International Journal of E-Government & E-Business Research
Online ISSN: 2456-8295
Volume-8 | Issue-1| 2023|
Journal homepage: https://arseam.com/journal?title=IJEGEBR
DOI: https://doi.org/10.5281/zenodo.10437420

Research Paper **Peer Reviewed Journal** open access

GOVERNMENT POLICIES AND CYBERSECURITY IN AFRICA: THE NIGERIAN PERSPECTIVE IN THE POST-COVID-19

[1]Busayo, Qazeem, Ibikunle, [2]Ibrahim Korede, Hassan, [3]Victoria Opeyemi, Hunga
Lecturer, Department of Public Administration,
Lagos State University, Ojo, Lagos, Nigeria
[1]Email Id: busayo.ibikunle@lasu.edu.ng [1]ORCID: https://orcid.org/0000-0001-5854-835X
[2]Email Id: ibrahim.hassan@lasu.edu.ng [2]ORCID: https://orcid.org/0000-0002-0404-5826
[3]Email Id: victoria.hunga@lasu.edu.ng [3]ORCID: https://orcid.org/0000-0003-4623-2803

Corresponding Author: Busayo, Qazeem, Ibikunle

Article History:
Received: 17- Feb-2023
Revised: 26 - Mar- 2023
Accepted: 17 -Apr-2023
First Published: 30-Jun-2023
Cite this Article as :
Ibikunle B.Q, Hassan I.K & Hunga V.O (2023), "Government Policies and Cyber Security in Africa: The Nigerian Perspective in the Post-COVID-19", International Journal of E-Government & E-Business Research, Vol. 8, Issue 1, 2023, pp 20-30,
DOI:
https://doi.org/10.5281/zenodo.10437420

ABSTRACT

Aim of the study: *This research examines the effect of government policies on cyber security in Africa from the perspective of Nigeria in the post-COVID-19 era.*
Design/Methodology: *The descriptive survey design was used for this study. Both primary and secondary data were utilized. A structured survey was conducted to generate data. For the secondary, data was sourced from the internet, articles, journals, newspapers, and policy documents.*
Findings: *The findings reveal that the agencies put in place to fight crime do not have the more sophisticated tools they need to deliver services in Nigeria effectively; the study also finds that government policies in Nigeria, as far as cyber security is concerned, are a blueprint, but those policies have not reduced the incessant cybercrime in Nigeria after the COVID-19 era.*
Practical Implications*: Cybercrime will continue to hamper Nigeria's prosperity if the government fails to provide tools and capacity for the agencies to fight cybercrime in Nigeria. The paper, therefore, suggested, among others, that policymakers need to occasionally train criminal agencies on the way cybercriminals operate in Nigeria.*
Originality/value*: The study adds to current information by exposing the government to technology infrastructure and institutions that would allow for rapid reaction to cyber-attacks.*

Keywords*: COVID-19, Cyber-security, Cyberspace, Institutional Capacity, Policy, Technological Infrastructure*

Paper Type: Research Paper

1. INTRODUCTION

E-governance and innovation are drivers of technology in the workplace where many developed countries' policymakers, such as in Germany, Canada, Norway, the Great Britain and in the United State of America are tapping into the imminent need for effective public service delivery in their various societies. African policymakers have also seen the coming world as a space through which effective public service delivery can be attained. It is important to note that the need to secure cyberspace should be considered as policymakers think about technology for meeting societal demands (Okunoye, 2022). In recent times, cybercrime has emanated as a global challenge; this became pronounced after the COVID-19 outbreak all over the world, where phishing schemes and ransom ware attacks, including malicious spam messages, became prominent (Ukwuoma, Williams, & Choji, 2022).

Africa, as a continent in a transiting category, needs technology to thrive. It is expected that over one hundred and eighty million dollars ($180 million) should be contributed to the growth of the African digital economy by 2025, and by 2050, seven hundred and twelve billion dollars ($712 billion) will have been contributed. To this end, African leaders and epistemic community are to connecting other unconnected African nations to address issue in cybercrime (Mackenzie, White, Bernstein, & Spencer, 2021). In June 2020, a report had it that South Africa ranked third in the globe as regards cybercrime victims, which requires the nation about $147 million per year. In Nigeria, one Android phone is infected with malware for every nine, while in Ethiopia, a significant increase in cyber-attack attempts has been reported. Hence, cybercrime has affected the African GDP by more than 10%, costing an estimated $4.12 billion in 2021 (Adegoke, Boakye, & Garson, 2022).

