CORONAVIRUS PANDEMIC, INTERVENTION FUNDS AND CYBERCRIME

Olayinka AKANLE
Department of Sociology, University of Ibadan, Nigeria
& Research Associate, Department of Sociology,
Faculty of Humanities,
University of Johannesburg, South Africa
*yakanle@yahoo.com, **o.akanle@ui.edu.ng***

David. O. NKPE
Department of Sociology, University of Ibadan, Nigeria/
Economic and Financial Crimes Commission (EFCC), Nigeria

Olusegun Israel OLANIYAN
Department of Sociology,
University of Ibadan, Nigeria

ABSTRACT
The Coronavirus pandemic is a remarkable event that has affected, reconfigured and altered ways of life of many individuals and groups globally resulting in what is now known as the "new normal" in human relationships. Part of the measures put in place to mitigate associated deaths and contagion of the disease were massive lockdowns of businesses, confinement of people and travel restrictions. In the process, people and organizations were forced to think of new alternatives of sustaining their social and economic activities without deviating from the COVID-19 precautions. One of these mitigation methods and coping mechanisms is teleworking. While teleworking and virtual relationships have been in existence prior to COVID-19, evidence abounds that the pandemic generated a unique vulnerability and crime; cybercrime. Cybercrime has affected lots of businesses, societies and the mode through which teleworking is carried out. The increased anxiety of most people to have proper knowledge of and cope with this pandemic often make them fall victim of cybercrime. A very good case is cybercrime and attack on coronavirus palliative funds. This paper examines cybercrime and diversion of Covid-19 funds through global perspectives particularly different cyber-attacks during COVID-19.

Keywords: *Coronavirus Pandemic, Cybercrime, Coronavirus Palliative Funds*

INTRODUCTION

The Coronavirus pandemic which emerged like a dinky event in Wuhan, Hubei China in year 2019, has become a global crisis resulting in massive death and quarantine of many people across the world. Human histories have evolved different forms of pandemic such as Antonine Plague (165AD), Cyprian Plague (250AD), Justinian Plague (541AD), The Black Death (1350AD), First Cholera Pandemic (1817), Fiji Measles Pandemic (1875), The Great Plague of London (1665AD), Spanish Flu (1918), Asian Flu (1957), HIV/AIDS (1981), SARS Pandemic (2003), Ebola (2014) and many more (Kumaran and Lugani, 2020). Evidence from available scientific research revealed that aside Spanish Flu of 1918, there has not been any pandemic worse than Coronavirus throughout human history (Kumaran and Lugani, 2020). According to World Health Organization (WHO) (2020), over 42 million cases of infection and 1.1 million Coronavirus associated deaths have been reported globally. As at 28th of October 2020, statistically the COVID-19 disease has spread to about 216 countries and territories. With absence of approved drugs and vaccine to stop the rising contagions and associated deaths from Coronavirus, many COVID-19 protocols have been put in place to mitigate rising cases and deaths. According to the Boris Johnson (UK Prime Minister), UK, for instance, has introduced tougher coronavirus restrictions across England as current approach had failed to stem an alarming second wave of the pandemic (Financial Times, 2020).

This is also the case in Canada, The United States, Australia and many European Union (EU) countries (Whitehouse, 2020, BBC News, 2020; Worldometer, 2020, Amzat et. al. 2020, NCDC, 2020, Ahmad and Ahmad, 2020, Du Toit, 2020, Moore, Gelfield, Okunogbe, 2017, Zhou, Yang and Wang et al. 2020, Foster and Renfrew et al. 2020, Gilbert et al. 2020, WHO, 2019, Shabir and Aijaz, 2020, Mo Ibrahim Foundation, 2020, Shabir and Aijaz, 2020, International Monetary Fund, 2020, CDC, 2020, Ihekweazu, 2020). Hence a major measure put in place to ameliorate the effects of Coronavirus Pandemic and associated socioeconomic meltdowns globally is strategic collaboration among nations, international donors and non-governmental organizations to drive massive provision of funds and other economic incentives. According to WHO (2020), the world is facing unprecedented challenges of COVID-19, the need to combat it through linking governments and organizations across the world to respond to this global challenge becomes imperative. The strategic response revolves, largely, around funding and this is not much less than US$675 million for critical response in countries most severely affected by the disease (WHO, 2020).

The newness of Covid-19 and emergency global movement of funds in unguarded and unprecedented manners has however opened another frontier of crime in the cyber space. The pandemic has led to surge in rate and ingenuity of cybercrime. Following the rapid growth of 21st century Information and Communication Technology (ICT) and the desire of various countries to catch up with growing effect of this technology, the novel Coronavirus has not only led to significant threat in technology-driven society but also created path through which people fall victim of cyber-attacks (Harjinder et. al. 2020). In response to this, on April 06, 2020, the Central Bank of Nigeria (CBN) Director of Corporate Communication, for instance, issued a press release on how cybercriminals are exploiting current pandemic (CBN, 2020). This advisory discussed issue such as phishing, diversion of relief packages, impersonation and how the general public can protect themselves against cyber offenders. Buttressing the above view, there has been increasing cases of scams, impersonation of public figures, and siphoning of funds from banks and organizations (Krebsonsecurity 2020; The Guardian Newspaper 2020 and Europol 2020). Stressing further, information from American Delta Association (2020) opined that cybercriminal are opportunistic in nature as they tend to take advantage of the pandemic to perpetuate crime through sending of malicious mails to individuals in order to cajole and elicit sensitive information.

Since working from home has become the new normal towards ensuring adequate safety, criminals are using this opportunity to widespread anxiety and panic of the virus to send coronavirus phishing mail with the aim of hooking and hacking vulnerable individuals and disruption of organization security system (Ahmad, 2020). Cybercrime is thus a major problem associated with the Coronavirus Pandemic and researches are very scarce in this area. Thus, this article examines the problematic of cybercrime and Coronavirus through the remit of funds. This article interrogates diversion of coronavirus palliative funds within global perspective to contribute to knowledge in this very area.

METHODOLOGY

This article adopted unobtrusive method of research to elicit relevant information from relevant sources. Unobtrusive is a method of research through which concrete and relevant information is collected without interfering or alerting the subject under study. This is to eliminate biases and promote conceptual and contextual analysis of data (Huysamen, 1994). As a result of the pandemic, ensuring safety of both researcher and the respondents is the core ethical value of a good research. In order to avert contagions and other risks of the virus both on the part of the researcher and the respondents, all COVID-19 protocols were observed. Therefore, this research article utilized primary insights and secondary data from journals, documents, books, reliable internet sources and information from reliable organizations to provide holistic view of the phenomenon of study. The unobtrusive method of research gave the research team opportunity

to cover large span of events and settings with limited cost and also provide relevant information about human events which the team may not have direct access and approach to because of social and physical distance, political events and ethical reasons (Huysamen, 1994). In light of this ongoing pandemic, the unobtrusive method of data collection was adopted as best practice and method.

Theoretical Framework

Routine Activity Theory (RAT) is used as theoretical scaffolding of this article. RAT was propounded by Felson and Cohen (1969). The theory started with the explanation for predatory crime. That is for crime to take place, there must be three forces; likely offender, suitable target and absence of capable guardians. The theory takes a look at how people fall victim of crime in their everyday activities. According to Felson and Cohen (1969), the likely offender is someone whose aim is to commit a crime. The target can be person or object whose position is prone to more risk of criminal attacks. Absence of capable guardian does not necessarily mean a police officer or security guards but rather someone/something whose presence or proximity would prevent a crime from happening. In the RAT, it is believed that targets most times are often absent from the crime scene. To influence a target's risk to criminal attacks, it must be based on four principles which are; value, inertia, visibility and access.

