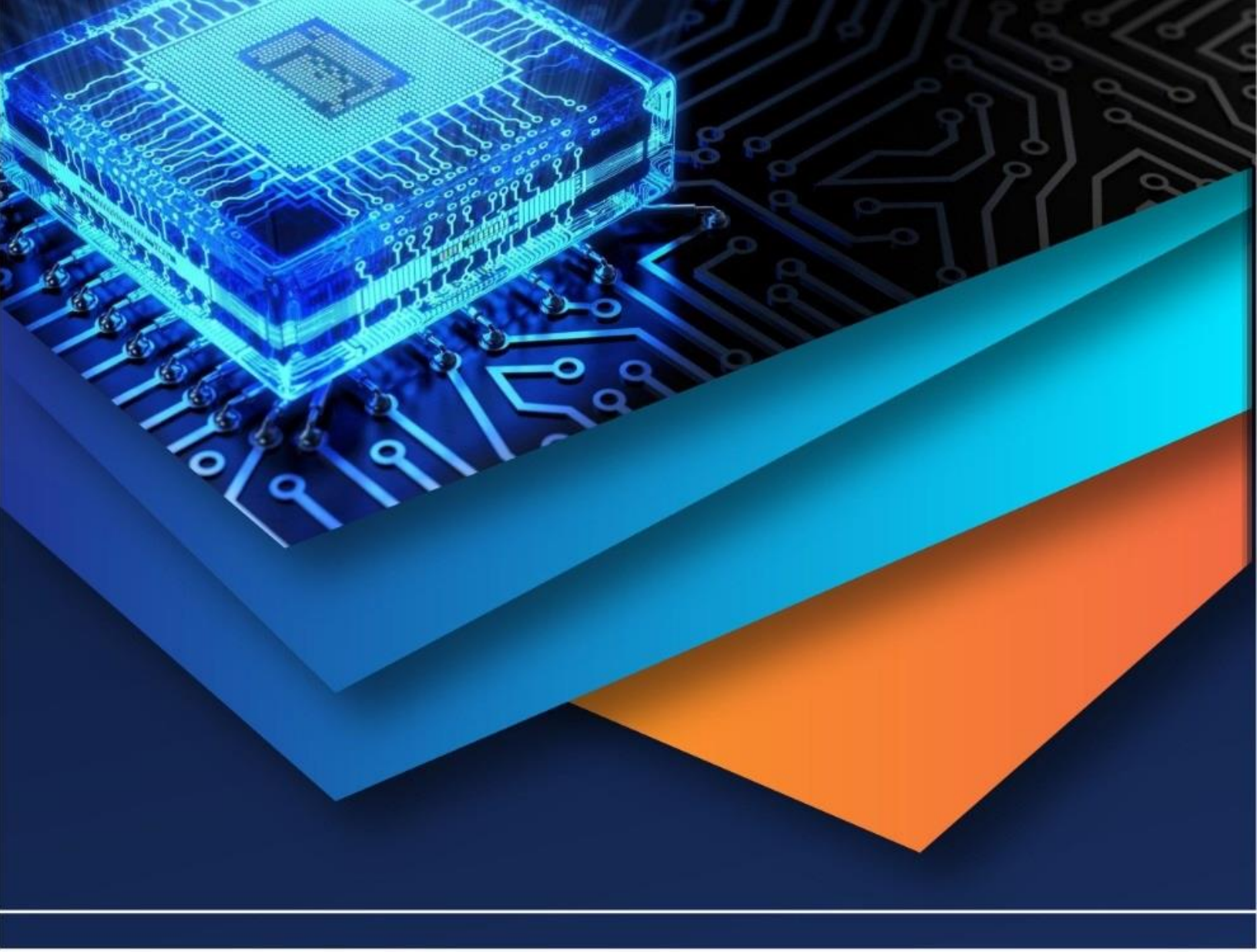
Unemployment and disorientation are the leading cause and challenges of cybercrimes in Nigeria. The impact on national Security, as identified, shows that it can lead to internal division within the country, which is in itself a threat to national Security.