To this end, several policies on cyber security have been established. Collaborations with the epistemic community have engendered various strategies to strengthen cyberspace. Countries like Ghana are investing in solid cyber security infrastructure, posing as a model for other African nations. Fourteen African nations (Kenya, Malawi, Nigeria, Rwanda, and others) have a national cyber security policy, and four are working on digital legislation (International Telecommunication Union, 2022). The Union of Africans (AU) at the Malabo Cyber security Convention developed a data protection model for her citizens to strengthen the continent's cyber capacity building and expertise as the continent is leveraging on significant global capacity development through this process (Ukwuoma, Williams, & Choji, 2022). In 2018, eight out of fifty-four nations developed national cyber security policies. Also, during the 2021 West African States Economic Community (ECOWAS) regional cyber security strategy, the summit conveyed that cybercrime and electronic evidence legislation need to be harm on ised within the framework of the rule of law and human rights safeguards (Ikuero, 2022).

Several government policies on cyber security were formulated in Nigeria even before the COVID-19 outbreak. However, the pandemic awakened the strategies of the government to tackle the cyber attack. During the 'sit at home policy', an identity theft and business compromise emails led to hijacked online banking where huge amount of money stolen (Ikuero, 2022).

To solve the issue of cybercrime in Nigeria, the government has developed several policies, which include: a legislative framework for child and gender online protection; a legislative

framework for online consumer protection; a legislative framework for bug bounty; integration of digital identity into national cyber security strategy; a legislative framework on technical and policy initiatives on federal cyber security programmes; data governance and protection of digital intellectual property; development and enactment of data protection and privacy laws; and harm onisation of e-business laws in line with global actices. In furtherance of the above legislation, the National Broadband Plan (NBP) (2020) has led to increased internet penetration across the nation, which has assisted the government in its Economic Recovery and Growth Plan (ERGP). To ameliorate the recessionary effects the country is battling while also ensuring social stability and economic vulnerabilities caused by the COVID-19 pandemic, it is a turning point for the government to implement a national identity programme and a data privacy and protection framework for the nation's cyberspace. The various platforms provided by cyberspace serve as an enabler for tackling some of the myriad forms of insecurity currently bedevil ling the country.

More so, cyberspace creates the link for synch ronising, which may enhance stability and improve the activities of the law enforcement agencies towards curbing various crimes such as human trafficking, arms proliferation, irregular migration, and others while improving border security and road safety as well as enhancing ongoing anti-banditry, anti-militancy, and counter-insurgency operations. Furthermore, cyberspace provides the platform to improve probity and openness in government businesses and combat corruption (Ibukun & Jeong, 2019). However, the ability to fully exploit and harness the maximum benefits of cyber security is threatened by numerous inherent challenges. The recent expansive nature of internet penetration has increased the diversification of threats in Nigeria's cyberspace, as has the proliferation of various forms of cyber-attacks such as fraud, identity theft, and property theft. Furthermore, the use of cyberspace to propagate fake news, hate speech, and seditious messages by regional and non-regional actors, as well as international and domestic elements, also forms part of the challenges to Nigeria's cyber security. Hitherto, it also served as the medium through which terrorist and separatist groups indoctrinated and propagated their nefarious activities to undermine the state's legitimacy and cause apprehension among the citizens (Arinze, Longe, & Eneh, 2020). Also, the outbreak of the COVID-19 pandemic has increased internet users, which has resulted in a massive migration of businesses and government activities to online exercise.

Several studies have been done on the related study. Some of which are Ibukun and Jeong (2019); Osho and Onoja (2015); and Arinze, Longe, and Eneh (2020), have revealed that there is institutional failure and incapacity of the law enforcement agencies in enforcing legislation on cyber-terrorism, malware, spoofing, key logging, cyber-theft, cyber-laundering, cyber contraband, cyber-vandalism, and others.

As a result, it has become a ubiquitous task as law enforcement agencies lack in-depth computer forensics training. However, this paper identifies the following as gaps in the existing knowledge: The current review in 2021 NCPS sets the direction for the engagement and coordination of Nigeria's cyberspace as the legal and regulatory framework hopes to strengthen institutional capacity, enhance regional and international cooperation and digital economy growth.