Value often refers to what the offenders desired and his zeal to pursue that criminal desires. Inertia simply means the weight of the items stolen whether light or heavy. Visibility refers to the exposure of theft target to offenders and access refers to the patterns of the individual life that propel offender to criminal acts. While Routine Activity Theory (RAT) has proven effective in the terrestrial world, it is important to note that it can also be applied to the virtual world. The likely offender as highlighted in the theory is the cybercriminal whose aim is to perpetuate cyber fraud on individuals, groups or organisations. The suitable target (akin to value) often comes from what attract the individual to perpetuate the cybercrime. Some of these values may cut across the desire to hack data of organizations and businesses, illegal transfer of fund for personal aggrandizement, cyber stalking and many more particularly during the pandemic when the cyberspace did not anticipate the outbreak and associated financial flow. During the Coronavirus Pandemic, visible guardians are generally either lacking and/or unprepared for the attendant cybercrimes. The absence of capable guardians revolves around the security measured adopted by different organizations, individuals and nations prior to COVID-19 and even much later. If such security is not fully maximized or there is absence or breach of this security to protect people who are relating and working virtually (as it has become the new normal), it can increase individuals, nations and organizations exposure to cybercrime and victimization.

What this implies is that the presence of adequate security is similar to the theoretical element of 'presence of capable guardians' to prevent cybercrime from happening. Importantly, when there is absence of security system in form of capable guardians, target (Coronavirus financial flows) are subject to risk of cybercriminal attack. While the above element plays greater role in crime victimization, it is important to note that cybercriminal will only have interest in something whose value is light in nature. And in this case cybercrime and proceeds are virtual and more than light. Funds, data, and many more are what will interest cybercriminals than heavy goods like television, vehicles and so on. Exposing details (personal identification number, bank verification number, other bank details, password, email addresses, social security number) of individuals, organizations and even nations and regular visit to malicious websites can lure cybercriminals to crime, cyberbullying, stealing and cyber victimization which are rampant during Coronavirus pandemic.

History of Pandemics

Infectious diseases have wreaked serious havocs on humans since ancient times. As humans continue to spread across the world, so also are harmful infectious diseases spreading. Particularly with globalization, outbreaks of pandemic have become common and more disastrous (Weforum, 2020). Patrick and Krewski (2016) opine that the rise of globalization has fostered social and economic changes that have enhanced the threat of disease occurrences and promoted the spread of novel viruses across countries. On the other hand, globalization has also fostered international cooperation and advancement in scientific research by altering the way infectious diseases originate, are understood and controlled as against the traditional belief of attributing themto divine ordinance (Patrick and Krewski, 2016).

Historical antecedent of pandemic dated back to the common BCE era when Plague of Athens (430 BCE) led to the fall of Golden Age of Greece. This form of pandemic has been attributed to epidemic caused by typhoid fever or epidemic typhus (Rubin, 2011). Following the fall of Greece during the Peloponnesian war, the Antonine Plague (often called Plague of Galen 165-180CE) coupled with Bubonic Plague (started around 540CE) emerged as one of the famous pandemic that shook the Roman Empire. These two pandemics were caused by bacterium *Yersinia pestis and* spread in cycles until the 18th century (Rubin, 2011). There is a general agreement among historians that an outbreak of pandemic called “Influenza” also occurred during the 412BC (Patrick and Krewski, 2016). However, lack of substantial data and the fact that the virus was not isolated, became a hurdle for medical historian to document the sign and symptoms of this influenza (Kuszewski, 2000; Potter, 1998; Potter, 2001 cited in Patrick and Krewski, 2016). The first reference to “influenza” pandemic in scientific literature was reported in the year 1650 (Potter, 1998). Since then, the history of pandemics has been well documented in scientific literature.

The first 18th century pandemic began in the early Russia spring of 1729, spreading across Europe within six months and around the world after three years of occurrence (Pyle, 1986; Hirsh, 1883; Patterson, 1987 and Finkler, 1899). With regards to more recent pandemic, the outbreak produced a multiple dimension characterized by higher morbidity and mortality rate. The second wave of the century pandemic appears to have begun in China during the autumn period of 1781 and spread through Russia and Europe for a period of eight months, with a particular susceptible attack among young adults (Pyle, 1986; Finkler, 1899; and Plye, 1984). The 19th century pandemic was recorded to have begun in the year 1830 of China winter and spread across Southeast Asia, Russia, Europe and later into North America in the year 1831. Though evidence from available literatures revealed that despite high rate of illness from this pandemic, mortality rate was low (Pyle, 1986; and Patterson, 1987).

A more deadly pandemic reoccurred in Russia and later spread to Europe and North America through rail and sea routes. Historical record revealed that this pandemic spread at a faster rate with an estimated fatality of 0.1%-0.28% and overall global death of one million people (Valeron et al. 2010). Several patterns have emerged in documenting the historical analysis of pandemic from time immemorial, what is important to note is that lack of effective data makes it difficult to trace the timeline. It is therefore worth nothing that out of the pandemics where fact is available, either China, Russia, or Asia have been identified as major point of origin. Transpandemic (From Ancient Time to Present) is also a major issue in historicizing pandemics. Transpandemic relates to spread of diseases through transportation enabled migration systems. It is contended that infections that became pandemics during the 18th century and up till present were facilitated mostly by movement and migration of people from one place to another.

The emergence of Industrial Revolution not only promoted efficiency of work by expanding the road network and introduction of machine but it also became the primary vector through which diseases spread across the world (Patrick and Krewski, 2016). For instance, the spread of Spanish Flu of 1918 has been attributed to movement of 100,000 Chinese Labour Group (CLC) to Europe to support the allied war effort (Palmer, 2014). The contact of the Chinese labour with

other countries like Singapore, Europe, Durban, Cape Town and North Africa and subsequent transfer of these labours to Vancouver to be brought by train sent to Halifax across the Atlantic paved way for the transfer of the plague (Humphries, 2013).

Waring (1971) observed that the Spanish Flu was among the worst and greatest threat throughout human history. Stressing further, Patrick and Krewski (2016) corroborated the above view that the Spanish Flu brought illness, deaths with an approximately ten million deaths across the globe. In February 1957, a new pandemic called “Asian Flu” was discovered in Yunnan China (Pyle, 1986). The pandemic was reported to originate from land routes from Russia to Scandinavian and Eastern Europe in an international conference held in Iowa (Langmuir, 1961 and Payne, 1958). A study conducted by Viboud et al. (2016) titled “Global Impact of the 1957-1959 Influenza Pandemic” revealed that historical mortality rate in 39 countries that suffered from the Asian flu pandemic was 598 deaths per 10,000 people. Ten years after the emergence of Asian flu, the pandemic went into strain and reconfigured itself into another H3N2 known as Hong Kong flu (Patrick and Krewski, 2016). Despites being highly transmissible, evidence abound that the mortality rate of Hong Kong Flu was milder than the Asian flu (Morens, Taubenberger and Fauci, 2009). While mortality rate of Asian flu was 40.6%, evidence from Morens, Taubenberger and Fauci (2009) revealed that Hong Kong flu mortality was 16.9%.

The pH1N1/09 virus also known as swine flu was another pandemic with impacts across the world. Evidence revealed that the extent of global trade and movement of people paved way for swine flu to spread widely within six weeks as against other pandemic that took six months to spread (Smith et. al. 2009). On 11th June 2009, the World Health Organization declared the virus as a pandemic having spread to about 122 countries. A month after the declaration, report shows that 134,000 cases and 800 deaths have already been recorded (WHO, 2009). However, it is important to note that efforts geared toward mitigating this pandemic was also similar to the method being adopted for the COVID-19 pandemic. Some of the efforts adopted are quarantine, closure of schools, banning of public gatherings and infection prevention protocols like cough, sneezing regulation and wearing of facemask (Markel et. al. 2006). It is therefore important to note that the advancement in human societies which was ushered in by Industrial Revolution does not only promote positive social change but also paved way for invention in vaccine production and pandemic prevention. The current historiography demonstrates pandemics are not to humans and consistent approaches and protocols have always been instituted. Of interest is that Covid-19 pandemic shares some semblance with documented histories of global pandemic. What has not been sufficiently documented is the role of technology moderated crimes in affecting effective financial flows in managing pandemics. This is the focus of this article through the case of Coronavirus Pandemic.

Pandemics and Funding Experiences

Despite the ravaging pandemics that has bewailed human societies for decades, popular opinion among scientists is how to provide viable solutions to recent and upcoming pandemics. As a result of this, it created the need for several governments and international organizations to provide funds in order to support scientific inventions and innovations. In 1918, owing to lack of effective vaccines and antibiotics to combat the Spanish flu and shortage of medical personnel to support challenges, people who fell ill had to resort to ineffective drugstore and home remedies such as topical creams, or mixture of water, salt and coal oil together to cure themselves of the virus (USDHHS, 2016). Hence, lack of technical knowhow of doctors to fully comprehend the etiology of the virus made them to prescribed alcohol consumption as a means of infection control; thus producing more than a little hike in consumption of alcohol among growing population (USDHHS, 2016). The discovery of penicillin in 1929 provided impetus through which primary death of influenza was cured (Chiou, 2006). In addition to this, the discovery of positive pressure

ventilators in 1940s for use in intensive care units helped improve health system in complicated cases (Kacmarek, 2011).

In year 2000, the ravaging effect of HIV/AIDS, tuberculosis and malaria appeared unstoppable most especially in developing countries. Effort geared towards preventing the transmission of the infection made international donors like The Global Fund to design innovative solutions to global health challenges. Since its creation in 2002, Global Fund has disbursed US$45.4 billion in response to fight against HIV, tuberculosis and malaria (The Global Fund, 2020). With partnerships and supports from governments, civil society, technical agencies and other private sector, the smart effective health investments pioneered by the Global Fund have saved 38million lives by providing prevention, and treatment to millions of people geared towards revitalizing the global health system (The Global Fund, 2020).

Similarly, a conference held at Beijing in 2006 which comprises of 800 representatives from 100 countries across the world and 20 international agencies look at how countries of the world can curtail the spread of bird flu influenza virus. A statement released by Margaret Chan, the WHO assistant director at the International Pledging Conference on Avian and Human Pandemic Influenza revealed that a pandemic of avian influenza could affect close to millions of people and rived the economy into depression (Moore et al. 2017). To prevent this loss, evidence abounds that pledges of funds came from richer countries like United States having a total share of $334 million, European Union $260 million, Japan $159 million, Russia $45 million, and Australia $42 million (Moore et al. 2017). According to WHO (2006), about 6% of the fund is to be allocated to human exposure, 22% to warning systems; 26% for rapid containment of spread; 28% for capacity building and 17% for vaccine development. In addition, a total sum of $58 million should be set aside for stockpile for antiviral protection drugs and individual protective equipment and supplies.

As part of effort to prevent the impact of diseases outbreak across the world, World Health Organization (WHO) in 2017 bulletin remarked titled “Options for financing pandemic preparedness” averred that the devastating death toll of Ebola outbreak of 2013-2016 accounted for 11,310, with Guinea, Liberia and Sierra Leone losing a total sum of 2.2 billion dollars gross domestic product (GDP) (WHO, 2017). In order to support countries hardest hit by Ebola outbreak, the World Bank mobilized a sum of US$1.62 billion as part of effort to build strategic plans that will prepare countries for pandemic outbreak (Katz and Seifman, 2016). Corroborating the above view, on February 5th 2020, The Bill and Melinda Gates Foundation announced that it will immediately fostered positive responses through viable commitment of $100 million for global response to 2019 Coronavirus in order to strengthen detection, isolation, treatments efforts and development of vaccines and diagnostic centers (Gates Foundation, 2020) for affected countries.

To further respond to global health challenges and the implication of pandemic on economic growth, New-York Times (2005) revealed that global human pandemic could cause $800 billion economic losses. To avert this problem and further prepare countries against this hit, in 2005, a $500 million loan program was initiated by World Bank for the main purpose of strengthening and getting money swiftly to Southeast Asian countries who has been dangerously hit by avian flu virus. While diseases outbreak are increasingly phenomena in human society and some are unlikely to become epidemics because the pathogen are not easily transmissible, it is important to note that human actions induce how infections become pandemic (World Bank, 2013). Human actions can easily affect whether a particular disease become global pandemics or not (World Bank, 2013). Funding pandemics remains a major issue in diseases management and how funds are circulated, used and diverted in the cyberspace remain poorly studied. Even when funds are disbursed by stakeholders, diversions remain worrisome and make effective utilization for disease control ineffective and wasteful. Thus the need for more researches in this remit.

Coronavirus Pandemic, Cybercrime and Diversion of funds

According to US Department of State, government has allocated $20.5 billion to benefit international response in relation to social commitment to vaccine production, therapeutics, preparedness efforts and foreign assistance (US Department of State, 2020). Ever since the emergence of coronavirus, report from the Department of State documented that the United States Government (USG) has spent more than $1.5 billion in emergency health, humanitarian, economic, and development assistance specifically aimed at helping governments, international organizations, and non-governmental organization (NGOs) to fight the pandemic. Report from World Bank (2020) titled "Fact Sheet: Pandemic Emergency Financing Facility" reported that on April 27, 2020, Steering Body of the PEF allocated a sum of US$195.84 million to 64 world's poorest countries to fight coronavirus. As of September 30, 2020, US$195.84 million COVID-19 palliative fund has been transferred to support 64 countries of the world (World Bank, 2020).

In a statement released by Andrew Bailey (The Bank of England Governor), amid fear of surge in unemployment in Britain hotels, the bank announced on 18th of June, 2020 that a new £100 billion stimulus package will be disbursed to rescue UK economy from going into recession (The Guardian, 2020). A report published by KPMG (2020) revealed that the Central Bank of Nigeria has set out different measures to combat the impact of the coronavirus through pumping of 50 billion naira to support the country's economy targeted at households, micro and small enterprises (KPMG, 2020). As massive amount of funds is disbursed globally to counteract Coronavirus, what role is technology playing in enabling criminals tamper with these lifesaving funds? This question is very important as the world struggle to contain the pandemic and this is the next focus of this article.

