International Journal of Multidisciplinary Research and Modern Education (IJMRME)
Impact Factor: 7.315, ISSN (Online): 2454 - 6119
(www.rdmodernresearch.org) Volume 7, Issue 1, 2021

GLOBALIZATION AND CYBER CRIMES: A REVIEW OF FORMS AND EFFECTS OF CYBER CRIME IN NIGERIA

Bosede Olanike Awoyemi*, Olufunmilola Adekiitan Omotayo & Jane John Mpapalika*****

* Department of Economics, Afe Babalola University Ado-Ekiti, Ekiti State, Nigeria
** Department of Philosophy, Ekiti State University, Ado-Ekiti, Nigeria
*** Macroeconomics and Governance Division, United Nations Economic Commission for Africa, Ethiopia

Cite This Article: Bosede Olanike Awoyemi, Olufunmilola Adekiitan Omotayo & Jane Mpapalika, "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.

Abstract:

Globalization involves interaction, collaboration and integration among individuals, organizations, societies, and governments of different nations. Globalization has enhanced progress in various parts of the world in different ways. Over the years, it has promoted access to education, transportation, communication, health facilities, importation and exportation, employment opportunities, revenue for the government and good standard of living for the people. Other aspects of the society that have been greatly influenced by globalization include trade and technology. Advancement in information technology presents new strategies for engaging in globalized economic activities as it facilitates easy transfer of properties, resources, money and collaboration with distant partners. A major negative impact on the society associated with the use of technology in the contemporary time however, is cybercrime. The paper investigates the various forms of cybercrimes, the effects and prevention of cybercrimes in Nigeria, and the connection between cybercrime and globalization from the reviews of literature. It was discovered that cybercrimes have deleterious effects on the lives, economies and international reputations of nations. Therefore, the battle against cybercrimes requires a holistic approach. Users of cyberspace are encouraged to be security conscious and engage antivirus computer programs to prevent cybercrime activities. At the same time, the government should enact comprehensive laws and regulations governing cyber security to punish offenders.

Key Words: Globalization; cybercrime; Nigeria, Cybercriminals, Victim and Technology

1. Introduction:

Globalization refers to the process of global transformation or internationalization interlinked with the socio-economic, technological, political and cultural aspects through different mediums of flows, including people, sharing of data and information, rural-urban migration, online trading of goods and services. It involves the integration of different societies, cultural practices, economies, technological innovations and institutional governance leading to the complex mutual interrelatedness. As theorized by Kellner (2002) and Adesina (2012), globalization is a complex and multi-dimensional concept that allows global economic interdependencies through cross-border trade, international capital inflows and outflows and the rapid diffusion of up-and-coming technologies such as Artificial Intelligence (AI), Internet of Things (IoT), Cloud Computing and Big Data analytics. The tech world has undergone an immense digital transformation to attain a digital economy in real-world applications such as smart learning, smart/precision farming, smart governance and smart cities (McAfee and Brynjolfsson 2012; Constantiou and Kallinikos 2015). Moreover, various data-intensive economic sectors, such as telecommunication and information technology, manufacturing, banking, investment, and health in advanced economies have managed to apply Big Data as a way of digitalizing their economies.

However, there is still no consensus on the definition and dimensions of globalization as well as indicators and its indices. Various indices have been developed such as the A.T. Kearney globalization index. According to Gygli et al. (2019), A.T. Kearney index acts as a basis for subsequent indices. A.T. Kearney assesses key components of trade openness and capital flows, migration, international phone call frequencies, global internet usage rates and public engagement in international organizations. Generally, the KOF[1] Globalization index is the most widely used globalization index that incorporates a large panel data set that covers the period 1970-2016 from 203 countries. Besides, another index developed by the Centre for the Study of Globalization and Regionalization (CSGR) over the period 1982–2004, CSGR Globalization Index measures the economic, social and political dimension of globalization using 16 variables (Lockwood and Redoano 2005). A unique feature of the CSGR Globalization index is that proxies for trade openness capture total exports and

[1]*KOF globalization index is a comprehensive measure that incorporates different aspects such as economic (trade regulations and policies); financial (FDIs, portfolio investment and reserves); social (phone subscriptions, tourism, International airports, migration); information (internet bandwidth usage, television access, international patents, internet access); Political (Embassies, global governance, UN peacekeeping missions, NGOs, CBOs and CSOs).*

imports of a country while the composite index captures the country's size and land lockedness as well as the population size. Some studies such as Raab et al. (2008), highlighted the cultural globalization index that considers variables related to traditional norms, customs and values. Other indices are the new Globalization Index (Vujakovic 2010); and the DHL Connectedness Index, that measures the correlation or connectedness between depth and breadth of various dimensions of globalization.

Cybercrimes refer to illegal, unethical and unauthorized behavior in a system that processes information or transfers data using computer and communication technologies (Okutan and 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 cybercriminals 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 and Sergi 2014, Oruç and Tatar 2017). Studies have shown that Nigeria is significantly affected by cybercrime followed by Russia, China and Brazil (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 and Odulaja 2012 and Omodunbi et al. 2016).

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. Organized crime caucus also have made it easy for cybercriminals to buy and sell information, such as stolen credit card data and other illicit goods, in underground forums, while it is proving challenging for law enforcement to shut these sites down, (Kitten, 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. 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. Centered on this background, the objectives of this paper are to investigate the various forms of cybercrimes, the effects and prevention of cybercrimes as well as the connection between cybercrime and globalization from the reviews of literature.

2. Conceptual and Literature Reviews:

The conceptual framework 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. Additionally, it has led to climate change, which threatens the extinction of some exotic species, eruption of lifestyle diseases due to unhealthy consumption of Genetically Modified Organisms (GMOs) e.g. Cancer, Non Communicable Diseases (NCDS) like hypertension, diabetes, etc., Emulation of Western cultures, norms and values, rural-urban migration (KNsamenang 2002). On a positive note, it has promoted trade and investment flows among countries, cultural diversity, technological advancement in the form of Artificial Intelligence (AI), Internet of Things (IoT) and the associated smart economies and societies in form of smart cities, precision farming, smart citizens and societies.

Several studies have shown mixed findings on the effects of globalization on culture. Global culture and western media have eroded the traditional cultures practiced by indigenous ethnic groups. For instance, in the South-East Asia and Africa, indigenous cultures are increasingly interlinked to the global culture and rates of premarital sex, abortion, monogamy, divorce, unwanted pregnancies, same-sex marriages are becoming the norm of the wider society (Roberts, 2019). Moreover, nowadays, international organizations and human rights

activists have been campaigning for gender equality and women empowerment in the male-dominated world that is contrary to the traditional culture advocating that men are more superior than women (Sundstrom et al. 2017). Thus, men are given priority in securing high-ranking positions relative to women. Such tendencies that favor men increase the gender gap where women have remarkably lower participation rates in the labor market, experience job discrimination and legal loopholes to protect women's rights (Al-Rifai et al. 2013). Meanwhile, there is a wide consensus that the global economy is slowing down due to the limited number of skilled labor in low-income countries. Most of the studies have shown that youth unemployment results from a relatively low demand for labor combined with a high supply of labor; high population growth rates; rural-urban migration; poor quality of the education system, industrial skills and training in the labor market; ineffective policies and poor institutions; Poor leadership and governance, (Salami 2013). Statistics show that the unemployment rate in the Southern Africa sub-region is more than 50 percent (Banerjee 2008). Globalization has certainly improved trade and business opportunities. However, the majority of these opportunities are limited to the people who already lead a respectable life. Educated and wealthy people from the urban areas have made most of opportunities to study, start businesses and get employment, which has further enhanced their standard of living. The majority of population in the rural areas is deprived of the basic social services. In fact, the people in the rural areas struggle for basic amenities like drinking water, hygienic food, medical facilities, electricity and roads.

Emerging technologies have their own adverse effects on both human beings and animals, especially the biotechnology in the form of GMOs that replaces organic foodstuffs has been a serious public health concern. 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 and 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. 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.

