DISRUPTIVE TECHNOLOGY ON THE CYBERSPACE: THE CONTESTATION BETWEEN CRIMINAL JUSTICE SYSTEM AND CYBERCRIMINALS

Ezeji, Chiji Longinus
Department of Criminology and Security Studies,
Caleb University, Imota, Lagos.
Email: chiji.ezeji@calebuniversity.edu.ng and clezeji@gmail.com

Abstract

The paper examines the contestation between criminal justice system and cybercriminals. Qualitative methodology was adopted for collecting data. The study sample was drawn from Nigeria Police Crime prevention and Investigative Unit, Cyber forensics experts, officials from the Economic & Financial Crimes Commission (EFCC), Cyber security experts, acadamics in Criminology and Security Studies, judges and prosecutors. Theses were interviewed to obtain information on the running battle between the authourites and the criminal elements. Findings revealed that cyber crime increased exponentially despite the promulgation of cybercrime prevention and prohibition Act of 2015. It was reported that Nigeria youth used the lack of empowerment as their excuse to engage in cybercrime. Findings also revealed varied corps of victims, people and local businesses in Nigeria. The paper recommends the need to campaign for moral regeneration, educating internet users on how to stay protected online, appeals for atitutude change among the youths, and those involved in cybercrime, specialised training for criminal justice officials to enable them tackle cyber related crimes.above all, the criminal justice system must be swift in apprehension, prosecution and setencing offenders.

Keywords: Cybercriminals, Cybersystems, Cyberwarfare, Justice and System.

Introduction

The proliferation of internet-related scams and crimes have seriously hurt the country’s image. Cybercrime, popularity known as “Yahoo Yahoo” in Nigeria, is one of the most common forms of cyberspace crime, with damage from the activity expected to cost the global economy heavily. The 419 scams, also called advance fee fraud, are still so common that the FBI carries a warning on its official website, cautioning against responding to a letter or e-mail from Nigeria asking their targets to send personal or banking information (Ezeji, 2020). Advancement in science and technology has not only created new experiences of change in the society, but also in the criminal justice system which is witnessing an increase in the use of such advancements by criminals to accomplish diverse illegal activities. According to Sullivan (2011), there has been a significant increase in the victimization of members of the society via computer networks cyber/online systems. Many people unaware of the dangers of exposing their personal details on the internet, and due to easy accessibility of cyber systems like computers, laptops, tablets, mobile phones and cell phones, expose themselves thus become vulnerable to cyber predators. Cybercrime is the use of internet/cyber system as an instrument
to further illegal ends, such as cyber fraud, drug and child trafficking, child pornography, intellectual property, stealing of identity or violating of privacy. Cybercrime has increased as the internet has become central to commerce, entertainment and governance (Thomas and Loader, 2013). Phishing is one of the most common cyber invasion targeting most sectors in Nigeria. Inadequate control and abuse of systems privileges are other cyber risks faced by the Nigerian financial sector and some government ministries. The abuse of privilege access by external service providers, third parties and contractors are also factors in these techniques. Others include malicious software (malware) attacks which seem prevalent. These are used by cyber criminals in creating support systems to conduct specific cybercrimes such as denial of service. Malware distributed by the social media has also become a popular means of cyber-attack (Jackson, 2012). Identity theft has also increased, this involves the use of email or web pages to convince victims to reveal their personal or financial information and the stolen information used to further other crimes. Web hacking crimes used by criminals to deface government or corporate websites have risen. This act is conducted to embarrass and to prove the security an organisation or government. Philip (2001) asserts that organizations and government which depend on the operation of computer and computer networks can easily be attacked. Cyber terrorists take advantages of factors such as jurisdictions, anonymous sources, easy access to networks, and access to information to create dangerous weapons which are made available on the net. The study resonates with Locard principle that a clue is usually left behind when two or more objects or people come into contact with each other. This is referred to as a reciprocal transfer of traces. The Locard principle means that an investigator can confidently assume that there will always be clues at the scene of the crime. If the investigator cannot find any clues, it is not because there are none but rather, because the techniques required in identifying the clues are not known by the investigator (Pepper, 2011). In its applicability to the practice of cyber-crim, cybercrimes could be committed from any cyber system in the world, if an investigator is not knowledgeable and skilled enough to detect and investigate cyber-crimes, it would be very difficult to apprehend the offenders due to problems associated with jurisdiction. Tracks or clues at the crime scene can be useful to reconstruct, or recreate, the crime scene and to individualize or positively link the perpetrators to the crime. This study evaluates prevalence and seriousness of cybercrime in Nigeria, consequences of cybercrime and the role of the government and criminal justice system in combating cybercrime in Nigeria.

