OPEN ACCESS Freely available online

Journal of Political Sciences & Public Affairs

Review Article

Globalization and Emergence of Cyber Crimes in Nigeria; the Yahoo Boys Syndrome

***Onota emmanuella**

Department of political science and diplomacy, Nigeria

ABSTRACT

The rise of cybercrimes in Nigeria has eaten deep into the fabrics of this nation and globalization which is not a new phenomenon is seen as the foundational cause of cybercrimes in Nigeria and other countries who are suffering from the same social menace. Although the author faulted the activities of the yahoo boys which includes internet frauds, counterfeits, extortion, phony scams, unsolicited bulk electronic messages, porn, internet gambling, etc. on the greed of these perpetrators and on the advent of globalization, the author did not however fail to ignore the role the Nigerian government play in this social decadence through their non-commitment in fulfilling the needs of the citizens. Consequently, this paper explained the meaning of globalization, cybercrimes and also tried to clarify the what ''yahoo yahoo'', an infamous term means in regards to this work. The thrust of this work was to find a relationship between globalization and cybercrimes and through its findings, a relationship was established and the gap the author sought to fill was accomplished. For proper investigation and research, this paper relied on secondary sources of data collection to draw objective conclusions and make recommendations for existing literature and practice.

Keywords: Globalization; Cybercrimes; Yahoo Boys; Government; Development

INTRODUCTION

As recent as the 21st century, globalization is still an ongoing issue that has raised a lot of debates amongst various scholars in academics regarding the impacts of globalization and whether it has done more harm than good or not. For the purpose of breaking down barriers of state boundaries, globalization set goal was to make the world a global village where countries across the world would interconnect for economic and socio-cultural development. Country and individuals have become abreast with technology as a result of the increase in the participation of both developed and less developed countries in the globalization process so much that they are now experts in the usage of technology. Although the awareness and knowledge of technology is advantageous to individuals and states, youths all over the world have used this opportunity to satisfy their own desires and make a living for themselves which cannot be achieved without defrauding other individuals who fall prey to them. It wouldn't be a neutral judgment to fault the perpetrators of these cyber-crimes also tagged ''yahoo boys'' because if the government provides sufficiently for its citizens which should include the provision of job opportunities, rather than resorting to illegal activities for their daily survival, because according to the old saying, ''an idle mind is a devil's workshop''. Abimbola (2013) posed an argument claiming that two edge functions has been introduced as a result of information technology revolution associated with the internet. These are; provision of meaningful values to the world and the generation of a large amount of ailments that challenge society's order with a new wave of crime inclusive. In regards to what has been stated earlier about the life style that has been adopted by some Nigerian youths in current times, this statement concurs with it. It is bad enough that Nigeria is still struggling to maintain its status as the giant of Africa giving its persistent economic backwardness and political instability, it will however be worse if Nigeria is excluded from global trade transactions just because of the illegal crimes perpetuated by its citizens on other foreigners because according to an analysis conducted, youths that engage in cybercrimes

***Correspondence to:** Onota Emmanuella, department of political science and diplomacy, Nigeria, Tel: 08120817822; Email: ellaonotee007@gmail.com

Received Date: March, 29, 2021; **Accepted Date:** September 6, 2021; **Published Date:** September 16, 2021

Citation: Emmanuella O (2021), Globalization and Emergence of Cyber Crimes in Nigeria; the Yahoo Boys Syndrome; J Pol Sci Pub Aff: 9 p240.

usually pick foreigners as their victims and this can affect diplomatic relations between Nigeria and other prospective countries which will in turn hamper on the nation's productivity (Onota, 2020).

The anonymity provided by the internet has increased the activities of yahoo boys in Nigeria in terms of fluidity and complexity. Without leaving their comfort zones, they can now access the internet. Fraudulent conversion of property, internet frauds, fictional property, vehicle purchases and fictious business transactions all take place without leaving a trace (Reddick and King, 2000).

As earlier mentioned, as a result of the action and inaction of non-state actors, the government's stance in cyber-crime has been illustrated. Looking at the government contribution to youth-crime bracketing, Nigeria's inability to implement many laudable National Rolling Plans since the country's independence has been emphasized by Nigerian Institute of Social and Economic Research (NISER) review (2001). Weak economic policy implementation, lack of data to help plan execution and resource constraints are factors that contributed to this failure. These gloomy conditions triggered a slew of economic issues including soaring public debt, soaring unemployment, falling gross domestic product, dwindling foreign exchange reserves, exchange rate decrease, persistent rise in the prices of goods, insufficient basic consumer goods and living standards in low levels (p175).

From the above premise, this paper evaluates globalization, the origin, dynamics and the effects of cybercrimes on Nigeria's socio-economic growth with a focus on Nigerian youths in these cyber-crimes. The study relied on secondary source of data collection making use of books, journal articles, internet materials and publications.

Conceptual Discourse and Literature Review

Globalization is one of the numerous concepts in social science that does not have a universally acceptable definition; it is a multifaceted concept that various scholars have defined based on their perspectives. This section would therefore conceptualize the key terms of this paper which are globalization and cybercrimes. In doing this, it would also review literature around cybercrimes and globalization which will give a better understanding to the scope of this paper.

Globalization

AL brow (1990) has defined as "all those processes by which the people of the world are incorporated into a single world society". Also for McGrew (1992), Globalization includes a number of interconnectedness which reaches across nations, states and societies that constitutes the contemporary world. It explains how the implications for people and communities in other parts of the world are as a result of the events, decisions and activities in another part of the world. Globalization has been described as a process of financial and economic integration by Cerny (1995), Jones (1995) and Bairoch & Kozul-Wright (1996). Globalization according to Cerny (1995), is a group of economic and political structures and processes that make up the foundation of the international political economy resulting from the changing character of the goods and assets, particularly the increase in structural differentiation of those goods and assets. As a result of the growth of competition in an international free trade environment exacerbated by the diffusion of technology, ''Globalization can simply be an intensification of the process of international interdependence, Jones (1995) suggested. The process in which countries production and financial system become increasingly intertwined through a hike in the number of cross border transactions, leading to international division of labor where the wealth creation of a nation depends on economic agents in other countries and the ultimate stage of economic integration where such dependence hits its peak has been described as globalization by Bairoch & Kozul-Wright (1996).

A number of scholars have made to attempts to explain globalization from their various points of views, but it is necessary to understand that globalization is not a new notion in the context of this research work. As part of the process of expansion across continents, migration, commerce, warfare, military alliances, conquest, discovery, colonization and new technology are all inclusive. From the ancient days to present times, the world has threaded into interconnected patterns that have weakened and strengthened overtime through interactions amongst nations, cultures and people. The result of the globalization process is defined by unpredictable, far-reaching and continuing shifts (Hebron & Stack, 2013).

Cyber Crimes

The secretary General of the Anti-Phishing Working Group known as Peter Cassidy coined the term ''cybercrime'' to distinguish computer programmes and coordinated interlocking sets of programmes designed specifically to animate financial crimes in relation to other types of malicious software (Shehu, 2014). According to Halder and Jaishankar (2011), cybercrime is characterized as crimes directed against a person or group of persons with a criminal disposition to taint the victim's image or cause physical or mental harm to the victim using modern telecommunication networks such as internet (social media, e-mails, notice board and groups) and mobile phones. This term confines cybercrime to illegal activities carried out with the assistance of the internet and directed at people and groups. Kamini (2011), on the other hand defines cybercrime as unlawful acts committed using the computer as a weapon (for example internet frauds, counterfeits, extortion, phony scams, unsolicited bulk electronic messages, porn, internet gambling, intellectual property crime, cyber defamation, cyber stalking and so on) or a pre-selected suspect (e.g. unauthorized access to computers networks, electronic information theft, denial of service attacks, malware, malicious codes, e-mail bombing, logic bombs, web jacking, internet time theft, Trojan attacks etcetera). This supports the claim that all cybercrime victims are both the computers and people; it just depends on which of the two is the main focus.

Yahoo boys; this is a term borrowed by the author to describe the activities of Nigerian internet youth fraudsters.

The Dynamics and Nature of Cybercrimes in Nigeria

It is no longer news that cybercrime is a reoccurring social vice in the country Nigeria. It is a source of concern for the nation and the need to curb this social vice should be amongst the topmost priorities of government officials. The internet offers limitless educational, social and economic opportunities thanks to technological advancement. However due to the unique characteristics of cybercrime, the internet still poses its own set of threats. According to a recent study in the Daily Trust (2010 cited in Maitanmi et al 2013; Folashade and Abimbola, 2013) by the internet crime complaint centre, Nigeria is ranked third amongst the top ten sources of cybercrime in the world behind the US by 8% (65%) and the UK (9.9%). Furthermore, Nigeria is ranked first in the African region as the focus and root of malicious cyber activities, according to Ribadu (2007), and this is spreading across the West African sub-region. As a result of technological advancement, the nature of cybercrime in Nigeria is constantly changing. More so, Kamini (2010) believes that tool cybercrimes takes centre stage amongst cybercrimes in Nigeria. This means that rather than specifically targeting computers, cyber criminals in Nigeria often use computers and the internet to defraud and damage others. This, he claims, is because Nigerians have yet to acquire the technological expertise needed to indulge and commit targeted cybercrimes. According to Saulawa and Abubakar (2014), because of the less technological sophistication required on the part of criminals, cybercrime in Nigeria is particularly directed at individuals rather than computer networks. Using a variety of computer and telecommunication tools, these types of tool cybercrimes are common in Nigeria. According to Ribadu (2007), majority of cybercrimes in Nigeria include website cloning, false claims, internet purchases and other types of e-commerce fraud. Website cloning, financial fraud also popularly known as Yahoo-Yahoo, identity theft, credit card theft, cyber theft, cyber stalking, fake electronic mails, cyber laundering and virus/ worms/ Trojans were also highlighted by Olugbodi (2010) as the activities associated with cybercrimes that are carried out by these fraudsters.

The examples given here vary from bogus lotteries to the most sophisticated internet scams. Four Nigerians who were accused of running a fraudulent scam on the internet to defraud foreign investors in Ghana were apprehended by security agents in July 2001. As a result of their actions, prospective investors are estimated to have lost many millions of dollars. A 16 years sentence was delivered to Mike Amadi on the basis of creating a website that advertised lucrative but fake procurement contracts. Posing as an Italian businessman, an undercover agent caught the man pretending to be an EFCC Chairman. Amaka Anajemba who was sentenced to 2½ years in jail, perpetrated the biggest scam of all. She was directed to return $25.5 million of the $242 million stolen from a bank in Brazil with her assistance. The Sunday punch newspaper published an article on July 16, 2006 about a Nigerian woman who 24years of age named Yekini Labaika of Osun and a 42 years old American nurse named Thumbelina Hinshaw who were searching for a Muslim man to marry. The man misled the victim by owing claim to name known as ''Phillip Williams'', an American who was a Muslim and was working for an oil company in Nigeria and he proposed marriage to the woman. The fraudster invented questionable methods to defraud the victim of $16,200 and numerous useful materials. After being found guilty of eight counts against him, he was sent to jail with a total of 19½ years. These kinds of incidences are becoming more common and several young men continue to carry out these criminal actions, robbing unsuspecting individuals and organizations. The EFCC has recently launched a major crackdown on the so-called ''yahoo boys''. Officers of the Economic and Financial Crimes Commission (EFCC) arrested 94 people accused of being ''yahoo boys'' during a raid in one night club in Osogbo, Osun state capital on October 14th, 2019. In an interview with journalists, the EFCC chairman, Mr. Ibrahim Magu reported that the commission has made 200 arrests of internet fraud suspects also known as ''Yahoo Boys'', in October alone. . According to Magu, Ismalia Mustapha a.k.a Mompha; and his Lebanese accomplice, Hamza Koudeih have become the biggest catch of the commission. The suspects, he said, laundered a total of N33billion as ''kingpins of an Organized Cyber Syndicate Network''. ''Five wristwatches with a money value of over N60million were recovered from Mompha at the point of arrest'', Magu said. '' Further research into the case revealed that he owns fifty-one bank accounts in Nigeria from which he purchased properties in Dubai and embezzled approximately N14billion through Ismalob Global Investments Limited. Koudeih, his partner in crime also has companies in his name, THK Services Limited and CHK Assets Limited which he allegedly laundered around N19billlion. The arrests, according to EFCC president, demonstrate the agency's zeal to tackling economic offenses and corruption. Magu said that youths who were mostly involved in cyber fraud needed to be educated about the implications of their behavior, not only for their own future but also for the country's image and economy. He reaffirmed that for those who are willing to turn a new leaf, the commission is committed and ready to assist them in putting their talents to good use in order to ensure that their abilities are positively implemented in helping to create a better society (Punch News, 2019).

More recently, the Dubai police on 25th June 2020 apprehended Nigerian fraudster Ramon Olorunwa Abass also known as ''Hushpuppi'' along with other members of his gang in Dubai. The 12 suspects were apprehended in six separate searches by the Dubai's police unit according to the reports by Guardian Newspaper. The gang was accused of defrauding over Dh1.6 billion (approximately N169 billion) from 1.9 million victims. There was also confiscation of items worth over N15.845 billion (Dh 150 million).

Theoretical Foundations

Globalization and how it contributes to cybercrimes can further be understood through the application of the risk society theory popularized by a German Sociologist known as Ulrich Beck. Beck's study is an attempt to comprehend the extraordinary shift in social attitudes and fears as well as an examination of the interstitial forces at work between social structures, technology, political and scientific as well as the risks that these

pose to individuals and society as a whole. For Beck (1992), risk society is defined as "a systematic way of dealing with hazards and insecurities induced and introduced by modernization itself".

An obvious result of industrial modernity's success according to Beck, has been its ability to cross borders, its vast spatial spread and also its ability to penetrate cultures. Globalization, on the other hand, is not a benevolent operation. Globalization threatens the nation-territoriality state and sovereignty, limits the state's and citizen's ability to function unilaterally and independently, and jeopardizes economic sovereignty by pressuring states to act and enact policies that are broadly in line with the whims of highly mobile capital. Risk society according to Bell (1998 cited in King and McCarty, 2009) is a ''society where rather than class contestations over the distribution of wealth and resources, central political conflicts are non-class based contestations over the distribution of technological risk". As a result, radioactivity, air bone and waterborne emissions and mass transportation hazards such as aircraft, truck, or train accidents as well as cybercrimes are all technical dangers in which every person is vulnerable to in the risk society. Paradoxically, this suggests that scientific and technological progress creates new types of unintended threats and has serious societal implications.

This theory discusses how the emergence of globalization has negative implications for individuals and society alike. In today's world, technological progress is continuous and technology creates new types of threats which we must continually adjust to and adapt to. The risk society, Beck argues includes a whole series of interrelated changes within modern social life such as shifting employment patterns, increase in job insecurities, cybercrimes and declining influence of tradition and custom. With the world shrinking into one global community, the globalization process is accelerated by information communication technology, which eliminates distance and space barriers between countries. As a result, the positive impact of the information technological revolution on society's growth cannot be overstated; but like any other technical breakthrough, it came with unintended consequences, one of which is cybercrime. Hacking, abuse and online scams are some of the threats which internet users are vulnerable to. There is a lot of danger that can spread with a single click of the mouse given the billions of computers with billions of users that the internet hosts on a daily basis. We now live in an information society that generates unpredictable risks such as property theft, embezzlement of money, insurgency, and so on that are largely virtual, invisible and most likely irreversible, resulting in a ''Risk Society'' for individuals, organizations and governments with serious consequences for technological and socio-economic prosperity.

Plausible Causes of Cybercrimes in Nigeria

Several scholars have brought forward their own views regarding the reasons and causes behind cybercrimes both in the global context and the Nigeria context. In this regard, Kamani (2011) cites the following reasons:

- The ability to store massive amounts of data in a relatively limited amount of space.
- Human errors are caused by difficulties of computer software and programs.
- Human error in cyber defense gives cyber criminals easy access.
- The regularity in the loss of data as cybercrime is related to evidence destruction, it makes it almost impossible to prosecute criminals.
- Within the Nigerian context, Hassan, Lass and Makinde, (2012) adding to the list identified the following causes of cybercrime in Nigeria:
- Rapid urbanization.
- The rise of the ''yahoo boys'' sub-culture amongst youths has been aided by the political leadership's corruption.
- Increasing youth Unemployment.
- The pursuit of money, values for materialism and bad mentors.
- Lack of enforcement of cybercrime legislation and unavailability of equipped departments.
- More specifically, Nigerian youths are knowledgeable in regards to the EFCC's presence and have even praised some of their operations. However, what has severely tarnished its reputation and by extension its effectiveness is attributed to the use of it as an instrument by the political class.

Impacts and Challenges

The effects of cybercrimes have a lot of impacts on the social and economic development of Nigeria and these impacts creates challenges for the government, the youths and the international community. According to Ehimen and Bola (2009), the internet has turned into a geometric development and accelerated windows of open doors for companies, as well as the elimination of economic barriers that countries around the world had previously faced. With these innumerable benefits of the internet, it is easy to see why for national development to thrive in a third world country like Nigeria, the internet is a significant tool that is needed. Cybercrime practices such as cyber stalking, abuse, and extortion, as well as cyber terrorism, according to Shehu (2014), pose a social threat to people's right to privacy and fundamental rights. Similarly, cybercrimes such as pornography, child predation, online prostitution, online gambling compromise society's morality, and place society at risk of social standard breakdown. Cybercrime has an effect on the country's socioeconomic development because knowledge from the country is regarded as suspect due the criminal aspect renders it unreliable, inaccurate, and untrustworthy (Iwarimie-Jaja 2010). According to Abimbola (2013), cybercrime impedes the country's socioeconomic growth because it fosters a lack of trust and faith in profitable transactions, encourages the denial of innocent Nigerians opportunities abroad, and results in job losses and revenue loss. Furthermore, according to the findings of Maitanmi et al (2013) due to the low level of trust cybercrimes has generated in the Nigerian economy, cybercrime impedes Nigeria's socio-economic growth by driving away foreign investors.

According to the above addressed so far, cybercrime's implications and challenges are still apparent, with numerous

possible negative consequences for Nigeria's socioeconomic growth. In summary, the following are some of the effects;

Cyber-attacks on companies and organizations have the potential to harm an organization's image as well as cause consumers and sales to disappear. ii. In the international scene, Nigeria's reputation has been tarnished by widespread cybercrime, rendering the country at risk for foreign investors. iii. Cybercrime has harmed Nigeria's confidence in the digital economy thereby stifling economic development. iv. Financial damages incurred by companies and customers as a result of data and money theft or extortion attempts to slow down economic growth and development. v. Cyber-attacks on Nigeria's critical infrastructure could result in both immediate and long term economic losses. vi. Organizations and businesses bear significant cost as a result of the need to develop measures to combat and respond to cyber-attacks. vii. While putting a strain on law enforcement agencies, time and resources, cybercrime also has the potential to increase other criminal operations. viii. Personal financial resources are depleted, resulting in emotional distress. ix. Finally, it has resulted to expenses incurred from re-establishing credit records, accounts, and identities for government agencies and governments as well as well as the loss of company assets.

Recommendations and Conclusion

The author brought forward the following recommendations with the hope that these recommendations will enlighten the youths, government and policy makers on how to curb cybercrime so it will be reduced to its barest minimum. They include the following;

- Provisions for Education: Since education is a significant tool for literacy, frequent seminars and workshops on cyber security need to be conducted so that people can learn how to protect their personal information and youths can avoid being victims of cybercrime. We will need to inform businesses and organizations about the best security management practices. For instance, some large companies already have a policy requiring all systems under their control to conform to rigorous security standards. Furthermore, computers and servers on the internal network receive automatic updates and no novel device should be allowed online till it complies with the security policy.
- Imposition of Cyber Ethics and Cyber legislation Laws: For cybercrime to be tackled, cyber ethics and cyber laws need to be developed. Every person has a duty to obey cyber ethics and laws in order to minimize the growing number of cybercrimes. To stay safe from cybercrimes, all computers should have security software installed, such as anti-virus and anti-spyware. iii. Provision of employment opportunities:
- Provision of Employment Opportunities: Jobs should be provided by the government and private sectors for recent graduates in order to impair the number of youths who are committing involved in cybercrimes. To achieve this, vocational skills and entrepreneurial development programmes requires establishment in situations where these jobs are not readily available.
- Punishment of offenders; the government should mandate law enforcement authorities to implement strict and robust regulations that persecute offenders in order to significantly minimize the rate of cybercrimes in the country.
- Lastly, embassies and travel agencies in Nigeria should adopt the policy of undergoing background check on individuals who are seeking visas to travel abroad. Through this policy, visa seekers will be thoroughly checked so as to know the details that are necessary to convince the embassies that they are clean from criminal records and their reason for travelling are for legit purposes. However, for such a policy to be effectively implemented, the government has to be supportive and provide monetary assistance.