Lastly, it is recommended that efforts be put into acquiring adequate tools and proper capacity development be done for staff of agencies and departments saddled with the responsibility of enforcing laws and guarding national systems against cyber-attacks. Furthermore, the current cybercrime act in Nigeria has been criticised by a number of organisations and individuals on a number of occasions. One of such criticism is reported in [13] as vague and unlawful. Efforts have been put in place by the newly appointed National Security Adviser of Nigeria – Mallam Nuhu Ribadu, to ensure that the Cybercrime Act is amended to meet up with policies implemented internationally [14].

REFERENCES

[1] Cybercrime Advisory Council (CAC), CYBERCRIMES (PROHIBITION, PREVENTION, ETC) ACT, 2015, 2015.
[2] B. Muktar, "INVESTIGATING CYBERCRIMINALS IN NIGERIA: A COMPARATIVE STUDY," Salford, 2018.
[3] V. Obarafor, Cyber crime in Nigeria, Causes, Effects, and solutions., figshare, 2019.
[4] F. Ibikunle and O. Eweniyi, "Approach to Cyber Security Issues in Nigeria: Challenges and Solution," International Journal of Cognitive Research in science, engineering and education, 2013.
[5] H. Muhammad, A. M. Idris, M. Ali and O. Morufu, "Analysis of Cybercrime in Nigeria," in IEEE 2nd International Conference on Cyberspace (Cyber Nigeria), 2020.
[6] Kaspersky , "Cyberthreat real-time map: Statistics," October 2021. [Online]. Available: https://cybermap.kaspersky.com/stats#country=141&type=IDS&period=m.
[7] NOA, "Stategic Plan for national Orientation Agency (NOA) (2017-2021)," 2017. [Online]. Available: https://noa.gov.ng/wp-content/uploads/2018/04/Draft-OF-STRATEGIC-PLAN-FOR-NATIONAL-ORIENTATION-AGENCY.pdf.
[8] S. O. Oluga, A. Haji-Admad, A. J. Alnagrat, S. O. Haroon, M. Abdullah-Sawad and B. M. Nur Adiya, "An Overview of Comtemporary Cyberpace Activities and the Challenging Cyberspace Crimes/Threats," International Journal of Computer Science and Information Security, vol. 12, no. 3, pp. 62-100, March 2014.
[9] H. D. Tamar, E. Metin, M. A. Ahmad, O. O. Victor, O. Ayodeji, O. A. Abdulgaffar and J. Ayodele, "Nigeria's #EndSARS movement and its implication on online protests in Africa's most populous country," Journal of Public Affairs, pp. 1-11, 2020.
[10] B. A. Omodunbi, P. O. Odiase, O. M. Olaniyan and A. O. Esan, "Cybercrimes in Nigeria: Analysis, Detection and Prevention," FUOYE Journal of Engineering and Technology, vol. 1, no. 1, pp. 37-42, 1 September 2016.

[11] K. N. Igwe and I. Ahiaoma, "Imperative of Cyber Ethics Education to Cyber Crimes Prevention and Cyber Security in Nigeria," Interntional Journal of ICT and Management, vol. II, no. 2, pp. 102-115, October 2014.
[12] J. C. Oforji, E. J. Udensi and K. C. Ibegbu, "Cybersecurity Challenges in Nigeria: The way forward," SosPoly Journal of Science & Agriculture, vol. II, pp. 1-5, December 2017.
[13] Sahara Reporters, "ECOWAS Court Declares 'Nigeria's Cybercrime Act Section 24 Vague, Arbitrary, Unlawful'," Sahara Reporters, 22 March 2023. [Online]. Available: https://sahrareporters.com/2023/03/22/ecowas-court-declares-nigerias-cybercrime-act-section-24-vague-arbitrary-unlawful. [Accessed July 2023].
[14] I. Olorunfemi, "NSA Ribadu moves for Cybercrimes Act amendment," PM News, July 2023. [Online]. Available: https://pmnewsnigeria.com/2023/07/12/nsa-ribadu-moves-for-cybercrimes-act-amendment/. [Accessed July 2023].



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY