Available online at https://asric.africa/social-sciences
ASRIC Journal on Social Sciences and Humanities Vol. 5(1)(2024) 118-126

Interrogating Globalization and its Implications for Cybercrime in a Globalized World

Adejoh Sunday[1], Olumorin. M. Olukemi[2]

[1]Department of Defence and Security Studies, Nigerian Defence Academy Kaduna
Sunday.adejoh@nda.edu.ng
[2]Prince Abubakar Audu University Anyigba. Kogi state
olumorinkemi@gmail.com

Corresponding Author: Sunday.adejoh@nda.edu.ng

Received 09 April 2024; revised 29 May 2024; accepted 04 June 2024

Abstract

The international system reflects a web of relations between and among countries with each projecting its national interest. The relationship between states within the international system has become more enhance as a result of globalization. Advancement in science and technology especially in relations to information and transportation technology constitute a major driver of globalization. Crime and criminality is a characteristic of the international system. The dynamism of the international system also make crime dynamic. Globalization has brough about newer forms of crimes that hitherto where non-existent. This paper therefore is an attempt to interrogate the nexus between globalization and crime. This paper therefore argued that cybercrime is possible because the world has become a global village. A migration from the analogue way of doing things to a digitalised and computarised way also brought about the migration of crime from analogue to digital. This paper is a desk research and it dwells basically on secondary data. This paper identified illicit financial flow, internet fraud, hacking, cyber bullying, malware, phishing, cyberstalking, cyberterrorism among other as examples of cybercrimes. It is the position of the paper that effective security system of states in this era of globalization must encapsulate cyber security. It recommends amongst others the need for states to put in place effective and efficient cyber security policies and measures to prevent cyber-related crimes.

Key Words: Cyber, Cybercrime, Security, Globalization, interconnectedness, Computer

Introduction

In contemporary world system, globalization remain the most dominant trend of all social, economic and political phenomena which is being driven particularly by a new wind of information technology that is unparalleled in the history of humankind. Nation states have consistently intensified efforts towards engaging in business across national borders and constructing production and distribution networks on a global scale (Ogoh, 2012). Thus, the world today is a global village given the unprecedented level of inter-connectedness of political, economic, social and technological forces that permeate contemporary international system.

Globalization is a phenomenon that is fast growing in both out of some natural as well as man made efforts. The emergence of a globalized world stems from the natural development of life which is spurred by the advancement of civilizations which are themselves occasioned by the overflow of technology in information and telecommunication. The internet, the global system for mobile communication (GSM), the telephony, the Satellite Television, the air transportation system, etc, have reduced the globe into a small but complex village. These factors have naturally narrowed the boundaries of otherwise very distant regions

to very close neighbors. The new technologies have drastically reduced people's perceptions of communities (Mathews, 1997). Remarkable political and economic issues that occur in distant lands such as Middle East or Australia become issues in Japan in faraway South-East Asia, Brazil in South America and Ghana in Africa thousands of miles across the Atlantic Ocean just in a matter of seconds. For instance, the our break of the Convid-19 in China in the year 2020 caused the countries of the world to lock down as to prevent the spread of the deadly disease across nations, also the financial crisis that has rocked the mortgage institutions in the United States of America which has seriously affected her entire economy had negatively impact on the entire world, thus forcing nations across the globe to strategize and bring up remedial economic approaches to prevent the breakdown of their own respective economies.

According to different scholars (Khor, 2008; Aluko, 2001; Gorstein, 2011), globalization is "the widening, deepening and speeding up of worldwide interconnectedness in all aspects of contemporary social life. The interconnectedness is in so many ways which includes among others: trade, communications, monetary, technical, scientific, technological and cultural. It is the process of reducing the entire world in to a global village which it is enhanced through technological development. Economic, social demographic and technological forces are dramatically altering relationships among nations as well as the nation and politics.

From the above definition of globalization provided by various scholars, globalization is therefore characterized by interconnectivity of different cultures, lifestyle, norms, and believes of various countries across the globe for the sole purpose of breaking down state barriers and achieving all round development and growth. It can also mean the removal of national barriers to achieve transfer of new technology, expansion of trade, financial integration and the formation of a global market that will cut across all states. 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 outcome of the globalization process are characterized by unpredictable, far-reaching and ongoing changes (Hebron & Stack, 2013). A more serious issue with globalization is that it allows criminal activities to flourish by leveraging new technology and as such there are referred to as cybercrimes.Paradoxically, this suggests that scientific and technological progress creates new types of unintended threats and has serious societal implications.