2. LITERATURE REVIEW

2.1 Government Policy

Government policy is the result of a set of activities that operate within an environment where government policymakers determine what to do and what not to do. According to Ibikunle, Ojo, Kuyebi, Okewale, (2021), government policy was viewed from a public policy perspective, as they defined public policy as that which the government decides to do or not do. This definition of government policy is directed towards the impact of the government's decisions on society. Attending to issues related to crime and cyber threats is a priority for the government. The government, through policymaking, now decides which of several issues affecting the public should be attended to.

2.2 Cyberspace

Cyberspace has been conceptual lised in various ways, and no universal definition is associated with it. Cyberspace can be referred to as the endless platform known as the internet. The virtual global domain impacts most commercial and non-commercial sectors, including socioeconomic activities, national security, and critical infrastructures (Monguno, Igbokwe, & Egbe-Nwiyi, 2021). With the digital transformation currently reflected in our e-governance and administrative processes, cyberspace has created opportunities for innovation and prosperity. Likewise, it serves as a means to improve the general welfare of the people. Cyberspace enhances the emerging technologies that dismantle barriers to commerce, bolster economic positions, and enhance easy interaction across borders (Afifi, Bolton, Mota, Marrie, Stein, Enns, & Sereen, 2021).

2.3 Cyber security

Nigeria's cyber security landscape is a comprehensive and all-inclusive policy and strategy framework that focuses on developing and protecting the nation's cyber security ecosystem. The policy serves as a strategic roadmap for stakeholders in the country to come together and drive the attainment of national cyber security objectives. Given this, the National Cyber security Policy and Strategy 2021 policy document came into existence from the review of Nigeria's National Security Strategy 2019 to realign it with current societal needs. The National Cyber security Policy and Strategy 2021 signify the renewal and commitment of national security and economic prosperity as they ensure that the country's cyber security programme is prioritised among other national exigencies.

Nigeria's cyber security landscape is beyond confronting the dynamic and emergent nature of the threat in our cyberspace during the COVID-19 pandemic. Cyber attacks and threats become apparent in our cyber security landscape as the nation's firewall experiences vulnerability, which was more evident during the End Sars protest. In this regard, the interference of the government was of utmost importance to create a strong cyber security strategy that can be used to coordinate and effectively harness the cyber security efforts of our professionals in the private sector, practitioners, industry, academia, public sectors, and civil society towards progressive national development (Afifi, Bolton, Mota, Marrie, Stein, Enns, & Sereen, 2021). The cyber security landscape must also synergize to develop the necessary human and technological capacity to harness the full benefits of the digital space, which will engender positive economic transformation in the country. Furthermore, the Nigerian cyber security landscape has revealed that the government is blessed with a large, young, and entrepreneurial population that is ready to tap and exploit the unique opportunities of the current cyberspace, as the country is currently designing the necessary mechanism for

annual licencing and registration of cyber security training institutes, which will be in line with global practices (Akinyetun, Erubami, Salau, Oke, & Samuel, 2021).

2.4 Government Policies and Cyber security in the Post-COVID-19 Era

Over the years, several policies have been enacted to protect the nation's cyberspace against attacks, crimes, and threats by cybercriminals. The de fence of cyberspace is germane to national cyber security, as it was more pronounced during as well as in the post-COVID-19 pandemic, where there is a surge in the usage of our cyberspace by domestic, foreign, and transnational state and non-state actors perpetuating attacks such as cyber espionage, cybercrime, cyber terrorism, and other forms of or ganised cyber-attacks (Mitchell, 2022). Meanwhile, policies and strategies have been developed to strengthen our institutional capability and defence mechanisms to identify, detect, and even deter any or ganised cyber attack launched on national cyberspace. It is on this basis that the National Cyber security Training Institute (NCTI), National Cyber security Coordination Centre (NCCC), and De fence Space Academy (DSA) collaborate with other relevant agencies to provide resilient cyberspace capabilities in cyber incident management, technology, and skills transfer. These agencies are pivotal in coordinating cyberspace activities, ensuring that all government and private sector stakeholders are ready to mobilise in unison to defend the nation against cyber threats and attacks (Ikuero, 2022).

In addition, government policies have led to the formation of more institutional agencies to regulate the activities of internet users through various laws. The Cybercrime Prohibition and Prevention Act (CPPA), the Critical National Information Infrastructure Protection Plan (CNIIPP), the Cyber Emergency Monitoring System (CEMS), the Cyber The Critical Information Infrastructure Protection and Resilience Emergency Response Team (CERT) (CIIPR), the Critical Infrastructure Programme for Model ling and Analysis, The Critical Infrastructure for National Information (CNII), and the Critical Information Infrastructure Measurable Programme (CIIMP) are set in place to fight cyber-attacks. The government is responsible for improving and updating federal and state laws to protect Nigerian cyberspace and combat cybercrime. The policies are meant to ensure the harm on isation of provisions in other legislation relating to online consumer protection, e-business, e-governance, e-government, and others, bringing to the fore the need for a robust legal and regulatory framework that will facilitate a more proactive approach to confronting and curtailing attacks or threats in our national cyber ecosystem (Ikuero, 2022).

2.5 Cybercrime in Africa: the perspective of Nigeria

As cyber attacks become a much more significant threat to the region and internet traffic doubles every eighteen months, African authorities and corporations risk investing heavily in digital security. The NITDA suggested that Section 14 of the Nigerian Constitution, which stipulates that "no person shall be punished for a crime unless such a criminal offence has been recognised as a punishable offence. However, an agency delegated to enforce any crime shall then use its discretion to curb any form of criminal activity. Such an agency is saddled with the responsibility to contribute cybercrime and capacity-building initiatives aimed at achieving cyber security bills, influencing updating the Evidence Act through the law reform commission and collaborating with the private sector to set network security rules. As a result, these countries possess the greatest quantity of cybercrime victims in the world (Mitchell, 2022).

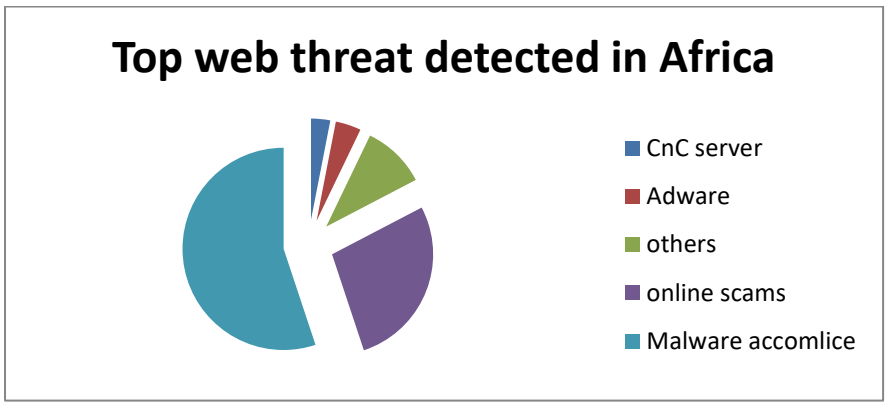

Diagram 1: The rate of web threats in Africa

Source: Mitchell, (2022)

The above diagram shows the incessant web threat in Africa. According to the rate, the analysis shows that the malware accomplice issue in Africa is the most pronounced cyber attack, covering a percentage of 54%, followed by online scams with 27%, other cyber threats with 10%, adware with 4%, CnC servers with 3%, and phishing with 1.9%. According to Mitchell (2022), "Currently, phishing attacks are the most common method used by cybercriminals in Africa. Over time, the emphasis has shifted away from attempting to hack into a company's central ICT system to target end users. End users are people who are not cyber-aware and are vulnerable to these attacks. They do not practice sanitary cyber security. The first step is to educate cyber users to create a cyber-aware workforce. 'Do not open unsolicited attachments should be the message. The question now is, who is responsible? He believes that the government bears the primary responsibility and must ensure that a national level of cyber security awareness is implemented throughout the country.

2.6 Theoretical Review

The Technology-Enabled Theory

This theory came into existence in 1998 through Samuel C. McQuade III's Encyclopaedia of Cybercrime publication. This theory therefore brings to light the approach for underscoring criminal activity revolving around computers and relating to the internet and technology. This approach directs our understanding towards threats engendered by cybercrime and terrorist networks. An issue of national security is cyber security. since Fundamental values and society as a whole are in jeopardy. by terrorists and information warfare threats; the need for state actors to rise against these challenges serves as the basis of the study.

The theory is important to study because it offers the covert instruments utilized to encourage cybercrime into the comprehension of the new instruments, strategies, and tactics employed by cybercriminals; in other words, there is a transition from simple crimes committed with simple tools to complex crimes committed with sophisticated tools (Odumesi, 2014). By adapting technology-enabled crime theory to Nigeria's circumstances, the method offers a perceptive comprehension of the novel instruments and methodologies employed in cybercrime operations.

3. THE AIMS OF THE STUDY

The study's main aim is to examine government policies and cyber security in Africa, particularly Nigeria's experience in the post-COVID-19 era. The specific aims are:

- To evaluate the significant relationship between cyber security policy and institutional capacity in the post-COVID-19 era in Nigeria,
- To ascertain the significant association of cyber defence mechanisms in the Nigerian national digital economy before and after the COVID-19 pandemic.

4. METHODOLOGY

A For this investigation, a descriptive survey was used. The entire staff of the Lagos Chapter of the Economic and Financial Crime Commission (EFCC) is the study's population. The population of the study consisted of 150 staff members who were chosen using a basic random sampling technique., as illustrated in the table 1 below:

Table 1. Staff Strength in selected Department

Department	No. Of Staff
Human Resources	78
Education	33
Finance and Accounting	39

Sampling and Sample Size: Hence, the sample size for this study is calculated as follows;

$$n = \frac{N}{1+ N (e)^2}$$

Where: n = sample size
N = Total population
e = Error margin

Therefore, $n = \frac{150}{1 + 150 (0.05)^2}$

$$n = \frac{150}{1.38}$$

$$n = 109.09$$

Therefore, the sample for this study is one hundred and nine (109).

Data collection instrument: Section A and B comprised the two sections of the questionnaire used in this study. The respondents' demographic information is gathered in Section A. It addresses topics including age, gender, educational background, number of years of employment or work experience, and department of the officials.

Method of Data Collection: The researcher and two trained assistance administered the questionnaires. The questionnaires where hand delivered and the researcher or research assistant waited and retrieved the questionnaires immediately from the respondents. The respondents were made up of the following people, public servant, private sector workers, traders, students, apprentice and residents located at their various offices, shops or markets and school. One hundred and nine questionnaires were distributed in total. while 95 (87%) and were further analysed using Spearman Rank Correlation.

5. RESULTS AND DISCUSSION

Test of Hypotheses

Decision Rule: The null hypothesis is accepted unless the P-value is less than five percent (P<0.05).

Hypotheses One (H_0): There is no significant relationship between cyber security policy and institutional capacity in the post-COVID-19 era in Nigeria,

Table 2: Spearman's Rank Correlations Hypotheses One (H0)

			ECOSCALE	Cybercrime
Spearman's rho	ECOSCALE	Correlation Coefficient	1.000	. 658
		Sig. (2-tailed)	.	.000
		N	95	95
	Cybercrime	Correlation Coefficient	. 658	1.000
		Sig. (2-tailed)	.000	.
		N	95	95

** Correlation is significant at the 0.05 level (2-tailed).

This finding means that the alternative hypothesis (Hi) is accepted and the null hypothesis (Ho) is rejected. Consequently, it can be said that there is a strong correlation between cyber security policy and institutional capacity in the post-COVID-19 era in Nigeria.

Hypotheses Two (H_0): There is no significant association of cyber defence mechanisms in the Nigerian national digital economy before and after the COVID-19 pandemic.

Table 3: Spearman's Rank Correlations Hypotheses Two (H_0)

			ECOSCALE	Impact
Spearman's rho	ECOSCALE	Correlation Coefficient	1.000	.690
		Sig. (2-tailed)	.	.000
		N	95	95
	Impact	Correlation Coefficient	.690	1.000
		Sig. (2-tailed)	.000	.
		N	95	95

** Correlation is significant at the 0.05 level (2-tailed).

In light of this outcome, the null hypothesis (H_o) is not accepted, whereas the alternative hypothesis (Hi) is. Thus, it can be said that there is a significant association of cyber defence mechanisms in the Nigerian national digital economy before and after the COVID-19 pandemic.

Discussion

From the first hypothesis, the findings revealed that a significant positive correlation (r = 0.658; P 0.05) was found between the independent and dependent variables. The probability of accepting the null hypothesis (Ho) is represented by the P value, which is insufficient to meet the decision rule. This finding means that the alternative hypothesis (Hi) is accepted and the null hypothesis (Ho) is rejected. Consequently, it can be said that a strong correlation exists between cyber security policy and institutional capacity in the post-COVID-19 era in

Nigeria. Furthermore, the second hypothesis reveals a significant positive correlation ($r=0.690$; $P<0.05$) was found between the independent and dependent variables. The decision rule is not met by the P value, which indicates the likelihood of accepting the null hypothesis (Ho). This finding means that the alternative hypothesis (Hi) is accepted and the null hypothesis (Ho) is rejected. Thus, it can be said that there is a notable association of cyber de fence mechanisms in the Nigerian national digital economy before and after the COVID-19 pandemic. However, previous studies argued that *the agencies put in place to fight crime do not have the more sophisticated tools they need to deliver services in Nigeria effectively; the study also finds that government policies in Nigeria, as far as cyber security is concerned, are a blueprint, but those policies have not reduced the incessant cybercrime in Nigeria after the COVID-19 era.*

6. CONCLUSION

This study concludes that cybercrime will continue to hamper the plan of Nigeria' prosperity if the government fail to provide tools and capacity for the agencies to fight cybercrime in Nigeria. More so, the study deduces that the improvement in cyber security will redeem the global cyberspace. Meanwhile, the study recommends that there should be policy in place for training and retraining the personnel in charge of managing Nigeria cyberspace. Again, the government at all levels is required to set up institutions and technical infrastructure that would allow for a prompt response to cyber attacks, pointing out that hackers might steal people's and organizations' hard-earned money and confidential information by breaking into devices. In order to avoid becoming victims, people are also urged to use common sense and follow the above preventive measures. Additionally, the government ought to prioritize the welfare and well-being of the citizens of utmost importance. This will lessen the suffering of the citizens and invariably reduce cybercrime in Africa.

7. LIMITATIONS AND SCOPE FOR FURTHER STUDY

Due to the limitations of the scope of this study, the results generated cannot be genera lised. This study was conducted by the EFCC, Lagos Chapter. This is due to a lack of funds to conduct holistic research. Again, the time in which this study was conducted was short. This has further resulted in narrowing the scope to the EFCC, leaving other agencies in doubt. Getting information only from the EFCC cannot be used to genera lise information about cyber security in Nigeria and Africa as a whole.

This study could be better if funds were available in Africa as a whole. This will assist in ascertaining the statistical evidence of cybercrime and the mechanisms that have been put in place to tackle it. The researcher therefore recommends holistic research on this topic in the future research.

8. SOURCE OF FUNDING: *Self*

9. CONFLICT OF INTEREST*: all authors confirmed that there is no conflict of interest.*

REFERENCES

Adegoke, A.; Boakye, B.; and Garson, M. (2022). Cyber security in Africa: What Should African Leaders Do to Strengthen the Digital Economy?

https://institute.global/policy/how-rethink-cybersecurity-africa-strengthen-digital-economy (Accessed 31/7/2022) Retrieved From : https://link.springer.com/chapter/10.1007/978-3-031-18475-8_3

Afifi, T. O., Bolton, S. L., Mota, N., Marrie, R. A., Stein, M. B., Enns, M. W.,... & Sareen, J. (2021). Rationale and Methodology of the 2018 Canadian Armed Forces Members and Veterans Mental Health Follow-up Survey (CAFVMHS): A 16-year Follow-up Survey: Raison D'être Et Méthodologie De L' enquête De Suivi Sur La Santé Mentale Des Membres Des Forces Armées Canadiennes Et Des Anciens Combattants, 2018 (ESSMFACM) *The Canadian Journal of Psychiatry*, *66*(11), 942–950. DOI: https://doi.org/10.1177/0706743720974837