CONCLUSION

The reoccurring menace inflicted on Nigeria as a result of cybercrimes have become a significant issue that if the government does not increase its efforts in curbing this social vice, years from now it will spin out of control and its effects will be disastrous. As shown in the arguments in this paper, not all the blame can be put on the youths as it is a reality that every action leads to a reaction. The action here is the inability of the government to perform its duties in making its citizens comfortable through the provisions of basic amenities and these actions prompts the reaction of the citizens in Nigeria especially the youths were they have to go extra miles to survive even if it means engaging in criminal activities because they have lost all hope in the government. From the foregoing, this paper concludes by giving its recommendations stating that the both the government and citizens should cooperate on a regular basis to put an end cybercrimes as cyber security is important in improving the socio-economic development of the country and maintaining the image of Nigeria in the face of the international community.

REFERENCES

1. Abimbola K.A (2013): The Nature, Causes and Consequences of Cyber Crime in Tertiary Institutions in Zaria-Kaduna State, Nigeria. American International Journal of Contemporary Research.
2. Albrow. (1990). Globalization, Knowledge and Society: Readings from International Sociology. Sage Journals.
3. Bairoch, P., & Kozul-Wright, R. (1996). Globalization Myths: Some Historical Reflections on Integration, Industrialization and Growth in the World Economy. United Nations Conference on Trade and Development.
4. Beck, U. (1992). Risk Society: Towards a New Modernity. London: Sage.
5. Cerny, P. G. (1995). Globalization and the Changing Logic of Collective Action. International Organization.
6. Ehimen, O.R. and Bola, A. (2010). Cybercrime in Nigeria. Business Intelligence Journal, 3(1).
7. Halder, D., & Jaishankar, K. (2011). Cybercrime and the Victimization of Women: Laws, Rights and Regulation. Hershey,
8. Hassan A.B, Lass F.D & Makinde, J. (2012): Cybercrime in Nigeria: Causes, Effects and the Way Out. ARPN Journal of Science and Technology.
9. Hebron, L., & Stack Jr, J. F. (2013). Globalization: Debunking the myths. Dorling Kindersley India Pvt. Ltd.

10. Iwarimie-Jaja D. (2010): Criminology, Crime and Delinquency in Nigeria. Port Harcourt, Pearl Publishers.
11. Jones, R. B. (1995). Globalisation and Interdependence in the International Political Economy: Rhetoric and Reality. London: Pinter.
12. Kamini, D. (2011): Cyber Crime in the Society: Problems and Preventions. Journal of Alternative Perspectives in the Social Sciences,
13. Maitanmi O., Ogunlere S, Ayinde S, & Adekunle Y. (2013): Impact of Cybercrimes on Nigerian Economy. The International Journal of Engineering and Science (IJES),
14. McGrew, A. G. (1998). Global Legal Interaction and Present-Day Patterns of Globalization. Emerging Legal Certainty: Empirical Studies on the Globalization of Law, Aldershot and Brookfield: Ashgate and Dartmouth,
15. Meke, E.S.N. (2012): An article "Urbanization and Cyber Crime in Nigeria: Causes and Consequences".
16. Nigerian Institute of Social and Economic Research (NISER) (2001). The State in Nigerian Development. NISER Review of Nigerian Development 2000. Ibadan, Nigeria: College Press and Publishers Ltd.
17. Reddick, R., & King, E. (2000). The Online Student: Making the Grade on the Internet: Forth worth: Harcourt Brace.
18. Ribadu, E. (2007). Cyber Crime and Commercial Fraud; A Nigerian Perspective. A paper Presented at the Modern Law for Global Commerce, Vienna .
19. Saulawa, M.A and Abubakar, M.K (2014): Cybercrime in Nigeria: An Overview of Cybercrime Act 2013. Journal of Law, Policy and Globalization,
20. Shehu A.Y (2014): Emerging Issues in Cyber-Crime: Causes, Implications and Effects for the Legal Profession. Online Journal of Social Sciences Research .
21. Thomas, C., & Wilkin, P. (1997). Globalization and the South. Palgrave Macmillan.