Concept of Cybercrime

Cybercrimes refer to illegal, unethical and unauthorized behavior in a system that processes information or transfers data using computer and communication technologies (Okutan & Cebi 2019). Cybercrime is also defined as unlawful or unacceptable acts committed by using electronic devices, including computers as either a target or a tool (Vadza 2011). These crimes comprise of illegal acts such as laundering, theft, fraud, hacking, forgery and defamation as highlighted in the Information, Communication and Technology Act 2000. Cybercrimes have been changing over the years with new techniques adopted by cyber criminals to target their victims online from individuals to international organizations. In recent years, the use of the internet, for instance, online banking and e-payments have exposed end users to online crimes (Lavorgna & Sergi 2014, Oruç & Tatar 2017). Studies have shown that Nigeria, Russia, China and Brazil is significantly affected by cybercrime (Doyon-Martin, 2015). In a tech-savvy world, the internet has so far created a breeding ground for contemporary crimes such as hacking, cyber terrorism, child pornography, spam, intellectual property piracy, denial of service and stalking among others. In essence, these crimes were practiced in the real world, but with the emergence of the internet, they escalated and became a concern for countries to deliberately embark on cyber security measures to protect their citizen's privacy and classified information stored in their intelligence systems. However, in the banking industry, the most dominant cybercrimes are phishing, Bank Verification Number (BVN) frauds, theft of bankcards, identity theft, cyber stalking and counterfeit online banking websites (Wada & Odulaja, 2012; Omodunbi et al. 2016).

Kamani (2011); Meke (2010); Hassan, Lass & Makinde, (2012) have advanced the following reasons and causes of cybercrimes which includes: 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; rapid urbanization; the pursuit of money, values for materialism and bad mentors; increasing youth unemployment; the regularity in the loss of data as cybercrime is related to evidence destruction, it makes it almost impossible to prosecute criminals

Cybercriminals are taking advantage of globalization as they go to places where the regulation is not that strong. In practice, cybercriminals often attack the global economy from nations where law enforcement agencies often pay no attention to the establishment of websites that are created to spread or sell malware. Cybercrime has an impact on the international system as a whole, cyber-attacks cause a major obstacle for global economic growth due to its damaging effects on innovation and the theft of ideas even as President Obama observed that the "cyber threat is one of the most serious economic and national security challenges we face as a nation" and that "America's economic prosperity in the 21st century will depend on cyber security". It is in the light of this background that we examine the nexus be between globalization and cybercrime.

Concept, Nature and Process of Globalization

Globalization is a phenomenon which cuts across entire world, and it means different things to different people. According to Albrow (1990), it is 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 the implications for people and communities in one parts of the world areas are affected by the results or events, decisions and activities in another part of the world. The current reality of the globalization phenomenon is 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 (Bairoch & Kozul-Wright, 1996).

Okpeh (2000) sees globalization as a process of change in which the world's countries and their economics are increasingly integrated as a function of rising cross-border economic and cultural activities. Vaughan (2005) was of the opinion that globalization is associated with the notion that the great scientific and technological advancements have revolutionized the way societies are organized and priorities around which they are ordered. Ubi (2008) remarks that it is a process of homogenization of the world along western world standards that have to do with spread of deregulation forces of technology, production, trade and finances across borders.

Mark (1999); Baylis & Smith (2001) has pointed out that globalization is the process of continuing integration of countries in the world that is strongly underway in all parts of the world. Supported by accelerated pace of technological change, by price and trade liberalization, and by growing importance of supranational rules, globalization has exposed national economies to much more intense competition than ever before. Many decry the inability of third world nations in reaping the dividends of globalization. They insist that even though most developing countries have been told to open up their economies, and receive development, they only ended up growing poorer. Despite the well-publicized claims of export and income gains, nothing as yet is there to show for it (Khor, 2000). Developing countries whose economic and social fabrics are rapidly being dislocated by extensive financial and trade liberalization is surely leading to gross inequalities of wealth and opportunities with the ultimate results to heightened poverty in their land.

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, Jones (1995) suggested that Globalization can simply be an intensification of the process of international interdependence. According to Kellner (1989), today's world is organized by accelerated

globalization, which is increasing the dominance of a multinational capitalist economic system, displacing national sovereignty with transnational corporations and organizations, and at the same time eroding local cultures and traditions through a global society. The new global economy and culture can be defined as a network society based on modern communications and technology as its foundation (Castell, 1998). Globalization is seen by some as a force for prosperity, wealth, equality, democracy and happiness, as well as a continuation of modernization. Others consider it to be yet another form of encroachment. Globalization is seen as negative by critics who see it as a force that increases wealthy and first world's countries dominance and power over poorer and third world countries. They believe it widens the divide between the have and have-not (Castell, 1996).

Globalization according to social theory entails the movement of goods, money, technology, ideas, cultural types, and people across national borders through a global networked society (Castells, 1998). Globalization is thus essential for global economic development and growth as it has also brought modernization to third world countries, through it there been a transfer of technology which reduces the stress involved in human labour which has been substituted over time with the use of machines. Furthermore, there is the advantage of communication between individuals across the globe for the purpose of business transactions, cultural and diplomatic interactions. With the emergence of globalization, individuals in the underdeveloped world are now abreast with new technology which has been able to broaden their horizon and make them able to compete favorably with other developed nations in the global market.

Globalization has both positive and negative effects, as well as opportunities and challenges. There are various positive effects or advantages, but the most significant are improved specialization and productivity, as well as higher quality goods at lower prices. Economies of scale in manufacturing, increased productivity and competitiveness, technical advancements and increase in managerial capabilities. Since the highest standards of quality are maintained through specialization and competition, consumers benefit from the increased global trade and output which are made possible by globalization. Furthermore, as individual welfare improves across countries, the volume of goods and services also increases.

Just as globalization has positive effects, it also has its downsides which has to do with countries with low-skilled work force as globalization increases unemployment. This is attributed to globalization as a result of increased labor mobility. Globalization in general tends to increase policy interdependence while decreasing national policy autonomy, especially in countries with low income competitiveness. The rapid integration of financial markets has dramatically altered the environment in which national policy makers execute monetary and financial policies. The proliferation of derivatives and off-balance sheet instruments as well as the liberalization of capital controls, have made it difficult to target monetary policy effectively. Another issue with globalization is the rapid transmission of shocks and disturbances from one financial market to the next. Despite the fact that such shocks can withstand large markets, they still pose risk to macroeconomic stability.

Nexus between Globalization and Cybercrime

The concept of globalization highlights the interconnectedness and the evolving of the society at a global level. Different aspects of the society are transformed by global dynamics to create an environment that stimulates interactions and integration of people and the wider society and economy. This transition of the modern world where the world is dubbed as a global village, has increased multicultural societies and borderless space, technological advancements and global environment. Given these diverse dynamics, globalization entails the worldwide changes in economic infrastructures and the associated emergence of global markets and a global trading system (Huynen et al. 2005). In this sense, global processes involve the increase in mobility of people, the interdependence among nations that, in turn, calls for alternative global governance structures. On the same note, in this digital era where information is at our fingertips, within an instant, information is shared rapidly on online platforms or the internet in a paperless environment. The internet is widely regarded as a way of exposing the world to a diverse array of ethnics, technology, religions, cultures and lifestyles among others. However, globalization has exacerbated online crimes such as cybercrimes.

It is argued that globalization is the motivating factor behind the trends of cybercrimes in different parts of the world. 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, groups, organizations and even countries.

The advent of new waves of crime has tainted the internet's contribution to the nation's progressive growth. The internet has evolved into a haven for the most lucrative and discreet forms of criminal activity. From Europe to America, Africa to Asia, cybercrime has spread around the globe. Cybercrime has come as a surprise that has become a strange phenomenon and this stamen proves that cybercrime is a global malady. These cybercrimes among others includes identity theft, cyber stalking, pornography, extortion, phony scams and internet frauds. In his part in naming cybercrime, Ribadu (2007) pointed out that majority of cybercrimes in developing countries of the world in general and specifically Nigeria include website cloning, false claims, internet purchases and other types of ecommerce 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 captured by Olugbodi (2010) as the activities associated with cybercrimes that are carried out by these fraudsters.

As reported by Sproat (2012), cyber criminals carry out their business activities in the areas where there is corruption and ineffective regulations. Many criminals launder their money in the banks of the countries where the government has lesser control on the bank secrecy. Through the dissection of their work, these criminals reduce their working risks and earn the benefits of globalization (Ahmed, 2016; Griffin, 2014). Losses from theft of intellectual property of individuals exceeds $160 billion each year. Studies show that most victims of cyber-hacking come from the world's most developed countries which include China, Germany, United States and Japan. Some major cyber-attacks are sponsored and the attacks can occur against a state, individuals and organization that are connected to the theft of information (Kitten, 2014).

Rapid globalization has also lowered the cost of accessing the internet that in turn, increased rates of cybercrime with its varied and diverse characteristic features. Some of the cybercrimes are in the form of Malware also known as malicious software or malicious code that creates a malicious task by cyber attackers on the targeted device to corrupt data and systems in order to gain unauthorized access to the system. As highlighted by Martens et al. (2019), malware is a major threat of cyber- dependent crimes that disrupts the proper functioning of the device.

Malware may be in the form of computer worms, viruses, ransom ware, bots, Key loggers, Trojan infections, spyware etc (Bossler & Holt 2009).

For instance, worms and viruses are malicious programs that self-replicate on computers without the consent of the user and cause adverse effects on the entire systems and networks. The only difference between viruses and worms is that worms can function independently of other files, whereas viruses rely on a host program to self-replicate. While, trojans are prevalently used by attackers in the financial sector to automate attack on computer systems. Similarly, key loggers or keystroke loggers being the oldest form of cybercrime are programs that record information typed in a website or application and in turn, share it with a third party without the approval of the user.

Globalization and how it contributes to cybercrimes can further be understood through the application of Key loggers attack PCs just like other malware but the only way to deal with Key loggers is to regularly scan for unforeseen anomalies via outbound or inbound traffic; the use of anti-virus and anti-spyware scanners and user awareness. Cybercriminals often use the normal mobile technology, which was primarily

created to assist people connect to spread terror. However, countries are formulating policies and laws that will discourage the rising trend of such crimes. Although, most of the countries are not fully equipped with the legal infrastructure to handle cybercrimes.

Despite the fact that the scope of cybercrime is such that geographical and political borders are meaningless, are not considered relevant, most cybercrimes studies focus on circumstances in the Western world, overlooking the fact that the nature of cybercrime is such that geographical and political boundaries are made irrelevant. Kumar (2003) argues that the participation, attempt and planning of a criminal act anywhere in the world can be carried out by a person who has access to computer and is connected to the internet. For Awe (2009), he confirms that irrespective of geographical location, criminals can generate cybercrimes from anywhere in the world and these crimes can be extended in other areas. With the use of the internet, these criminal acts are easier, more damaging and faster. The reoccurring menace inflicted on the countries of world as a result of cybercrimes have become a significant issue that need attention before it spin out of control and its effects become more disastrous.

Implications of Cybercrime for Nations

As discussed above cybercrime comprises any crime connected with the use of computer and network. It includes, but not limited to, hacking, cyber harassment, bank verification number scams, ATM spoofing, phishing, fraudulent emails, and spamming, social media hijacking and any other means of exploiting the vulnerabilities of both electronic devices and their users (Sabillon et al,2016). It is multifaceted and refers to as cyber terrorism and cyber warfare. Cybercrime is a globalized misconduct cutting at light speed across borders, and perpetrated by attackers who are often impossible to identify and difficult to locate even sometimes. Cybercrime destroys the reputation of a country, it makes the business environment difficult as it discourages potential foreign investors from doing business in a country with a bad reputation and hampers the growth of micro, small and medium-sized enterprises. Some foreign investors are scared of doing business in the country, considering it as a risky and unattractive business zone and financial instruments are accepted with great caution. From the evidence provided by some countries shows the effect on nation's security by implication their national interest because their cyber space has been compromised.

According to a research report by Cyber security Ventures, the global costs of cybercrime activity may increase by 15 percent annually over the next few years, reaching an estimated damage of $10.5 trillion annually by 2025. For comparison, the same number was $3 trillion in 2015. This massive transfer of economic wealth undermines innovation and investment, as it is larger than the cost inflicted by natural disasters. Moreover, it brings profits to the entities that engage in it higher than the profits achieved by trading all major illegal drugs combined. Stolen funds, loss of intellectual property and other valuable data, drop in productivity, identity theft, and reputational harm are some of the heaviest consequences of a severe hacking attack suffered by individual PC users and businesses.

All the risks associated with hacking attacks put digitized businesses under enormous pressure to find a way to secure their data, customers, networks, and Internet of Things (IoT) devices from cybercrime. Spending on cyber security products and services is supposed to reach a total of $1.75 trillion globally for the five years from 2021 to 2025, turning that market into one of the fastest-growing sectors of the IT economy. One particular high-damage sector is Ransomware, where the predicted costs may exceed $265 billion annually by 2031, which reflects a 57X increase to $20 billion for six years. Cyber security ventures have also estimated that Ransomware is the fastest-growing malware type that will hit a business every few seconds this year. That frequency is likely to increase to every two seconds by 2031. Considering the rapid growth of global data storage on public clouds operated by social media platforms, private vendors, and clouds owned by governments and institutions, the amount of data that will need to be protected may surpass 200 zettabytes by 2025.

Conclusion and Recommendations

This study shows how the emergence of globalization has come up with some challenges which has 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 adopt to. The argument 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. 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 what can be called a very high risk society for individuals, organizations and governments of different nations with serious consequences for technological and socio-economic prosperity.

Since the fight against cybercrimes requires a holistic approach not only just law enforcement, but also in terms of social-technical and socio-legal measures to strengthen its security capability. It is further recommended that awareness should be raised on different channels of cybercrimes for instance, child pornography. Similarly, the media can train citizens through programs on cybercrimes and how to protect them from these crimes. Countries should pass Films and Publications Act where filtering software is designed to reduce children's access to inappropriate material from the internet. Similarly, it is recommended that individuals should use phishing filtering to scan phishing websites to protect the end-user from being scammed. Every measure should protect institutions and organizations, real and legal persons against cyber-attacks.

References

Ahmed, N (2016). The Effect of Globalization: Terrorism and International Crime.Journal of Business and Management (IOSR-JBM). 18(11): 43-49.

Albrow. (1990). Globalization, Knowledge and Society: Readings from International Sociology. Sage Journals.

Huynen, M., Martens, P., & Hilderink, H.(2005). The health of globalization: A conceptual framework. Globalization and health, 1-12.

Aluko, S. (2001) "Background to Globalization and Africa"s Economic Development" Nigeria Economic Society, 2001

Awe, J. (2009). Fighting Cyber Crime in Nig. http://www.jidaw.com/itsolutions/security3.html.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.

Baylis J, &Smith S, (2001). The Globalization of World Politics: An Introduction to International Relation New York, Oxford University Press

Bosede, O. A., Olufunmilola, A. O., & Jane, M. (2021). "Globalization and Cyber Crimes: A Review of Forms and Effects of Cyber Crime in Nigeria", International Journal of Multidisciplinary Research and Modern Education, Volume 7, Issue 1, Page Number 18- 25, 2021.

Bossler, A., & Holt, T. (2009). Online activities, guardianship and malware infection: An examination of routine activities theory. International Journal of Cyber criminology, 3(1), 400-420.

Cerny, P. G. (1995). Globalization and the Changing Logic of Collective Action.International Organization, 49(4), 595-625.

Doyon-Martin, J. (2015). Cybercrime in West Africa as a result of Trans-boundary e-waste. Journal of Applied Security Res., 10(2), 207-220.

Folashade B.O & 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. Vol. 3 No. 9; September 2013

Griffin, J. (2014). Child sex tourism warning for fans attending World Cup in Brazil. The Guardian. Retrieved from http://www.theguardian.com/world/2014/feb/09/brazil-sex-tourism-world-cup.

Halder, D., & Jaishankar, K. (2011). Cybercrime and the Victimization of Women: Laws, Rights and Regulation. Hershey, PA, USA: IGI Global. ISBN 978-1- 60960830-9.

Hassan A.B, Lass F.D & Makinde, J. (2012): Cybercrime in Nigeria: Causes, Effects and the Way Out. ARPN Journal of Science and Technology. 2 (7) August "12.

Hebron, L., & Stack Jr, J. F. (2013). Globalization: Debunking the Myths. Dorling Kindersley India Pvt. Ltd.

Huynen, M., Martens, P., & Hilderink, H.(2005). The health of globalization: A conceptual framework. Globalization and health, 1-12.

Jones, R. B. (1995). Globalisation and Interdependence in the International Political Economy: Rhetoric and Reality. London: Pinter.

Kellner, D. (2002). Theorizing globalization. Sociological theory, 20(3).

Khor, M (2008) Globalization and the South: Some Critical Issues, Ibadan, Spectrum Books Ltd.

Kitten, T. (2014).Fighting the Globalization of Cybercrime Report: 'Cybercrime As a Service' on the Rise. https://www.bankinfosecurity.com/interviews/group-ibi-2480

Kowalski, M., Giumetti, W., Schroeder, N., & Lattanner, M. (2014). Bullying in the digital age: A critical review and meta-analysis of cyber bullying research among youth. Psychological Bulletin, 140(4), 1073-1137.

Kumar, K. (2003). Cyber Laws, International Property and E-commerce Security. Dominant Publishers and Distributors, New Delhi.

Lavorgna, A., & Sergi, A. (2014). Types of organized crime in Italy. The multifaceted spectrum of Italian criminal associations and their different attitudes in the financial crisis and in the use of Internet technologies. . International Journal of Law, Crime and Justice, 42(1), 16-32.

Martens, M., De Wolf, R., & De Marez, L. (2019). Investigating and comparing the predictors of the intention toward staking security measures against malware, scams and cybercrime in general. International Journal of Multidisciplinary Research and Modern Education (IJMRME) Impact Factor: 7.315, ISSN (Online): 2454-6119 (www.rdmodernresearch.org) Volume 7, Issue 1, 2021Computers in human behaviour, 92, 139-150.

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, 325-345.

Meke, E.S.N. (2012): An article "Urbanization and Cyber Crime in Nigeria: Causes and Consequences".

Okpeh, O., (2002). Globalisation and the African Question in the 21st Century, African Journal of Economy and Society. Vol. 2(2). pp. 43-50.

Okutan, A., & Cebi, Y. (2019). A framework for cybercrime investigation. Procedia Computer Science, 158, 287–294.

Olugbodi, K. (2010). Fighting Cyber Crime in Nigeria. http//www.guide2nigeria,com/news_articles_About_ Nigeria.

Ogoh, A. O and Orbunde E. (2012), Globalization and the Challenges for Poverty Eradication and Development in Africa: The Nigerian Experience. *IOSR Journal of Humanities and Social Science*. Volume: 5, Issue:2, Pp. 40 – 47. www.iosrjournals.org

Omodunbi, B. A., Odiase, P., Olaniyan, O., & Esan, A. (2016). Cybercrimes in Nigeria: analysis, detection and prevention. Journal of Engineering Technology, 1(1), 37-42.

Osei-Bryson, K.-M. & Donalds, C. (2019). Toward Cybercrime classification ontology: A knowledge-based approach. Computers in human behaviour, 92.

Oruc, E., & Tatar, C. (2017). An investigation of factors that affect internet banking usage based on structural equation modelling. Computational Human Behavior, 66, 232–235.

Pascoal, T., Fonseca, I., & Nigam, V. (2020). Slow denial of service attacks on software defined networks. Computer Networks, 1-12.

Phung, C. D., Silva, B. F., Nogueira, M., & Secci, S. (2019). MPTCP robustness against large scale man in the middle attacks. Computer Networks

Ribadu, E. (2007). Cyber Crime and Commercial Fraud; A Nigerian Perspective. A paper Presented at the Modern Law for Global Commerce, Vienna 9th – 12th July.

Sabillon, R., Cano, J., Cavaller Reyes, V., & Serra Ruiz, J. (2016). Cybercrime and cybercriminals: a comprehensive study. International Journal of Computer Networks and Communications Security, 2016, 4 (6).

Saulawa, M.A and Abubakar, M.K (2014): Cybercrime in Nigeria: An Overview of Cybercrime Act 2013. Journal of Law, Policy and Globalization, Vol.34.

Schell, B., Martin, M., Hung, P., & Rueda, L. (2007). Cyber child pornography: A review paper of the social and legal issues and remedies and a proposed technological solution. Aggression and violent behaviour, 12, 45-63.

Shehu A.Y (2014): Emerging Issues in Cyber-Crime: Causes, Implications and Effects for the Legal Profession. Online Journal of Social Sciences Research Volume 3, Issue 7, pp. 169-180. ISSN 2277-0844.

Sproat, P. (2012). A critique of the official discourse on drug and sex trafficking by organised crime using data on asset recovery. Journal of Financial Crime. 19(2): 149 –162

Ubi, E. N. (2000). Globalisation and the Eroson of the Sovereignty of States in the 21stCentury.Kafar Journal of International Relations. 2(1), 13-21.

Vadza, K. (2011). Cybercrimes and its categories. Indian Journal of Applied Research. Wada, F., & Odulaja, G. (2012). Assessing cybercrime and its impact on E-banking in Nigeria using social theories. African Journal of Computing ICTs, 4(2), 69-82.