The following questions will be addressed in the study:

- Identify cybercrimes that are prevalent in Nigeria?
- How serious is cybercrime incidences in Nigeria?
- What are the consequences of cybercrime in Nigeria?
- What are the roles of the government and criminal justice system in combating cybercrime in Nigeria?
2.0 Conceptual Framework

Concept of cyber-crimes

The term cybercrime refers to computer related activities which can be carried out by global electronic networks which are illegal or viewed as such by some parties (examples of cyber-crimes are Hackers). Cyber hackers, also known as computer tinkerers, are people who enjoy computer as a hobby or professionals who frequently have illegal or unauthorized access to the cyber systems and thus, damage the systems or the information these systems contain (Ezeji, 2017). According to Joyce and Barrett (2012), majority of attacks by hackers results in huge financial losses and sometimes unreported. There appears to be several reasons why financial organizations are reluctant to report cyber-crime, but chief among them is the potential loss of the public trust in their institutions. Ezeji (2014) defined cybercrime as any crime that involves a computer, cyber systems and a networks. The computer may have been used in the commission of a crime or it may be the target. Net crime refers to criminal exploitation of the internet.

According to Joyce and Barrett (2012), cybercrimes are classified as computer-related crimes. This include; arson (intentionally setting fire to a computer center), burglary: (establishing a computer center illegally to commit a crime therein), extortion/blackmail: (making threat against the operator of a computer center to obtain money), Conspiracy: (several persons agreeing to commit an illegal act on cyber systems), Counterfeit:(copying or imitating computer documents), embezzlement:(fraudulently converting property to personal use); espionage:(stealing secret documents or information), forgery:(issuing false documentation); fraud:(altering false or illegal transfer of funds), malicious damage (destroying computer hardware or software), murder: (tampering with life-sustaining computerized equipment resulting in the death of a patient), receiving : accepting goods of information stolen property by computer knowing that they were stolen), sabotage: intentionally destroying computer information programs or hardware, theft: stealing goods or money by use of a computer or stealing computer parts and materials (Joyce and Barrett, 2012).

The Nigeria Cybercrime Prevention and Prohibition Act (2015), defined cybercrime as any illegal activity that uses computer as its primary means for storing illegal documents and in orchestrating attacks on individuals, private, public and governmental institutions. Cyber-crimes include crime that have been made possible by computers, such as network intrusion and the dissemination of computer viruses, as well as computer-based variations of existing crimes, such as identity theft, stalking, bullying and terrorism. This ACT also provides measures towards safeguarding the nation’s presence in cyberspace while ensuring protection of critical national infrastructure. The ACT focuses on prohibition, prevention, detection, response, investigation and prosecution of cybercrimes and cyber related matters. (NCPA ACT, 2015). Comprehensively, Halder and Jaishankar (2011), classified cyber-related/computer crimes into two categories namely crime targeting cyber systems/computer directly and crime facilitated by cyber system/computer networks or crime that primary target cyber
systems/computer or devices includes; computer viruses, denial of service attack and malware (malicious code).

**Cyber Terrorism**

Arquilla and Ronfeldt (2013) spotlighted the emergence of cybercrimes that are political in nature, ranging from sabotage and defacement of official websites, to the use of the internet to instigate ‘hate’ campaigns by ‘right wing’ extremists, to the activities of terrorist groups aiming to recruit members and to raise funds. The availability of internet, mobile and digital networks are positive development, when in the hands of good people, but when in the wrong hands, are used for nefarious acts. According to Denning (2012) cyber terrorism is the convergence of terrorism and cyberspace which means the unlawful attacks and threats of attacks against computer, networks, and the information stored therein, the act is carried out to coerce government or its people in furtherance of political or social objectives. Cyber-terrorism emerged as the result of advancement in technology and innovations in the area of telecommunication, thus, the cybercriminals use these facilities to orchestrate terrorist attacks on their targets (Lawson, 2011). Furthermore, Philip (2011) defines cyber terrorism as an act of terrorism carried out by using the internet and/or against internet infrastructures.

Politts (2012) asserts that cyber terrorism is a premeditated, politically motivated act against information, computer systems, computer programs, and data which results in violence against a non-combatant targets by sub national groups or clandestine agents. Such attack may lead to death or bodily injury, or cause explosions, plane crashes, water contamination, severe economic loss or serious attack against life and electronic infrastructures which are directed against national security establishment and critical infrastructures. Furthermore, cyber terrorism attacks are directed to life, electronic infrastructures aiming to cause panic in the general public and state terror.

Politts (2012) cited in Ezeji (2014) confirms that, cyber terrorists make use of information technology after proper planning and intelligence gathering, carry out attacks on vulnerable targets due to inadequately security measure in protecting their infrastructure, the security flaws made it possible for cybercriminal to carry out attacks on specific targets. According to Philip (2001), organizations and government that depend on computer operations and networks can easily be attacked. Cyber terrorists take advantage of jurisdictions, anonymous sources, easy access to networks, and access to information in creating dangerous weapons that are readily available on the net. The cyber terrorists use computers to disseminate information and also communicate with their syndicates across other states in preparation to launch an attack or plan methods to launch attacks on their target.

According to Schell (2011), cyber terrorism has become a dominant force in the global battle between information technology and network warfare, however, it is necessary to note that, not all cyber space threats can be classified as terrorism, and failure to distinguish between cyber terrorism and hacking may cause gross panic and fear in the society. Moreover, Ezeji
(2014) points out the difference between cyber terrorism and hacking. Denning (2012) denotes, hacking is the use of software technique to exploit computers or launch attack on targets. Whereas, cyberterrorism is orchestrated by organized cyber criminals and terrorist groups, they make use of sophisticated computer technology to bypass government surveillance in order to carry out destructive acts of violence and the act is premeditated, politically motivated attacks against targets or critical infrastructures. Schell (2011) warned that the threat of cyber terrorism stems from a combination of fear and ignorance, misinformation by some cyber security experts, the exploitation of the general public, the absence of a suitable legal framework and effective software to address cyber terrorism at national and, regional levels, inadequate telecommunication infrastructures and problems associated with poverty, unemployment, lack of social service delivery, food and water, and high crime rates have created avenues for the vulnerability of attacks from cyber criminals.

**Cyber-warfare**

Cyber warfare refers to politically motivated hacking or sabotage activities, in the form of information warfare, sometimes seen as analogous to conventional warfare. Recently, cyber warfare has been considered a larger threat than terrorism and other attacks. Cyber warfare is defined as actions by a nation to penetrate another nation’s computer or networks for the purpose of causing damage or disruption (McNeil, 2012). Cyber warfare attacks are directed to cripple telecommunication, critical infrastructures and computer networks, whereas cyber threat is directed against the public, private facilities and national infrastructures. Cyber warfare consists of different threats and is divided into cyber espionage and cyber-attacks. Cyber warfare could be an espionage and national security breaches or as an attack or practice of obtaining secret, sensitive, proprietary or classified information from individuals, competitors, rivals, groups, government and enemies. Classified information not handled securely can be intercepted and even modified, making espionage possible from the other side of the world (Ezeji, 2014).

According to McNeil (2012) cyber warfare perpetrators target power, water, fuel, communication and transportation infrastructures that are not adequately protected are vulnerable to sabotage, could also be directed to the civilian hence, security breaches have gone beyond stolen credit card number to potentially targeting the electric power grid, stock market and public places. Cyber warfare could be perpetrated through distributed of denial of service (DDOS) which is an attempt to make a machine or network resources unavailable to intended user. Perpetrators of DDOS attack target sites or services hosted on high profile web servers such as banks, credit cards payment gateways, and even root name server. DDOS attack may be perpetrated as physical attack such as cutting undersea communication cables in order to severely cripple some country’s information warfare ability.

2.1 **Theoretical Framework**

The following theories underlie this study:
Investigative principle and cybercrime investigation theory

Van Rooyen (2012) postulates that crime investigation reflects the process of tracking down, identifying, collecting and preserving the facts that will be used to solve a case and then prepare them as evidence in court. Westhuizen and Perez (2009) define criminal investigation as a systematic search for the truth, with the primary purpose of finding a positive solution to the resolve crime with the help of objective and subjective clues. Van Heerden (2011) describes objective clues as the factual proof and objective explanation for indirect or circumstantial evidence and subjective clues as the evidence offered by people (victims, complainants, eye witness and culprits) who are directly or indirectly involved in the crime. Pepper (2011) stated that in Locard principle, a clue is usually left behind when two or more objects or people come into contact with each other. This is referred to as a reciprocal transfer of traces. For instances, when a suspect touches a glass window he or she leaves traces on it in the form of finger prints. Reciprocal traces from the windowpane, such as dust or glass splinters are transferred to the suspect’s hand. Locard principle means that an investigator can confidently assume that there will always be clues at the scene of the crime. If the investigator cannot find any clues, it is not because there are none but rather, because the techniques required in identifying the clues are not known by the investigator. In the context of its applicability to cybercrime, Ezeji (2014) notes that, cybercrimes could be committed via any cyber system in the world, and if investigators are not knowledgeable and skillful to detect and investigate cyber-crimes, may be very difficult to apprehend the offenders, due to factor such as jurisdiction. Tracks or clues at the crime scene can be useful to reconstruct, or recreate, the crime scene and to individualize or positively link the perpetrators to the crime.

Furthermore, McEwan (2010) states that during cybercrime investigation, thorough search must be initiated which includes extensive search of each cyber system/computer, terminals or servers and all computer related hardware, software and networks. Cybercrime investigators or cyber forensics should take precaution when applying investigative principles. McEwan (2010) notes that a comprehensive search should not be restricted to locating and seizing physical objects. Evidence may be in the form of corroborative and peripheral evidence which would assist in creating or supporting the suspect’s personality, frame of mind or state of mind. However, in security or secrecy investigation paradigm, when suspected items are absence, investigators are expected to find, look for what is there and what is not there. Kopelev (2010) maintains that when investigating crimes committed via network and telecommunication devices, the investigator should have in mind that criminals may launch an attack for various purposes and reasons such as trading and sharing information e.g. documents, photographs, movies, sound files, texts and graphic files, and software programs and investigators must be guided by investigative principles.

Explanation of crime and cybercrime prevention theory

The search for causes of crime led to the development of different theories to explain crime, which are divided into individual (centered) and environment (milieu/sociological) theories. The individual centered theories assert that crime is as the result of faults within the individual,
which are mostly attributed to biological and psychological irregularities that the individual cannot control. Milieu centered theories on the other hand, focuses on the social aspect of human behaviour, which includes organization culture and group behaviour, as well as the interaction between individuals and groups (Maguire and Radosh, 2011). Furthermore, Barlow (2012) explains, there are many other different theories that attempt to explain criminal behaviours apart from the ideological, conservative, liberal and ranched perspective. In addition, macro and micro theories focus on the wider socio-cultural context in which people operate, especially in a big social pattern such as social change, or the social, economic and political organization of the society (Barlow, 2012). Macro and micro theories are concerned with individuals’ activities, especially the way in which people interact with others and with the groups in which they belong. Criminal behaviour is acquired or learnt, the differential association theory is thus a micro theory, as learning is a process. Barlow further observes that the general theory explains a wide spectrum of criminal behaviours and different forms of crimes (Barlow, 2012).

In its applicability to cyber-crime, most people are exposed to cyber-attack because of their eagerness to learn what others are doing on the internet and not understanding the ugly side of online activities thus, exposing them to be vulnerable to cyber-attacks (Ezeji, 2014). Brown (2012) asserts that in general theory lack of self-control is the cause of crime, people who lack self-control will repeatedly behave in a way that will cause problem for themselves and for others, not only criminal behaviour but other negative behaviours such as excessive drinking and ineffective child rearing. When children are not monitored and punished for bad behaviours, the behavioral pattern is affected due to the lack of self-control exhibited by the parents or guardian. In this note, Ezeji (2014) pointed out that people who lack self-control will always commit and repeat criminal acts, due to inability to control themselves, the reason most cyber criminals get involved in cybercrime is due to greediness, lack of self-control and financial gain, lack of opportunities and employment. For example, cyber criminals who perpetrate cybercrime such as identity theft, credit card fraud and phishing are regarded as greedy because they are not contented with what they have and thereby engage in the crime to acquire what does not belong to them.

2.2 Empirical Review

The role of the community in cybercrime prevention

The community based crime prevention assumes that by creating the perception among potential offenders, the risk of being caught is high in a specific neighbourhood. According to Graham and Bennett (2013), there is no consensus on what this model really entails, as it also contains elements of social prevention and reducing crime opportunities. The above authors affirmed that social, economic and demographic circumstances promote crime, as well as collective cooperation, community development and individual attempts by households all form part of community based crime prevention. Community based crime prevention programs
can succeed only if the community is involved with a sense of neighborliness and various organizations, people cooperate collectively (Graham & Bennett, 2013)

Ezeji (2020) notes that in respect of cyber-crime, members of the community should act proactively in reporting it to the authorities, the public may have information about suspects in their locality and the kind of businesses or activities members of their community are engaged in. If members of the public notice someone who has no means of livelihood or who receives certain amount as salary but is seen living above, his or her income should be reported to the authorities so that the source of wealth can be investigated and established. Naude (2005) asserts that, if members of a community become aware of cyber-crimes or as the relationship with the police or perception of the criminal justice system improves, the public report cybercrime, more effective criminal justice system will result hence more offenders would be convicted and sentenced. At this juncture, it is necessary to state that the police and other counterparts of the criminal justice system should ensure that the public trusts the police who in turn should maintain a close relationship with members of the community to ensure they feel free to report cyber-related crime and not be made scape goats after reporting a crime. It is noteworthy to note that the police should protect lives not live destroyers (Graham & Bennett, 2013).

Ezeji (2020) pointed out expected roles by the community to enhance an effective cyber-crime prevention. The roles include; monitoring cybercrime suspects that make use of wireless cyber networks, monitor the activities of users at internet cafés who make use of the facilities in carrying out identity theft, credit cards fraud and other online criminal activities. The society should keep an eye on the youth and monitor their activities on the internet, to avoid cyber-attacks and victimisation of members of the society. Graham and Bennett (2013) note that the following roles are expected to be played by the community in cyber-crime prevention; reporting of cyber-crime to the appropriate authority, liaising with members of the community, supporting the criminal justice system officials, sponsoring of cyber-crime prevention programs and participating in creation crime awareness programmes.

The role of forensic investigators in cybercrime investigation

During cyber-crime investigation, the investigator is required to safe keep and identify physical evidence retrieved from computer and cyber system, which was used in committing the crime. If the investigator fails to safe keep the computer or cyber system used in committing the crime, the evidence would be tampered with and may not be admissible in court. Continuity of possession begins as soon as physical evidence has been found at the scene and persists until the article is produced as evidence or proof in the court, the handling, and handing over of samples and their return after scientific analysis (Van Heerden, 2011).

The Nigeria Police Act provides that the investigators gather evidence during investigation, and also collect necessary and available information regarding the crime. An investigator’s duties include; communicating with witnesses and prosecutors processing the crime scene and
assisting in preparing cases for court proceedings, identifying and tracing witnesses, identifying and tracing suspects, individualization of crime, taking statements to prove the case, preparing dockets for court, arresting and charging suspects and assisting in the prosecution (Ezeji, 2020).

The followings are the objectives of an investigation; identification of the crime and perpetrators, collecting and preserving evidence in a systematic and legal manner, individualization of crime, arresting criminals, recovering stolen properties, involvement in the prosecution process by preparing witnesses for trial and assisting the prosecutor, also solving crime by establishing who, what, when, why, where and how the crime was committed, and also ensuring that all statements are obtained and all exhibits are properly secured (Van Heerden, 2011).

3.0 Methodology
Qualitative methodology was adopted in this study. Interview technique was used to obtain information from twenty-five (25) carefully selected participants from Nigeria police crime prevention and investigative unit, cyber forensics experts, officials from EFCC, senior lecturers of criminology and security studies, judges and prosecutors. The above participants were selected due to their vast knowledge on the topic under study. Qualitative analysis was used for data analysis and interpretations.

4.0 Findings and Discussions of Results
Cybercrimes prevalence in Nigeria
Respondent (R21) reports that Nigeria is ranked third in global internet crimes behind the UK and U.S. A. Respondents (R16) reports, that cybercrime is rated as the fifth top rated crime and security risk in Nigeria in 2020, behind terrorism, cybercrime has become a norm across public and private sectors and cyber-attacks and victimization continued to grow till 2021 and 2022. The report has it that, cyber-attacks are expected to double by 2025 and will cost companies globally an estimated $10.5 trillion lost annually by 2025. Cybercrime related transactions represent the greatest transfer of economic wealth in history, and has affected all businesses, especially, small to medium sized businesses, that are frequently targeted.

80% of the respondents agreed that, the number of internet users in Nigeria is about 91.6 million, that cyber fraud cases traced to Nigerians have increased drastically. They believed that about N127 billion was estimated from loss accrued from cybercrime in Nigeria between 2015 to 2016, the commercial banks lost about N237 billion in 2017. In 2018, over 17,600 bank customers recorded losses of about N1.9 billion to cyber fraud, and the total financial loss was about N288 billion. In 2019 Nigeria banks lost, about N552 million and in 2020, Nigeria banks lost, about N3.5 billion between July and September 2020 and the lost has increased between 2021 and 2022.

Respondents (R18) spotlighted that cyber-attacks have disrupted normal operations of various industries, organizations, parastatals, caused damage to critical IT assets and infrastructure that
cannot be easily replaced. According to respondents (R11), ‘Small and medium scale business have suffered different categories of cyber-attacks which includes; phishing, social engineering, compromised stolen devices, credential theft. Most of the organizations are not capable of defending their infrastructures from cyber-attacks, as a result of lack of adequate and sufficient security measures, their processes are ineffective to mitigate attacks, their infrastructures are exposed to frequency targeted attacks, hence unable to protect their cyber systems and infrastructures, due to lack of capacity in protecting their infrastructures’.

70% of respondents pointed out various attacks meted at some of the notable corporations by cybercriminals. They believed that, cybercriminals have targeted and launched attacks on product concepts, intellectual property, marketing strategies, client and employee databases, contract deals and client pitches. Also, cybercriminals have attacked some of the higher institutions holding information on enrollment data, academic research, financial records, and personally identifiable information like names, addresses, and billing info and cybercriminals can attack any of the information at their disposal.

From the study 75% of the respondents converged that, cyber criminals make use of malicious software such as virus, a software that attach itself to a normal file and then reproduces itself to cause damage to a computer system or network thereby destroying sensitive government and cooperate infrastructures. Cyber criminals use of worms, software that look for vulnerabilities in a computer or internet network in order to reproduce itself to attack businesses and individuals. Cyber criminals launch attacks on victims by using Trojan Horse, a program that appears to be normal but in reality is used to introduce a malicious program to a computer system or networks. Backdoors are used by cyber criminals, a program used by cyber criminals to gain access to a computer system or network at a later date or time giving them access to launch an attack on the victim.

Respondent (R15) asserts that; cyber espionage involves the utilization of computers to aid in the act of stealing sensitive information; these activities are mostly sponsored by a state or other cooperation attempting to damage a rival company’.

65% respondent agreed that, Nigerians have witnessed E-commerce fraud. They believed that, the cyber criminals make use of internet and computer networks to defraud victims by posting fraudulent items that do not exist, deceiving and defrauding victims. According to the above respondents, phishing is one of the common cyber invasion targeting most sectors in Nigeria. They pointed out that, cyber criminals preformed phishing attack on different organizations including the public and private sectors. In this respect, respondent (R1) pointed out that; ‘Inadequate control and abuse of system privilege is another cyber risks faced by Nigeria government ministries, parastatals and financial sectors’. The above respondent buttressed that, abuse of privilege access by external service providers, third parties and contractors are factors that enhance attacks on organizations.
75% of the respondents agreed that, malicious software (malware) attack is prevalent in Nigeria. They believed that, cyber criminals make use of the software in creating support systems to conduct specific cybercrimes such as denial of service. They agreed that, the government and organizations dealing with procurement are hot targets for business information, theft by contractors and third parties who are often commissioned. According to respondent (R5), ‘‘Malware attack is prevalent in Nigeria and have been detected where incidences of information theft or espionage take place.’’ Respondents (R13) is of the opinion that, inadequate protection and control of devices in the network has led to increase in malware attacks against individuals and organisations. Consequently, respondent (R5) concurred with the above respondent that, inadequate application of software security gives room for attack, while ineffective policies within organization and governmental department allows for accidental or intentional breaches from insiders. Respondent (R9) views that, lack of skilled experts hinder effective management of applications related to cyber security, while inadequate protection from attacks due to internal and external influence (personnel) creates vulnerability within public/private organizations and governmental departments.

75% of the respondents spotlighted the existence of cybercrime organized group(s), involved in causing damages to individuals, organizations and government offices in the form of extortion, blackmail, spreading of viruses, DDOS, malware and ransomware attacks directed at their targets. They also, converged that viruses and malicious software can be transported by cyber criminals; through a variety of mechanism like emails. Respondent (R4) opines that, identity theft is prominent, in this respect, cyber criminals use email or web pages to convince victims to reveal their personal or financial information and the stolen information is used to further other crimes. 80% of the respondents concurred that, cybercriminals use web hacking techniques to deface government or corporate websites. The act is conducted to embarrass or test the security capacity of an organisation or government. Cyber hackers use of computers and the internet to conduct resistance against a government or cooperation. Hacktivists conduct DDOS attacks, intrusion, and web defacing to make a point in their political views.

**Seriousness of cybercrime**

According to 75% of the respondents, most individuals and organisations have been attacked by cyber criminals. They believed that cybercriminals make use of the following techniques to orchestrate attacks on victims; malware attacks, computer viruses, ransomware, worms, trojan horse, root kits, key loggers, dialers, spyware, adware, rogue security software and other malicious programs. In this respect, Schultz (2013) notes that, malware is a short name for malicious software used or programmed by attackers to disrupt computer operation, gather sensitive information or gain access to private computer systems. It appears in the form of codes, scripts, active, content, and other software. These techniques have been used by cyber criminals. In the opinion of respondents (R7) phishing internet scam technique has been widely used to obtain credit card numbers, account numbers, passwords and other confidential information, often is the first stage of identity theft. According to the above respondent,
different organizations have suffered lost as a result of the attacks on them by cyber criminals that stole vital information from the organization.

According to respondent (R8), many companies, industries, organizations and individuals have been victimized by hackers in Nigeria. Moreover, in the hackers’ underworld, Peter Krapp (2011) reveals the difference between hackers that are cyber criminals and hackers that are experts. Cyber criminals are called black hats and cyber security experts are called white hats. White hat hackers claim that they deserve the title hackers and that only black hats should be called crackers.