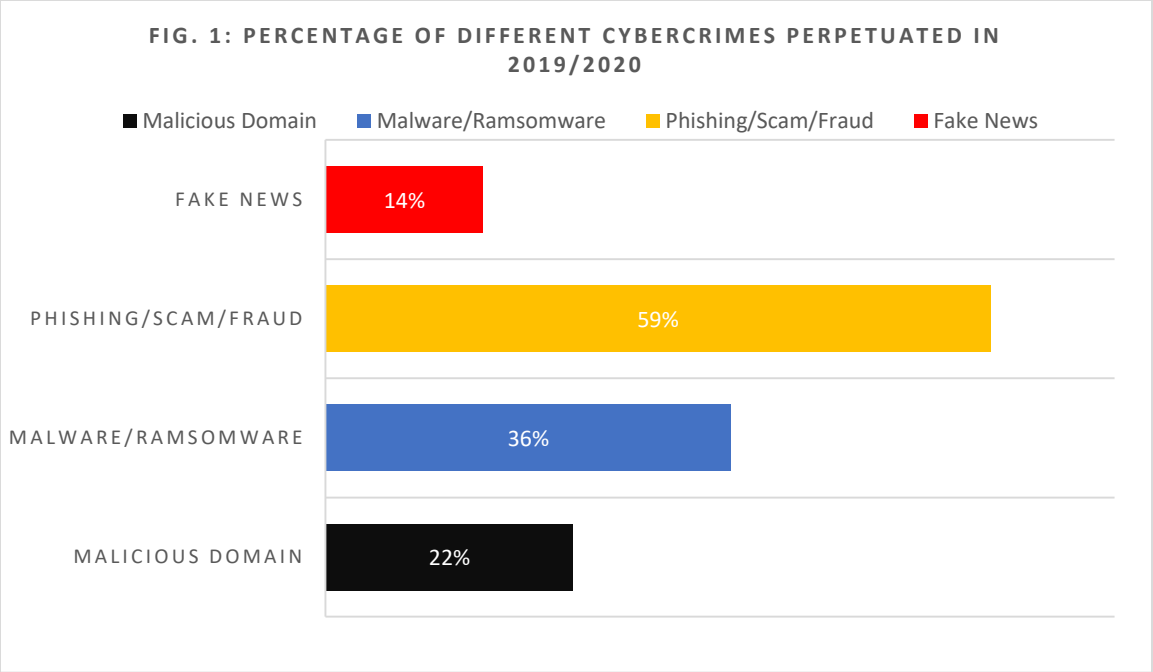
The role of Information and Communication Technology (ICT) in this 21st century cannot be underemphasized especially when taking a look at how ICT has revolutionized the whole sectors of human endeavours. With the adoption of digital technologies, present societies are heavily relying on the internet to carry out day to day activities of their businesses with several benefits (Omodunbi, Odiase, Olaniyan and Esan, 2016). While the adoption of technologies has increased efficiency of systems and nations, it is also important to note that the harm which the advent of ICT has done on the society is becoming enormous and this can be seen in cyberattacks on funds and people during the Coronavirus Pandemic. With broad adoption of digital technologies in all shereof society, it has also created lacuna which if not filled may destroy the entire global system (Omodunbi, Odiase, Olaniyan and Esan, 2016). Such is the case of cybercrime that has become a bottleneck for most societies to curtail. According to Akanle and Shadare (2020), Akanle and Shadare (2019) and Okeshola and Adeta (2013) cybercrime is any form of criminal activities that involve the use of computers and internet facility to perpetuate illegal acts. These forms of illegal act involve theft, forgery, blackmail, embezzlement that are contrary to social norms of society (Akanle, Adesina and Akarah, 2016).

Maitanmi (2013) supported the above definition by defining cybercrime as any crime committed by criminals who makes use of the computer networks as a tool in capturing varieties of objectives not limited to illegal downloading of music files, piracy, spamming and many more. In the past, little is known about the phenomenon of cybercrime. However, with the emergence of internet, the unintended digital information has manifested in global luminosity. Hassan et al. (2012) and Wada and Odulaja (2012) categorized cybercrime to include cyber terrorism, cyber fraud, malware, spamming, wiretapping, logic bombs, phishing and password sniffing. Cyber terrorism involves the use of computer network to disrupt national peace, public infrastructures and sponsoring of terrorist for the main purpose of achieving social and political gain (Hassan et al. 2012). Cyber fraud involves the use of cyber space for illegal transfer of funds from innumerable accounts for the main aim of achieving personal aggrandizement (Odiase, Olaniyan and Esan, 2016). Malware (also known as malicious software) refers to the use of computer software to harness individual data without proper consent (Umaru, n.d).

Malicious software can be in form of Trojan (illegal action with the impression of been legitimate), logic bomb (the use of slow and dormant host system that disrupt files), trapdoor (the process of circumventing access control mechanism), ransomware (encryption of victim device with unknown code for the purpose of demanding ransom in exchange for the data recovery) and Zombie (the process of launching a coordinated attack) (Powell and Stroud, 2003). Spamming refers to sending unsolicited bulk electronic mail to victim through electronic mail system (Umaru, n.d). Wiretapping refers to illegal eavesdrop access to individual communication and banking details (credit card, ATM pin and Bank Verification Number) (Omodunbi etal. 2016; Umaru, n.d). Password sniffing involves the use of installed networks crackers to collect bytes of network connection for the main purpose of retrieving username and passwords of individuals visiting the website (Hassan et al. 2012). Phishing involves the theft of identity which involves fraud and stealing personal information from public authorities, financial institutions and businesses to lure potential individuals for crime victimization (Omodunbi, Odiase, Olaniyan and Esan, 2016, Moshin, 2006, Moshin, 2006).

The rate at which cybercrime is growing is worrisome. It is estimated that by 2021, gross loss to cybercrime would have reached $6 trillion (from $3 trillion in 2015) and even infuse on other traditional forms of crime in magnitude and cost (Anderson et al. 2019). Lakshmi (2015) averred that as at 2003, the United States and South-Korea are listed among countries having the highest rates of cyber-attacks of 35.4% and 12.8% respectively. However, considering the series of cyber-attacks that is occurring across the globe, it is not surprising that similar events have erupted during the COVID-19 pandemic. The outbreak of 2019 pandemic has caused massive havoc worldwide, with people being forced to adapt their activities to new reality such as working from home, wearing of face mask, social and/or physical distancing, massive shopping online, confinement to home and business, minimal of physical contacts and relationships and shock of the novel virus (WHO, 2020 and NHS, 2020). These situations, as opined by Harjinder et al. (2020), can overwhelm lots of individuals, cause stress and anxiety that will later increase vulnerability to cyber-attacks. The implication of this pandemic is that companies have to improvise and change the working patterns by adopting new working structures, thereby leaving potential assets and valuable data less secured than before for the sake of interoperability (Harjinder et al. 2020).

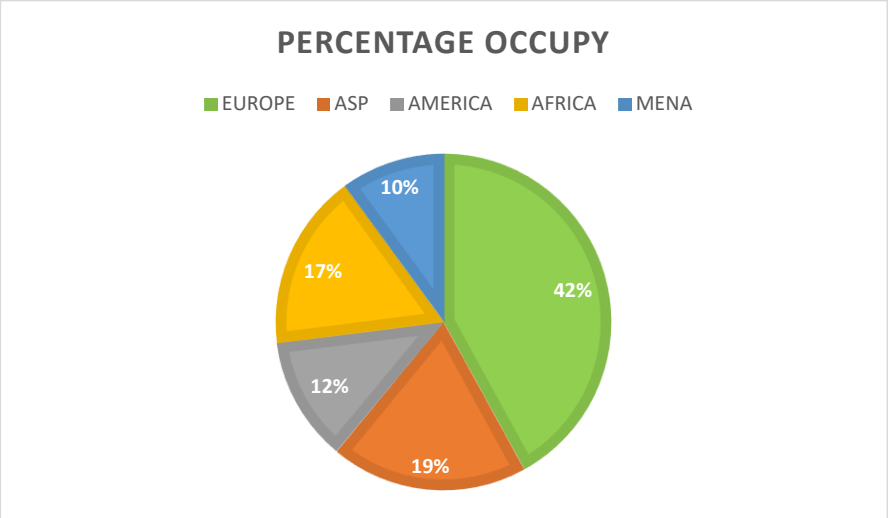
As a result of the global directives by national governments to curtail the contagions of the virus, several workers are now confined to their homes thus engaging in teleworking with computers and internet facilities as major instruments (National Crime Agency, 2020). Consequently, cybercriminals are capitalizing on this work schedules to trick people by mounting on their anxiety for COVID-19 relief messages (Department of Justice, 2020). Since the emergence of the COVID-19, the number of online scams and malware have considerably increased with phishing and malware occupying larger rate of crime perpetuated by criminals in March 2020 (Shi, 2020; and Kumaran and Lugani, 2020). Data by Interpol (2020) revealed different cyber threats received from countries and private partners across the world. Interpol data show between January and April 2020, 907,000 spam messages were received from private companies, 737 of the messages related to malware and 48,000 of the malicious messages all relative to COVID-19 (Interpol, 2020).



Source: Interpol 2020. COVID-19 Inflicted Cyber-threats Across Countries

During April 2020, as part of effort to prevent email phishing and diffusion of virus to steal personal information from individuals, Google blocked 18 million malware and phishing emails relating to the pandemic (Brien, 2020). In order to keep the general public abreast of likelihood of success these attacks may have on sales and demands for goods (E-commerce store, Personal Protection Equipment (PPE) and Coronavirus kits), and impersonation of public figures, blocking malicious mails from acting on the cyber space becomes general concern for different countries to uphold (Kumaran and Lugani, 2020). In light of these events, Interpol Cybercrime Directorate (2020) produced global assessment of COVID-19 related crime across 194 countries. The report stressed further as follow; in Africa, the surge in phishing, charity and sextortion and circulation of fake news have been rampant. In Americas, there is an increase in phishing and coronavirus fraud campaign, massive target of teleworking employees to steal sensitive information and increment in online child sexual exploitation by criminals. In Asia, circulation of fake news and misinformation relating to COVID-19 and lack of cybersecurity awareness and unhygienic environment have also been documented. In Europe, Middle East and North Africa, there is significant increase in malicious domains registered as corona and deployment of ransomware against critical infrastructure and health system charged with the responsibility of mitigating COVID-19 (Interpol, 2020).

Fig. 2: Cybercrime by Geography



Source: Interpol Region Cybercrime Survey

The cybercrime incidents emerging from COVID-19 pandemic posed serious concern for individual safety and world in general. Recently in Nigeria, the Federal government advised Nigerians to be meticulous on existing android based malicious and fraudulent ransomware application that pass updates regarding COVID-19. Evidence suggests a ransomware have been installed on the website (https://www.coronavirusapp.site/), which blocks citizen access to their personal data and accounts and issued a threat that payment of $100 have to be made within 48 hours to avoid losing their accounts (Punchng, 2020). In April 27, 2020, about 30 companies were arrested in US for involvement in fraudulent, unapproved, and misbranded sales of product relating to COVID-19 as a way of ameliorating and mitigating COVID-19 through the sales of these products on the company social media and websites (FTC, 2020). Among companies that were arrested was Free Speech Systems LLC that directs customers from www.infowars.com and www.baned.video to www.infowarsstore.com to purchase products like Superblue Sliver Immune Gargle, Super Sliver Whitening Toothpaste, Super Sliver Wound Dressing Gel, and Superblue Floride Tree Toothpaste that will address growing effect of COVID-19 on US citizen (FTC, 2020). The popular website called John Doe with the url (www.coronavirusmedicalkit.com) was identified as one of the fraudulent websites that tries to impersonate World Health Organization (WHO) through luring any visitor who visit their website to pay $4.95 vaccine kit shipping.

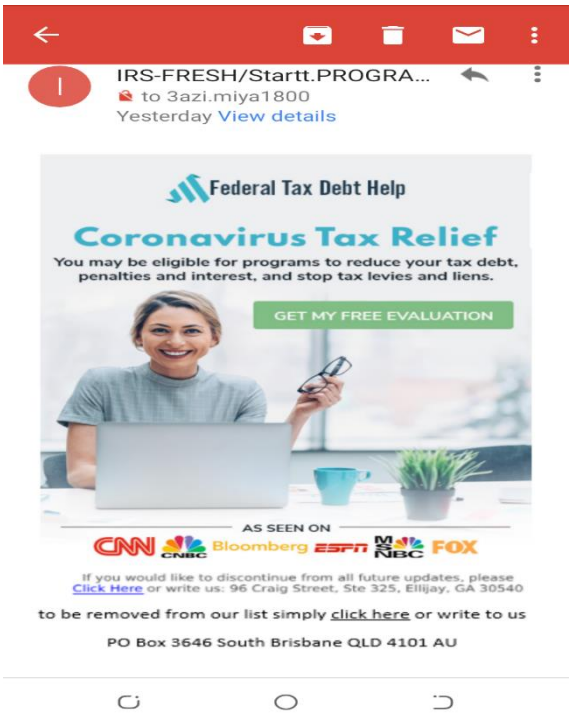
Upon visiting the website, a link has been inserted on the website that once clicked, it redirects individuals to FedEx logo page where they will have opportunity to input their card details so as to order for the COVID-19 kit. The claims made on the website with the photograph of Dr. Anthony Fauci (the Head of National Institute of Allergy and Infectious Diseases at the National Institutes of Health) have been declared false as all information on the website were only geared towards adding imprimatur to fraudulent act (Eboibi, 2020). In January, 2020, NCSC reported that in Japan a banking Trojan depicted as state welfare providers were sent across to many banking sector in the countries to breach the security system of most financial institution (NCSC, 2020). Similarly, in US, Indonesia and Italy, attempts were also made to steal public and state information through the deployment of 'Lokibot infostealer', Remcos RAT and other malicious software (NCSC, 2020).

In Nigeria (Africa's largest economy), one popular cybercrime strategy is impersonation of banking sector whereby cybercriminals pretend to be victims' bank account officers by putting a call through, requesting victims' names, dates of birth, Bank Verification Numbers, account

numbers and Automated Teller Machine (ATM) pins to facilitate proper registration of federal government N25,000 Covid-19 palliative funds (The Cable, 2020). It was reported by Interpol on the 9th September, 2020 that two suspects were arrested who were believed to be the mastermind of huge Germany Health Authorities fraud of £2.4 million fraudulent facemask (Interpol, 2020). Information from CNN (2020) also revealed how Ramon Olorunwa Abbas popularly known as *Hushpuppi* was arrested by United Arab Emirates on June 25 2020 for Business Email Compromise (BEC) scams. BEC is a fast-growing form of cyber fraud that involve hacking into corporate emails and sending fake messages to different clients for the purpose of redirecting money transfer and stealing of bank details. *Hushppupi* was also accused of cybercriminally diverting Covid-19 funds meant for indigenous Americans. *Hushppupi* was accused of several crimes including fraudulent transfer of US$1 trillion from a New York based law firm, cyber heist fraud of foreign financial institutions amounting to $14.7 million and an attempted fraud of English Premier League football club to steal a whooping sum of $125 million (OCCRP, 2020, Eboibi, 2020). The Hushpuppi case demonstrates how daring, pervasive and dangerous cybercrime has become in the age of Coronavirus. Although Hushpuppi has been shattered and arrested, there are certainly many Hushpuppies still carrying out their cybercrime enterprise and targeting Covid-19 funds.

Cybercrime and Covid-19 funding and others targeting operates across levels including national, international, corporate and personal. The illustrations and templates below show examples of different phishing emails sent to one of the authors of this article:

Fig. 3 & 4: Examples of Phishing Emails (Source: Auhours' Email Accounts)



Similarly, another organization phishing mail sent to Trish Sunnet (adolorpatricia30@gmail.com cited in Eboibi, 2020) is also highlighted below:

> this is not a joke. Aliko Dangote is set to put a smile on every Nigerian citizens face. he wants to do what federal government failed to do! fg promised to pay 8500 to weekly allowance to Nigerians during the pandemic but failed. in a bid to control the spread now dangote is set to put a smile on our face. all Nigerian citizens are entitled to 20000 weekly allowances just to stay safe. click to apply ðy €'‡ðy €'‡ðy €'‡ https://tinyurl.com/ dangotefoundationfund.

According to Eboibi (2020), the purpose of sending these malicious mails is to diffuse viruses, Trojan, and ransomware, to harvest with the main aim of defrauding victims even during Coronavirus pandemic. In the absence of any statutory enactment to prosecute cyber coronavirus fraud, several countries still rely heavily on constitutional laws enacted prior to advent of COVID-19. In the UK, the prosecution of fraud can be undertaken under the UK Fraud Act of 2006. Under the UK Fraud Act of 2006 Section 1(1) "a person is guilty of cyber fraud if he or she has breached any section listed under section 2 (the section proscribed several ways of committing any cyber offense) and subsection 2(a) (fraud by false representation) of the UK cyber laws (UK Fraud Act, 2006). The United States of America (USA) provided a clear definition that "if a criminal is found guilty of cybercrime and convicted, such criminals will be liable to twenty years imprisonment (Sarbanes Oxley Act, 2002). Furthermore, in Nigeria Section 14(2) and Section 22 of the Cybercrime (Prohibition, Prevention, etc) Act, 2015 stressed that any person who with intent to defraud sends electronic message materially misrepresents any fact or set facts upon which reliance the recipient or another person is caused to suffer any damage commits an offence and shall be liable on conviction to imprisonment for a term of not less than 5 years and to a fine of not less than N10,000,000.00 or both fine and imprisonment.(Cybercrimes Prohibition, Prevention, etc Act, 2015). It is important to note that most of these laws as spelt out in different countries, especially in developing countries, only exist in paper while the implementation and enforcement have been jeopardized due to corruption among law enforcement agencies and officers (Akanle, Adesina and Akarha, 2016, Akanle and Shadare, 2019, Akanle and Shadare, 2020), weak cyber vigilance and poor cyber capacities specially to tackle Covid-19 string of cybercrime.

Conclusion

As the world battles the Coronavirus Pandemic, it is important to appreciate the fact that the disease has generated remarkable social, economic and systemic circumstances that are peculiar and being leveraged on by cybercriminals to dupe unsuspecting nations, organizations, societies and individuals. Unfortunately, researches are too little in this area. Thus, the need for this exploratory article to fill this important gap. The outbreak of Coronavirus virus has ignited several reactions from governments and stakeholders including rolling out different legislations, health regulations, lockdowns and financial interventions. As workers in organizations now work more remotely and governments as well as partners disburse intervention funds online, cybercriminals are on the prowl taking advantage and targeting Covid-19 funds and others. Hence, as people are utilizing this period to seek safety and maximize their income, cybercriminals are also using this *opportunity* to defraud individuals, groups, nations and organizations through sending of malicious mails and cyber hacking.

While governments are partnering organizations and individuals to mitigate and counteract COVID-19 pandemic hardship through distribution of palliative incentives to citizens, including fund disbursement, cybercriminals are constituting huge challenge and this is what this article has explored. It is therefore imperative for critical stakeholders and indeed everyone in the virtual world to pay more attention to cybercriminals at this time guard against their activities. There is the need to create more awareness about how people can protect themselves digitally during this pandemic. And governments, development partners, technology giants and the media- social and traditional- should play active and frontline roles in this regard.

REFERENCES

Ahmad S. L. and Ahmad A. (2020). "COVID-19 pandemic – an African perspective, Emerging Microbes and Infections". 9:1, pp.1300-1308. DOI:10.1080/22221751.2020.1775132

Akanle, O. and Shadare, B. R. (2020). Why has it been so difficult to counteract Cybercrime in Nigeria: Evidence from an Ethnographic Study. *International Journal of Cyber Criminology.* 14.1, 21-43.

Akanle, O. and Shadare, B. R. 2019. Yahoo-plus in Ibadan: Meaning, Characterization and Strategies. *International Journal of Cyber Criminology.* 13. 2, 343-357.

Akanle, O., Adesina, J.O. and Akarah, E.P. 2016. Towards human dignity and the internet: The cybercrime (yahoo yahoo) phenomenon in Nigeria. *African Journal of Science, Technology, Innovation and Development.* 8.2. Pp. 213-220.

American Delta Association (ADA). 2020. "Be Alert for Cybercrime Scams". ADA, publish.

Amzat J; Aminu K; Kolo V.I; Akinyele A.A; Ogundairo J.A; and Danjibo M.C; 2020. "Coronavirus Outbreak in Nigeria: Burden and Socio-Medical Response during the First 100 Days." *International Society for Infectious Diseases*. Available at: www.elsevier.com/locate/ijid

Anderson R. C. Barton, R. Bolme, R. Clayton, C. Ganan, T. Grasso, M. Levi, T. Moore, and M. Vasek. 2019. "Measuring the changing cost of cybercrime," *Workshop on the Economics of Information Security (WEIS)*, 2019.

BBC News. 2020. "Coronavirus Lockdown: Nigerians Cautious As Restrictions Eased In Lagos and Abuja. Available at: www.bbc.com/news/amp/world-52526923

Brien. T.L. 2020. "Covid aid scams and dodgy deals could have been avoided." Available at: https://www.bloomberg.com/opinion/articles/2020-05-01/coronavirus-trillions-in-aid-draws-scams-anddodgy-deals

CDC. 2020. "Africa Centres for Disease Control and Prevention. Africa CDC establishes continent-wide task force to respond to global coronavirus epidemic". Available from: https://africacdc.org/news/africa-cdc-establishes-continent-wide-taskforce-to-respond-to-global-coronavirus-epidemic/

CDC. 2020. "COVID-19 Dashboard". Available at: https://africadc.org/covid-19/

CDC. 2020. Africa Centres for Disease Control and Prevention. Africa CDC establishes continent-wide task force to respond to global coronavirus epidemic. Available from: https://africacdc.org/news/africa-cdc-establishes-continent-wide-taskforce-to-respond-to-global-coronavirus-epidemic/

Central Bank of Nigeria (CBN) 2020. "Alert Beware of COVID-19 Cyber Attacks". CBN Press Release. Available at: www.cbn.gov.ng

Chiou, C. 2006. "Does penicillin remain the drug of choice for pneumococcal pneumonia in view of emerging in vitro resistance"? *Clin. Infect. Dis. 42*, 234–237.

CNN. 2020. "He flaunted Private Jets and Luxury Cars on Insragram. Feds Used His Posts to Link Him to Alleged Cyber Crimes". Available at: www.amp.cnn.com/cnn/2020/07/12/us/ray-hushpuppi-alleged-money-laundering-trnd/index.html

Cybercrimes (Prohibition, Prevention etc.) Act 2015. 14(2).

Department of Justice. 2020. "Georgia Man Arrested for Attempting to Defraud the Department of Veterans Affairs in a Multimillion-Dollar COVID-19 Scam" https://www.justice.gov/opa/pr/georgia-man-arrested-attempting-defrauddepartment-veterans-affairs-multimillion-dollar-covid

Department of Justice. 2020. "National Crime Agency warn that organized crime groups may try to exploit the coronavirus outbreak to target the UK**".** Available at**:**

https://www.nationalcrimeagency.gov.uk/news/national-crime-agency-warn-thatorganised-crime-groups-may-try-to-exploit-the-coronavirus-outbreak-to-target-the-uk

Du Toit A. 2020. "Outbreak of a novel coronavirus". *Nat Rev Microbiol*. 18:123. Doi: 10.1038/s41579-020-0332-0.

Eboibi F. E. 2020. "Cybercriminals and Coronavirus cybercrimes in Nigeria, the United States of America and the United Kingdom." *Cyber hygiene and preventive enforcement measures, Commonwealth Law Bulletin*, DOI: 10.1080/03050718.2020.1834424

Europol. 2020. "Pandemic Profiteering: How Criminals Exploit COVID-19 Crisis". https://www.europol.europa.eu/publicationsdocuments/pandemic-profiteering-how-criminals

Felson M. and Cohen L.E. 1980. "Human Ecology and Crime: A Routine Activity Approach." *Human Ecology,* 8(4), pp. 389-405.