3. Methodology:

This section presents a methodology which includes a deductive approach to observe and explain the phenomenon of cybercrime and globalization in term of its effects, interrelationship and prevention from the existing literatures and available facts. This was done to draw conclusions and provide ways of addressing the problem of concern in the study. Although cybercrime is a global phenomenon, however, the scope of this study was narrowed down to Nigeria to review the different forms of cybercrime, their effects and possible ways of curbing the menace.

4. Discussion of Findings:

4.1 Types of Cybercrimes:

Cybercrimes may be carried out against individuals, property and government or organizations. Cybercrime against individuals includes cyber pornography, in particular, child-pornography, invasion of privacy, cyber bullying or harassment of individuals via e-mail spoofing, stalking, hacking, credit card frauds, password sniffing and defamation. Identity theft refers to the illegitimate use of one's account to retrieve crucial information relating to the account (Brody et al. 2007). For instance, in Nigeria, fraudsters retrieve valuable information from users' accounts through fake online banking web pages. In this scenario, identity theft may be minimized by installing antivirus software, shredding documents and routinely changing passwords. As suggested by Reyns and Henson (2016), protective measures such as the use of antivirus software lower identity theft victimization whereas other measures like modifying security settings and passwords encourage greater victimization. Burnes et al. (2020), affirms that as countries embark on stricter cyber security measures, cybercriminals respond with sophisticated techniques like hacking, malware and skimming to bypass security controls.

In another instance, cybercriminals collect information by phishing and spoofing where the imposter uses the victim's information without their consent. Phishing refers to the sending of unnecessary emails to corporate clients of different institutions by manipulating them to share their personal account information via fake websites (Hassan et al. 2012). One of the wireless LAN cybercrime is the evil twin attack that is similar to phishing scam. This type of cybercrime involves generating evil modems using wireless routers like WPA2 to bypass security protocols. Such attacks may be used to illegally access various passwords. In this scenario, as a precautionary measure for ordinary internet users, end-users can protect their accounts by frequently altering their privacy settings on networking sites consistent with cyber security measures (Timm and Perez 2010). Furthermore, ethical hacking may be used to detect the unwanted emails from spammers and loopholes in the network system. The suggested Multi-Split Spam Corpus Algorithm (MSSCA) detects the most frequent spam thread occurred in the email dataset (Murugavel and Santhi 2020). In another instance, Yar (2006) singled out the fraudulent use of bank credit cards is raising a concern in the banking system. In response, banks opted to install software's that ensure the client's information is not easily accessible. For instance, Bank Verification Number (BVN) fraud is one of the forms of cyber security threat that prompted commercial banks in Nigeria to install the biometric identification system across all states to tackle fraudulent crimes. Similarly, the UK experienced cyber frauds amounting to yearly losses of more than £100 million (Vadza 2011).

On the other hand, cyber defamation or cyber stalking is the deliberate infringement of an individual's right to tarnish other people's reputation online. According to Veerasamy (2019), the perpetrators of cyber stalking may hack their victims' accounts and harass or bully them resulting to emotional abuse, substance abuse and trauma. In the worst-case scenario, it may lead to suicidal attempts. On the same note, cyber-harassment or bullying include traits such as unfounded allegations, data theft, identity theft, child pornography, etc. In the case of pedophiles and stalkers, they falsify their identities to lure vulnerable toddlers and youngsters via social media platforms such as Facebook. For instance, cyber pornography entices sexual acts via online platforms, involving persons under the age of 18 commonly referred to as child pornography. In essence, culprits of cyber pornography, pedophiles, attract youngsters by posing with fake identities to arouse sexual acts on their victims. Schell et al. (2007), suggested that tackling child pornography requires a multidimensional approach that will raise awareness on sexual misconducts carried out on minors, educating victims about minimizing the use of social media for their own safety while interacting online and improving digitally-enabled approaches to track down the would be and existing online child pornographers. However, several studies have shown that victims of cyber bullying or harassment are exposed to low self-esteem, panic attacks, fear, depression, sleep deprivation and anti-social behavior (Kowalski et al. 2014).

Cybercrime against property involves theft of intellectual property, malware that interferes with the proper functioning of the system, cyber trespassing, software piracy and theft of marketing information among others. Other malware attacks, according to Pascoal et al. (2020) include denial-of-service (DoS) attacks where attackers deny service of a web-server (VoIP server) by sending low request rates to the targeted server. Other malware attacks include Man in the Middle (MitM) attack where an attacker establishes a position between the sender and receiver of e-messages and intercepts them. This type of cyber attack is commonly favored in the military to confuse foes. In practice, MITM attacks may be carried out by an optical layer or BGP route hijacking (Phung et al. 2019). They found that Western Europe outperforms others in terms of MITM robustness while Central Asia, Caribbean and Northern Africa, have zero robustness.

Cybercrime against government or organizations referred to as cyber terrorism involves the illegal use of cyberspace by hackers to infringe on the privacy of government or organizations/institutions. This particular cybercrime is regarded as terrorism or treason when classified information is tampered with on a country's military or government's websites. Cybercrime against organizations entails denial of service attacks (DoS), password sniffing, malware attacks, spy/espionage crimes and network intrusions. Cyber terrorism is another type of cybercrime carried out against the state encompassing a range of activities that violates a country's cyber security. It includes espionage and disclosure of classified information to rivals, resulting in a potential increase of external threats. Since September 2011, various institutions worldwide such as financial institutions, military, telecoms, nuclear and chemical facilities, have been more vigilant to protect their systems from cyber attacks. In response, countries have attempted to create an enabling environment for cyber security measures in terms of legal, institutional, policy and regulatory frameworks. Furthermore, some countries have established cyber security units under the Ministry of Information and Communication Technology. For instance, Computer Security Rapid-Response Teams were established to act and prosecute cybercrimes in misusing information and communication technologies (Donalds and Osei-Bryson (2019).

4.2 Globalization and Cyber Crime:

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. Organized crime caucus also have made it easy for cybercriminals to buy and sell information, such as stolen credit card data and other illicit goods, in underground forums, while it is proving challenging for law

enforcement to shut these sites down, (Kitten, 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. 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.

Furthermore, globalization creates many national security interests well outside a country's border through the link between countries and economies. The impact of Cybercrime can hit a nation's security as well as other interests of a nation from places where the nation has little or no control over or has no sufficient ability to defend or protect itself without international cooperation. The crimes with a transnational body, have gone beyond the state and regional levels and shade threat and its damaging effects on cross-border and global levels. As reported by Ghaderi, (2016), an attack on the military operations of a NATO state in a way that falls under NATO Article 5 is one example. Also, a major attack on offshore branches of US corporations in a way that will unfavorably affect the US economy or an electronic takeover of air command of airports in different areas of the world are others. Some modern information and communication technologies with networks have resulted to the spread of cyberspace and globalization of cybercrime now plays a strong role in posing a threat and great risk to countries.

The principles of globalization of free trades and markets have weakened the national interventions. Globalization has increased countries' interactions and reduced trade regulations, which has increased the external trade and investments by countries around the world. This situation in some way has promoted cross-border crimes (Corraya, 2015). The cybercriminals often exploit the limited border controls, poor law enforcements for an expansion of their activities across the globe. As reported by Sproat (2012), cybercriminals 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).

4.3Effects of Cybercrime in Nigeria:

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. In Nigeria, high rate of unemployment, the quest for wealth among youths, incompetent security of personal devices and lack of effective cybercrime laws, unskilled have largely contributed to the rise in the level of cybercrime and make it a serious problem for the country. Olugbodi (2010), identified cyber harassment, credit card theft, website cloning, cyber theft, financial fraud well-known as Yahoo-Yahoo, fraudulent electronic mails, cyber laundering among others as the commonly perpetrated cybercrimes in Nigeria. These criminal acts are perpetrated by youths, especially university undergraduates and graduates. From the evidence provided by (Folashade and Abimbola, 2013), the cybercriminals used tools such as key loggers, port scanners, password cracker, network sniffers, vulnerability scanners etc. and they involved defrauding unsuspecting victims, hacking and cloning.

The Canadian Anti-Fraud institute reported 59,009 fraud cases from individuals and firms, with losses totaling $97,654,160.35 (MacEachern, 2019). However, the center estimates that less than 5 per cent of the victim's report fraud cases and this situation reduces the possibility of obtaining current information on means to avert similar attacks. Similarly, in the United State, roughly 62,000 people aged 60 or older reported losses totaling over $649 million. As reported by (Obinna, 2020), the estimated annual financial loss in Nigeria due to cybercrime was N250 billion ($649 million) in 2017 and N288 billion ($800 million) in 2018, these estimates are based on the reported cases, in the face of many unreported cases. McAfee (2018) reveals that 95 per cent of cyber crime is unreported. This analysis shows huge resources that would have been directed toward addressing the issue of underdevelopment in Nigeria are lost to cybercrime annually and inadequate reporting of these crimes also prevent appropriate measures to be taken against cybercrime. According to Jack and Ene, (2016) cybercrime results in the loss of intellectual property or personal confidential information, financial resources and the damages can be extreme for individuals who are vulnerable.

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. The incidence of cybercrime has given Nigeria a bad image amongst the group of nations as one of the most corrupt nations in the world. This tainted national image impact on the way Nigerians are being treated overseas with distrust and extreme caution as Nigerians are stereotyped to be 419ers (conmen) and hence to be suspicious of (Jack and Ene, 2016). 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.

4.4 The prevention of Cybercrime in Nigeria:

The incidence of cybercrimes has been increasing over the years, thus, there is a need for an increasing focus on individuals, corporations and states on building tools to improve the capabilities to fight cybercrime, cyber terrorism, cyber espionage, and cyber warfare. Many countries are creating cyber defense bodies within their national security establishments and increasing their cyber competencies, including through the establishment of dedicated cyber warfare divisions within their security forces. The cyber arena is multidimensional and persistently evolving. Recognizing the critical interlink between the different actors and the need for collaboration and innovation, nations are increasingly trying to build mutual aid between domestic cyber institutions and academia, and develop devices for internal and external cooperation between different national units and agencies.

The United States Cyber Command has already proclaimed that over the next few years it intends to recruit about 6,000 cyber specialists and build teams of cyber-soldiers and civilians to assist in defending US national infrastructure and for both invasive and defensive purposes. In the UK, the Ministry of Defense sets up a Joint Cyber Reserve, this is a new cyber unit charge with the responsibility to defend the UK critical computer networks from attack. Lewis and Timlin (2011), conducted a study on cyber security and cyber warfare and identified 33 states that introduced cyber warfare in their military arrangement and organization. The Nigerian government also needs to be proactive in taking steps to curb the cybercrime menace in the country, training and recruiting special cyber security experts and make the existing law enforcement and intelligence agencies as well as the security agencies to understand both the nature of machinery and strategies involved in cybercrime.

Moreover, creating serious awareness about the techniques and strategies that cybercriminals are using is a means of self-protection and self-policing. The users of cyberspace should be encouraged to become security conscious and apply antivirus programs and firewalls that can prevent cybercrime activities. Also, companies and organizations should invest in major training programs for their employees on cybercrime detection and reporting. Combating transnational cybercrime should become one of the major public education issues and security measures that will protect online users from every form of cybercrime should be put in place. Fighting the cybercriminals and terrorists, as well as cybercrime organizations, will require not only strong domestic infrastructure and capabilities, but also strong collaborations among countries and their various security institutions, intelligence agencies, and militaries. The establishment of a global action premeditated plan in this regard must be put forward. International standards and methods, including enforcement mechanisms should be applied by countries, and tools for sharing information and collaboration of effort, should be a priority.

Also, improving personal security, establishment of anti-cybercrime agencies are equally crucial in curtailing cybercrimes. The government should enact comprehensive laws and regulations to punish offenders. Recently, the Central Bank of Nigeria (CBN) established a risk-based cyber security structure and guidelines for deposit money banks and other payment service providers in order to effectively curb the rate of cybercrime. This structure lays out practical ways to secure some information about the customers that is accessible via the internet. Other government institutions should introduce the same measures to protect their customers and the public at large. It is also important that individuals avoid faked software, never to share their Bank Verification Number (BVN), bank account details, email access code to anonymous persons, or divulge any classified information to anybody as none of these networks were designed to be ultimately secure.

5. Conclusions and Recommendations:

Over the years, African countries have experienced cyber-related threats such as financial frauds or money laundering, cyber terrorism and cyber harassment among others due to weak network and information system security. According to Hassan et al. (2012), cybercriminals are regularly exploiting the existing legal gaps to bypass cyber security. In support of this, Dada et al. (2013) argued that African countries have been unable to effectively deal with cybercrimes because their law enforcers in regards to intelligence, infrastructure and personnel are insufficiently equipped. Countries lack some of the sophisticated state-of-the-art technical equipment required to trace cybercriminals and subject them to face justice. In general, the fight against cybercrime requires coordinated multi-stakeholder's efforts to raise awareness on curbing cybercrimes. The government should set up procedures to report fraudulent activity.

From the cyber security perspective, 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. Under the ministry of Communication and Technology, cybercrime unit should be established to create an enabling environment in terms of policy, legal, institutional and regulatory frameworks governing cyber security. 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.

6. Acknowledgements:

The authors acknowledge the support of Afe Babalola University Ado-Ekiti (ABUAD) in providing facilities during the writing of this paper. The views expressed in this paper are that of the authors and do not represent that of the institution. The authors also acknowledge the support of John Awoyemi for proofreading this work.

7. References:

1. Ahmed, N (2016). The Effect of Globalization: Terrorism and International Crime. Journal of Business and Management (IOSR-JBM). 18(11): 43-49.
2. Al-Rifai, A., Lallement, D., Said, N., & Wihaidi, R. (2013). USAID/West Bank and Gaza Gender analysis. Washington, DC: United States Agency for International Development.
3. 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.
4. Burnes, D., DeLiema, M., & Langton, L. (2020). Risk and protective factors of identity theft victimization in the United States. Preventive Medicine reports, 17.
5. Constantiou, I., & Kallinikos, J. (2015). New games, new rules: Big data and the changing context of strategy. Journal of Information Technology.
6. Corraya, S. (2015). Prostitution and forced labour: trafficking in human beings in Bangladesh.
7. Retrieved from http://www.asianews.it/news-en/Prostitution-and-forced-labour:-trafficking-in-human-beings-in-Bangladesh-33572.html
8. Dada, S., Owolabi, S., &Okwu, A. (2013). Forensic accounting a panacea to alleviation of fraudulent practices in Nigeria. International Journal of Business Management Economic Res, 4(5), 787-792.
9. Donalds, C., & Osei-Bryson, K.-M. (2019). toward cyber crime classification ontology: A knowledge-based approach. Computers in human behaviour, 92.
10. 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.
11. Folashade B.O and 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
12. Ghaderi, M. (2016). Cyberspace and globalization of crime and punishment. International Journal of Humanities and Cultural Studies (IJHCS) ISSN 2356-5926, 3(2), 600-609.
13. Gygli, S., Haelg, F., Potrafke, N., & Sturm, J.-E. (2019). The KOF Globalization index- revisited. The Review of International Organizations, 14, 543--574.
14. Griffin, J. (2014). Child sex tourism warning for fans attending World Cup in Brazil. The
15. Guardian. Retrieved from http://www.theguardian.com/world/2014/feb/09/brazil-sex -tourism-world-cup.
16. Hassan, A., Lass, F., & Makinde, J. (2012). Cybercrime in Nigeria: causes, effects and the way out. ARPNJ Science and Technology, 2(7), 626-631.
17. Huynen, M., Martens, P., & Hilderink, H. (2005). The health impacts of globalization: A conceptual framework. Globalization and health, 1-12.
18. Jack, J. T., &Ene, R. W. (2016). Cybercrime and the challenges of socio-economic development in Nigeria. JORIND, 14(2), 42-49.
19. Kellner, D. (2002). Theorizing globalization. Sociological theory, 20(3).
20. Kitten, T. (2014).Fighting the Globalization of Cybercrime Report: 'Cybercrime As a Service' on the Rise. https://www.bankinfosecurity.com/interviews/group-ib-i-2480
21. 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.
22. 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.
23. Lewis, J. A., &Timlin, K. (2011). Cyber security and cyber warfare: Preliminary assessment of national doctrine and organization. UNIDIR.
24. Lockwood, B., & Redoano, M. (2005). The CSGR globalisation index: An introductory guide. Technical report. 155 (04), CSGR working paper.
25. McAfee (2018). The Economic Impact of Cybercrime-No Slowing Down.
26. https://www.mcafee.com/enterprise/en-us/solutions/lp/economics-cybercrime.html
27. 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.