80% of the respondents revealed, the techniques used by cyber criminals to orchestrate DDOS attack. They believed that, DDOS perpetrator’s aim is to prevent legitimate users of a service from using that service; the attackers could either adopt methods such as crashing or flooding of services. The perpetrators of DOS attack target sites or service hosted on high profile websites/servers, such as banks, credit card payment gateways, and even root name servers.

Respondent (R7) pointed out that, ransomware is a malware that infects computers (and mobile devices) and restricts their access to files, often threatening permanent data destruction unless a ransom is paid, this attack has reached to epidemic proportions globally and is the “go-to get method of attack” for cybercriminals. The above respondent believed that many organizations in Nigeria have been victimized using DDOS technique.’’

70%m of the respondent agreed with Jackson (2012) who revealed that before the advent of internet or cyber systems, video shops have a small sex section. A video shop is where videos are obtained and adults take out the video to watch at home. Sex magazines, books and sex cartoon were made available, but cyber systems, computer, cell phone, tablets and portable networks have changed this scenario. Minors who are not monitored have access to internet and social media networks where they engage in the viewing of pornographic materials. They agreed that, internet has made it possible for the adult, youth and minors to have access to pornography without any personal contact with the role players. Female internet /online dating addicts have been raped, murdered, and kidnapped by offenders when they arrange to meet online lovers face to face and the meeting turns ugly.

75% of the respondents agreed that cybercrime has variety of implications in Nigeria in relation to insurance cost, the direct cost against the victims and resource allocation for apprehension and prosecution of offenders. They revealed that, a perpetrator can steal the life savings of a victim by just pressing few buttons. Many businesses have folded up as the result of cybercrime attacks and some have bankrupted unable to pay staff salaries, adding to the pains and loss of jobs and unemployment rate in Nigeria. Respondent (R4) opines that cyber criminals have targeted and attacked organizations such as banking industries, insurance, government ministries and departments, private/public companies, e-commerce and social media sites. Cyber criminals have made their ways into the private information of customers who possess
bank credit cards and steal money to buy commodities with the stolen credit cards via the internet, and then ship the goods from one country to the other.

75% of the respondents agreed that cyber-attacks could cripple any organization, and an organization can lose its competitive advantage and suffer huge losses when a hacker steals its confidential information and sells it to the business rivals. After cyber-attacks against critical infrastructure of any organization, will require fixing the problem. Respondent (R9), stated that ‘the time spent by IT personnel to rectify harmful incidents caused by computer criminals could have been used to earn profit for the organization.’ The above respondent pointed out increase in the operating cost of businesses due to huge expenses incurred on purchase of security software applications to reduce the rate of cyber-attacks. Respondent (R4) confirms that, cybercrime reduces the productivity of an organization, and suggests that, businesses take measures to prevent its infrastructures from cyber-attacks and improve the security of their networks. The involvement of the youths in cybercrime is alarming. in this vein, 70% respondents lamented at the level involvement of the youth in cybercrimes. They believed that the high rate of young Nigerians involving in cybercrime is an indication that, the society has degenerated into a comatose state.

Consequences of cybercrime in Nigeria

Respondents (R7) recounts the losses incurred by the government, cooperate organizations, individuals, businesses, private/ public organizations who have lost so much in monetary value and assets, the losses have adverse effects on the nation’s economy to the extent that it discourages foreign investors from coming to invest in Nigeria due to fear of losing their resources/funds, insecurity and fraudulent activities of Nigerians.

Respondents (R17) asserted that, some industries or organizations are more vulnerable to cyber-attacks than others, because of the nature of their business. Companies that hold sensitive data or personally identifiable information are the most targeted by hackers. Many businesses and organizations have witnessed cyber-attacks such as loss of data, business disruption, revenue losses from system downtime, notification costs, or even damage to a brand’s reputation. The most vulnerable industries or organizations that are prone to cyber-attacks are the banks and other financial institutions, who makes use products like credit card information, bank account information, and personal customer or client data. Also, healthcare institutions that keep repositories for health records, clinical research data, and patient records such as social security numbers, billing information, and insurance claims.

According to respondent (25), cybercrime costs include damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm. 65% of the respondents agreed that, the financial costs to economies and businesses from cyber-attacks include the loss of intellectual property, financial fraud, and damage to reputation,
lower productivity, and third party liability. They pointed out that the negative effect of cybercrime is that, it tarnishes the image Nigeria as a nation. Once a country is labeled as a harbor for cybercrime activities, potential investors are cautious of investing in such countries. This has some dire implications for the nation’s macroeconomic stability.