Finkler, D. 1899. "Influenza in twentieth century practice". In *An International Encyclopaedia of Modern Medical Science*; Shipman, T.L., Ed.; Sampson Law & Marston: London, UK, pp. 21–32.

Forster P, Forster L, Renfrew C, et al. 2020. "Phylogenetic network analysis of SARS-CoV-2 genomes". *Proc Natl Acad Sci*, U S A.

FTC. 2020. "FTC Coronavirus Warning Letters to Companies." Available at https://www.ftc.gov/coronavirus/enforcement/warning-letters

Gilbert M, Pullano G, Pinotti F, et al. 2020. "Preparedness and vulnerability of African countries against importations of COVID-19: a modelling study". Lancet. 395: 871–877. Doi: 10.1016/S0140-6736(20)30411-6.

Harjinder S.L; Lynsay A.S; Jason R.C.N; Arnau E; Gregory E; Carsten M; and Xavier B. 2020. "Cyber Security in the Age of COVID-19: A timeline and analysis series of cybercrime and cyber-attacks during the pandemic". Available at: arXiv: 2006:11929v1

Hassan A. B., Lass F. D. and Makinde J. 2012. "Cybercrime in Nigeria: Causes, Effects and the Way Out". *ARPN Journal of Science and Technology*, vol. 2(7), 626 – 631.

Hassan, A. B. Lass F. D. and Makinde J. (2012) *"*Cybercrime in Nigeria: Causes, Effects and the Way Out*". ARPN Journal of Science and Technology*, vol. VOL. 2(7), 626 – 631.

Hirsh. 1883. *"*Handbook of Geographic and Historical Pathology.*"* New Sydenham Society: London, UK.

Humphries, M. 2013. "Paths of infection: The First World War and the origins of the 1918 influenza pandemic." *War Hist*. *21*, 55–81.

Huysamen G.K; 1994. "Methodology for the Social Sciences and Behavioural Sciences". *Halfway House: Southern Book Publishers.*

Ihekweazu C. 2020. "Steps Nigeria is taking to Prepare for Cases of Coronavirus". Available at: http://theconversation.com/steps-nigeria-is-taking-to-prepare-for-cases-ofcoronavirus-130704

International Monetary Fund (IMF). 2020. "Policy responses to COVID-19". Available from: https://www.imf.org/en/Topics/imf-and-covid19/Policy-Responses-to-COVID-19

International Monetary Fund. 2020. "Policy responses to COVID-19". Available from: https://www.imf.org/en/Topics/imf-and-covid19/Policy-Responses-to-COVID-19

Interpol. 2020. "Cybercrime - COVID-19 Impact". Available at: www.interpol.int

Interpol. 2020. https://www.trendmicro.com/vinfo/fr/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains

Investopedia. 2020. "The Special Economic Impact of Pandemics – Expect effects to be massive in ways that differ from other disasters". Available at: www.investopedia.com/special-economic-impact-of-pandemics-4800597

Kacmarek, R.M. 2011. “The mechanical ventilator: Past, present, and future”. *Respir. Care 56*, 1170–1180.

Katz R. and Seifman R. 2016. “Opportunities to finance pandemic preparedness”. *Lancet Glob Health*. 4(11), 782-3. http://dx.doi.org/10.1016/S2214-109X(16)30202-9pmid:27692862

KPMG. 2020. “The Central Bank of Nigeria Pledged Fund to Critical Sectors of the Economy…” Available at: https:home.kpmg/xx/en/home/insights/2020/04/Nigeria-government-and-institution-measures-in-response-to-covid.html#:~:text=The%Central%20Bank%20pledged%20to,critical%20sectors%20of%20the%20economy.&text=Similar%20moratorium%20to%20be%20given,the%20Nigeria%20Export-Import%20Bank

Krebs on Security. 2020. “Live Coronavirus Map Used to Spread Malware.” Available at: https://krebsonsecurity.com/2020/03/live-coronavirusmap-used-to-spread-malware/

Kumaran N. and Lugani S. 2020. “Protecting businesses against cyber threats during covid-19 and beyond.” Available at: https://cloud.google.com/blog/products/identitysecurity/protecting-against-cyber-threats-during-covid-19-and-beyond

Lakshmi P. and Ishwarya M. 2015. *“*Cyber Crime: Prevention and Detection*”.* International *Journal of Advanced Research in Computer and Communication Engineering*, vol. Vol. 4(3).

Langmuir, A.D. 1961. “Epidemiology of Asian influenza”. *Am. Rev. Respir. Dis. 83*, 2–18.

Maitanmi, O. Ogunlere, S. and Ayinde S. 2013. “Impact of Cyber Crimes on Nigerian Economy” The International Journal of Engineering and Science (IJES, vol 2(4), 45–51.

Markel, H.; Stern, A.M.; Navarro, J.A.; Michalsen, J.R.; Monto, A.S.; DiGiovanni, C., Jr. 2006. “Non-pharmaceutical influenza mitigation strategies, us communities, 1918–1920 pandemic”. *Emerg. Infect. Dis. 12*, 1961–1964.

Mo Ibrahim Foundation. 2020. “COVID-19 in Africa: A call for coordinated governance, improved health structures and better data”. Available from: https://mo.ibrahim

Mohsin, A. 2006. “*Cybercrimes and Solutions*”. Retrieved from http://eziniearticles.com/?Cyber-Crimes-AndSolutions&id=204167

Moore M, Gelfeld B, Okunogbe A, et al. 2017. “Identifying future disease hot spots: infectious disease vulnerability Index”. Rand Health Q; 6(5). Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5568150/

Morens, D.; Taubenberger, J.; Fauci, A.S. 2009. “The persistent legacy of the 1918 influenza virus”. *N. Engl. J. Med. 361*, 225–229.

Nairametrics. 2020. “List of all companies and billionaires that have contributed to COVID-19 Relief Fund”. Available at: https://nairametrics.com/2020/04/18/list-of-all-companies-and-billionaires-that-have-contributed-to-covid-19-relief-fund/

National Crime Agency (NCA). 2020. “Beware of Crime”.

NCA. 2020. “Beware of fraud and scams during Covid-19 pandemic fraud.” Available at https://www.nationalcrimeagency.gov.uk/news/fraud-scams-covid19 April 2020.

NCDC. 2020. “First Case of Coronavirus Disease Confirmed In Nigeria. Available at: ncdc.gov.ng/news/227/first-case-of-corona-virus-disease-confirmed-in-nigeria.

NCSC. 2020. “Coronavirus-themed Attacks Target Global Shipping Concerns”. Available at: https://www.proofpoint.com/us/threat-insight/post/coronavirus-themed-attacks-target-global-shipping-concerns

New York Times. 2020. Available at: www.nytimes.com/2005/11/07/health/world-bank-creates-500-million-loan-plan-to-combat-bird-flu.html

NHS. 2020. "10 tips to help if you are worried about coronavirus". https://www.nhs.uk/oneyou/every-mindmatters/coronavirus-covid-19-anxiety-tips

Okeshola F.B. and Adeta A.K; 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(9), 98-114.

Omodunbi B.A; Odiase P.O; Olaniyan O.M. and Esan A.O. 2016. "Cybercrime in Nigeria: Analysis, Detection and Prevention". *FUOYE Journal of Engineering and Technology*, 1(1), 2579-0617.

Organized Crime and Corruption Reporting Project (OCCRP) 2020. "Alleged Cyber-Godfather Hushpuppi Arrives in US". Available at: www.occrp.org/en/daily/12704-alleged-cyber-godfather-hushpuppi-arrives-in-us

Palmer, J. 2014. "Chinese labour corps". *World Chin. 4*, 25–26.