Computers in human behaviour, 92, 139-150.
28. McAfee, A., & Brynjolfsson, E. (2012). Big Data: The Management Revolution. Harvard Business Review, 1-9.
29. Murugavel, U., &Santhi, R. (2020). Detection of spam and threads identification in Email spam corpus using content based text analytics method. Materials Today: Proceedings.
30. Obinna. C, (2020).Nigeria: IFC Seeks 'Ambitious' Reforms for Inclusive Growth in Nigeria.
31. https://allafrica.com/stories/202002030123.html
32. Okutan, A., &Cebi, Y. (2019). A framework for cyber crime investigation. Procedia Computer Science, 158, 287–294.
33. Olugbodi, K. (2010): Fighting Cyber Crime in Nigeria. Retrieved September, 2016 from http//www.guide2nigeria,com/news_articles_About_ Nigeria
34. 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.
35. 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.
36. Pascoal, T., Fonseca, I., & Nigam, V. (2020). Slow denial-of-service attacks on software defined networks. Computer Networks, 1-12.
37. Phung, C.-D., Silva, B. F., Nogueira, M., &Secci, S. (2019). MPTCP robustness against large-scale man-in-the-middle attacks. Computer Networks.
38. Raab, M., Ruland, M., Schonberger, B., Blossfeld, P., Hofacker, D., Buchholz, S., &Schmelzer, P. (2008). Global Index: A sociological approach to globalization measurement. International Sociology, 23, 596-631.
39. Reyns, B., & Henson, B. (2016). The thief with a thousand faces and the victim with none: identifying determinants for online identity theft victimization with routine activity theory. International Journal of Offender Th., 6(10), 1119–1139.
40. Roberts, L. (2019). Changing worldwide attitudes toward homosexuality: The influence of global and region-specific cultures, 1981–2012. Social Science Research, 80, 114-131.
41. Sabillon, R., Cano, J., Cavaller Reyes, V., & Serra Ruiz, J. (2016). Cybercrime and cybercriminals:
42. a comprehensive study. International Journal of Computer Networks and Communications Security, 2016, 4 (6).
43. 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.
44. 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
45. Sundstrom, A., Paxton, P., Wang, Y.-T., & Lindberg, S. (2017). Women's political empowerment: A global index 1900-2012. World Development, 14, 321-335.
46. Timm, C., & Perez, R. (2010). Chapter 4: Evil twin attacks. In Seven deadliest social network attacks (pp. 63-82).
47. Vadza, K. (2011). Cyber crimes and its categories. Indian Journal of Applied Research.
48. Veerasamy, N. (2019). Cyberstalking and bullying. In The dark side of social media (pp. 43-58).
49. Vujakovic, P. (2010). How to measure globalisation? A new globalisation index (NGI). Atlantic Economic Journal, 38(2), 237–237.
50. 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.
51. Yar, M. (2006). Cybercrime and Society. London: Sage Publication Ltd.