Akinyetun, T. S.; Erubami, P. H.; Salau, J. A.; Oke, B. T.; & Samuel, A. A. (2021). Coronavirus Disease (Covid-19) Pandemic and Violent Extremism in Nigeria: The Two-Faced Agony *African Journal of Terrorism and Insurgency Research*, *2*(1), 69. DOI: https://doi.org/10.31920/2732-5008/2021/v2n1a4

Arinze, U. C., Longe, O. B., & Eneh, A. H. (2020). Regulatory Perspective on Nuclear Cyber Security: The Fundamental Issues, *International Journal of Nuclear Security*, *6*(1), 3. DOI: http://dx.doi.org/10.7290/ijns060103

Ikuero, F. E. (2022). A Preliminary Review of Cyber security Coordination in Nigeria *Nigerian Journal of Technology*, *41*(3), 521–526, DOI: http://dx.doi.org/10.4314/njt.v41i3.11

Ibikunle Busayo Francis Friday Nchuchuwe Ann D. Ojo (2021). FUDMA Journal of Politics and International Affairs (FUJOPIA) Advanced Technological Innovation and the Future of Public Administration in Post Covid-19 Era in Nigeria. The Journal of Politics 3(7):159-170. Retrieved From : https://www.researchgate.net/publication/349882043_FUDMA_Journal_of_Politics_and_International_Affairs_FUJOPIA_Advanced_Technological_Innovation_and_the_Future_of_Public_Administration_in_Post_Covid-19_Era_in_Nigeria.

Ibukun, O., & Jeong, H. K. (2019). Improved photo catalytic efficiency of titanium dioxide-hematite composites by air plasma. *Chemical Physics Letters*, *730*, 259–265. Doi: https://doi.org/10.1016/j.cplett.2019.06.022

Mackenzie, W., White, K., Bernstein, M., & Spencer, S. (2021). Skeletal Dysplasia Quiz, *JPOSNA®*, *3*(2). DOI: http://dx.doi.org/10.55275/JPOSNA-2021-292

Mitchell, J. (2022). *Africa faces a huge cybercrime threat as the pace of digitalization increases.* Investment Monitor. https://www.investmentmonitor.ai/analysis/africa-cyber-crime-threat-digitalisation (Accessed, 31/7/2022). Retrieved From : https://www.retailbankerinternational.com/features/africa-faces-huge-cybercrime-threat-as-the-pace-of-digitalisation-increases/?cf-view

Monguno, M. B., Igbokwe, I. O., & Egbe-Nwiyi, T. N. (2021). Protein, electrolyte contents, and histopathology of longus colli muscle in cachexia of Red Bororo beef cows, *Comparative Clinical Pathology*, *30*(2), 327–333. DOI: https://link.springer.com/article/10.1007/s00580-021-03218-z

Narodowy Bank Polski (NBP) (2020): Initial monetary policy response to the COVID-19 pandemic in inflation targeting economies. NBP Working Paper No. 335. Retrieved form: https://static.nbp.pl/publikacje/materialy-i-studia/335_en.pdf

Odumesi, J. O. (2014): A socio-technological analysis of cybercrime and cyber security in Nigeria. *International Journal of Sociology and Anthropology*, *6*(3), 116–125. DOI: http://dx.doi.org/10.5897/IJSA2013.0510

Okunoye, B. (2022). Digital identity for development should keep pace with national cyber security capacity, with Nigeria in focus. *Journal of Cyber Policy*, *7*(1), 24-37. DOI: http://dx.doi.org/10.1080/23738871.2022.2057865

Osho, O., & Onoja, A. D. (2015). National cyber security policy and strategy of Nigeria: a qualitative analysis *International Journal of Cyber Criminology*, *9*(1), 120. DOI: http://dx.doi.org/10.5281/zenodo.22390

Ukwuoma, H. C., Williams, I. S., & Choji, I. D. (2022). Digital Economy and Cyber security in Nigeria: Policy Implications For Development *International Journal of Innovation in the Digital Economy (IJIDE)*, *13*(1), 1–11. DOI: http://dx.doi.org/10.4018/IJIDE.292489.

Union Budget (2022). Explained: Finance Minister Nirmala Sitharaman Tuesday presented the Union Budget 2022-23 in Parliament. Here are the highlights from Sitharaman's Budget speech, and an explanation and analysis of it. Retrieved form: https://indianexpress.com/article/explained/union-budget-2022-explained-nirmala-sitharaman-live-updates-7750628/