Patrick R. and Krewski D. 2016. "Reviewing the History of Pandemic Influenza: Understanding Patterns of Transmission". *McLaughlin Centre for Population Health Risk Assessment, University of Ottawa, 850 Peter Morand Crescent*.

Patterson, K.D. 1987. *"*Pandemic Influenza 1700–1900: A Study in Historical Epidemiology*."* Rowan & Littlefield: Totowa, NJ, USA, 1987.

Payne, A.M. 1958. "Symposium on the Asian influenza epidemic". *Proc. R. Soc. Med. 51*, 1009–1015.

Potter, C. 1998. "Chronicle of influenza pandemics". In *Textbook of Influenza*; Nicholson, K.G., Webster, R.F., Hay, A.J., Eds.; Blackwell Science LTD: Oxford, UK.

Potter, C. 2001. "A history of influenza". *J. Appl. Microbiol. 91*, 572–579.

Powell D. and Stroud R. 2003. "Conceptual Model and Architecture of MAFTIA". MAFTIA.

Pyle, G.F. 1986. *"*The Diffusion of Influenza: Patterns and Paradigms"*. Rowan & Littlefield: Totowa, NJ, USA.*

Pyle, G.F.; Patterson, K.D. 1984. "Influenza diffusion in European history: Patterns and paradigms". *Ecol. Dis. 2*, 173–184.

Rubin H. 2011. "Future Global Shocks: Pandemic". OECD. *Multi-Disciplinary Issues, International Futures Programme.* University of Pennsylvania.

Shabir Ahmad Lone and Aijaz Ahmad 2020. "COVID-19 pandemic – an African perspective, Emerging Microbes & Infections". 9:1, 1300-1308 DOI:10.1080/22221751.2020.1775132

Smith, G.J.; Vijaykrishna, D.; Bahl, J.; Lycett, S.; Worobey, M.; Pybus, O.G.; Ma, S.K.; Cheung, C.L.; Raghwani, J.; Bhatt, S.; et al. 2009. "Origins and evolutionary genomics of the 2009 swine-origin H1N1 influenza an epidemic". *Nat. Med. 459*, 1122–1125.

The Cable. 2020. "ALERT: Zenith Bank warns against fraudsters, says 'we're not disbursing COVID-19 funds". Available at https://www.thecable.ng/alert-zenith-bank-warns-against-fraudsters-says-were-not-disbursing-covid-19-funds

The Gates Foundation. 2020. Available at: www.gatesfoundation.org/Media-Center/Press-Releases/2020/02/Bill-and-Melinda-Gates-Foundation-Dedicates-Additional-Funding-to-the-Novel-Coronavirus-Response

The Global Fund. 2020. Available at: www.theglobalfund.org/en/overview/

The Guardian. 2020. "Bank of England pumps an extra £100bn into UK economy". Available at: www.amp.theguardian.com/business/2020/jun/18/bank-of-england-uk-economy-quantitative-easing-coronavirus-crisis

The Punch. 2020. *"*FG alerts Nigerians to dangerous computer coronavirus." Available at https://punchng.com/fg-alerts-nigerians-todangerous-computer-coronavirus/

The Sarbanes-Oxley Act of 2002, (codified as amended at (2006 & Supp. 2007)).

The Times. 2020. “Fraudsters impersonate airlines and Tesco in coronavirus scams.” Available at: https://www.thetimes.co.uk/article/fraudstersimpersonate-airlines-and-tesco-in-coronavirus-scams-5wdwhxq7p

UK Fraud Act 2006. Available at: **http://www.legislation.gov.uk/ukpga/2006/35/**section/1

Umaru Ibarahim. n.d. “The Impact of Cybercrime on the Nigerian Economy and Banking System”.

US Department of State 2020. “Update: The United States Continues to Lead the Global Response to COVID-19”. Available at www.state.gov/update-the-united-states-continues-to-lead-the-global-response-to-covid-19-5/

USDHHS. 2016. “The Great Pandemic: The United States in 1918–1919”. Available online: http://www.flu.gov/pandemic/history/1918/index.html (accessed on 9 March 2016).

Valeron, A.J.; Cori, A.; Waltat, S.; Meurisse, S.; Carrat, F.; Boelle, P.Y. 2010. “Transmissibility and geographic spread of the 1889 influenza pandemic”. *Proc. Natl. Acad. Sci. USA*, *107*, 8778–8781.

Viboud, C.; Simonsen, L.; Fuentes, R.; Flores, J.; Miller, M.A.; Chowell, G. 2016. “Global mortality impact of the 1957–1959 influenza pandemic.” *J. Infect. Dis. 213*, 738–745.

Wada F. and Odulaja G. O. 2014, "Electronic Banking and Cyber Crime in Nigeria - A Theoretical Policy Perspective on Causation" *Afr J Comp and ICT*, 4(3), no. Issue 2

Waring, J. 1971. *“*A History of Medicine in South Carolina*”*. South Carolina Medical Association: Columbia, SC, USA, 1971.

Weforum. 2020. “A Visual History of Pandemics”. Available at: www.weforum.org/agenda/2020/03/a-visual-history-of-pandemics

White House. 2020. “Presidential Proclamation, Proclamation on Declaring a National Emergency Concerning the Novel Coronavirus Disease (COVID-19) Outbreak.” Available at: https://www.whitehouse.gov/presidential-actions/proclamation-declaringnational-emergencyconcerning-novel-coronavirus-disease-covid-19-outbreak

WHO. 2009. “World Now at the Start of 2009 Influenza Pandemic”. Available online: http://www.who.int/mediacentre/news/statements/2009/h1n1_pandemic_phase6_20090611/en/ (accessed on 23 March 2016)

WHO. 2017. “Option for financing pandemic preparedness”. http://dx.doi.org/10.2471/BLT.17.199695 Available at: www.who.int/bulletin/volumes/95/12/17-199695/en/

WHO. 2020. “Healthy At Home”. https://www.who.int/news-room/campaigns/connectingthe-world-to-combat-coronavirus/healthyathome

World Bank. 2006. “Avian and Human Influenza: Financing the Gaps”. Available at: www.siteresources.worldbank.org/PROJECTS/2015336-1135192689095/20766293/AHIFinancingGAPSFINAL12-21.pdf

World Bank. 2013. “Pandemic Risk”. World Development Report

World Bank. 2020. “Fact Sheet: Pandemic Emergency Financing Facility”. Available at: www.worldbank.org/en/topic/panemics/brief/fact-sheet-pandemic-emergency-financing-facility

World Bank. 2020. “World Bank Group launches *fi*rst operations for COVID-19 (coronavirus) emergency health support, strengthening developing country responses”. Washington, DC. Available from: https://www.worldbank.org/en/news/press-release/2020/04/02/world-bank-group-launches-first-operations-forcovid-19-coronavirus-emergency-health-supportstrengthening-developing-country-responses

World Health Organization (WHO). 2020. Available at: www.who.int/bulletin/volumes/95/12/17-199695/en/

World Health Organization 2019. Available from: https://www.afro.who.int/regional-director/speeches-messages/world-aids-day-2019-messagewho-regional-director-africa-dr

Worldometer. 2020. “COVID-19 Coronavirus Pandemic”. Available at: www.worldometer.info/coronavirus

Zhou P, Yang XL, Wang XG, et al. 2020. “A pneumonia outbreak associated with a new coronavirus of probable bat origin”. Nature. 579:270–273. Doi: 10.1038/s41586-020-2012-7

Zhou P, Yang XL, Wang XG, et al. 2020. “A pneumonia outbreak associated with a new coronavirus of probable bat origin”. Nature. 579:270–273. doi:10.1038/s41586-020-2012-7