70% of the respondents agreed that cybercrime cost can be analyzed as direct, indirect losses and defence cost. They pointed out that the direct losses are the monetary losses or other suffering felt by the victims as the consequence of cybercrime. Direct loss comprises of money withdrawn from victim’s account, during the time the incident occurred, the time and efforts to reset account, credentials (for both bank and consumers), distress suffered by victims. Secondary cost involves overdrawn accounts, deferred purchases, not having access to money when needed and loss of attention and bandwidth caused by spam messages, are some of the direct losses identified as an aftermath of the crime.

Respondent (R12) states, ‘’The damage cost estimation of cybercrime is based on historical cybercrime figures including recent year-over-year growth, a dramatic increase in hostile nation-state sponsored and organized crime gang hacking activities, and a cyberattack surface which will be an order of magnitude greater in 2025 than it is today.’’

Respondent (R23) reports that indirect losses comprise of loss of trust in online banking, leading to reduced revenues from electronic transaction fees and higher cost of maintaining branch staff and cheque clearing facilities, misused business opportunity for banks to communicate with their customers by emails, reduced uptake by citizens of electronic services as a result of lack of trust in online transaction and effort to clean up PCs infected with malware /viruses.

Respondent (R5), reports, ‘’Cybercrime is no doubt providing a dent on Nigeria’s image which remains a crucial source of national embarrassment for the country. The fear of cybercrime has made several persons to avoid the use of ICT. The perceived loss of confidence may also affect the country’s developmental progress; as foreign investments find it difficult to flow into the economy.’’

65% of the respondents pointed out that the defence costs are the monetary equivalent of prevention efforts which include direct defence costs, i.e. the cost of development, deployment and maintenance of prevention measures. They believed that, defence cost includes: security hardware and software products such as firewalls, antivirus, and browser extension to protect users, security services provided to individuals such as training and awareness measures, security services provided to industry such as website ‘take down services’, fraud detections, tracking and recuperation efforts, law enforcement and the inconvenience of missing an important message falsely classified as spam.
Role of the government and criminal justice system in combating cybercrime

The government through legislation has stepped up to address cybercrime in Nigeria. The study revealed that the Cybercrimes Prohibition ACT 2015 “provides an effective, unified and comprehensive legal, regulatory and institutional Framework for the prohibition, prevention, detection, prosecution and punishment of Cybercrimes in Nigeria”. The Act needs to be constantly reviewed to align with dynamic nature of the cyber environment to accommodate more crimes and address more cyber-related issues that are unique. Also, the Nigeria Data Protection Regulation 2019 is also another regulation that is targeted at protecting both data in motion and at rest. Moreover, there are general laws that deal with financial crimes such as the Nigeria criminal code, Economic and Financial Crimes Commission (EFCC) Act 2004, and the Advance Fee Fraud and other Related Offences Act, 2006.

Respondent (R5) revealed other notable cybercrime control initiatives emanated from Nigerian government, which includes the setting up of a National Cybercrime Working Group (NCWG) with stakeholders drawn from the law enforcement agencies, the financial sector and ICT professionals, and a pilot project of a Computer Emergency Response Team (CERT) Centre by NCWG and NITDA. 65% of the respondents agreed that partnership and cooperation should exist among the criminal justice system relating to apprehension of cybercrime suspects, gathering evidence, investigating cybercrime, prosecution and sentencing should be swift. They believed that the criminal justice need to develop strategies and plans to tackle cybercrime such as campaign strategies whereby the public goes into partnership agreement with the Government in creating awareness of cybercrime. In this regard, respondent (R2), reveals that lack of implementation of plans and strategies hindered the criminal justice system from addressing cybercrimes effectively. Respondent (5) adds that, most of the police officers are not skillful, do not posse adequate knowledge of how to prevent or investigate cybercrime. According to respondent (R21), only few of the investigators possess the necessary skills required to investigate cybercrime, the police officers at local stations lack the experience in handling cyber related crimes. 55% agreed that criminal justice officials lacked the adequate skills and knowledge to prevent and investigate and prosecute cybercrimes. They agreed that cyber-crime requires well trained and specialized officials and need to be taken very seriously.

5.0 Conclusion

In conclusion, the global cybercrime damage costs are; $190.00 per second, $11.4 million per minute, $684.9 million per hour. $16.billion a day, 115.4 billion a week $500 billion a month and 6 trillion a year. The indirect losses accrued from cybercrime includes; monetary equivalent of the losses and opportunity cost imposed on society. Cyber criminals orchestrate attacks against organizations’ using distribution of denial of service attack (DDOS) technique or distribution of denial of service attack (DOS) by slowing down machine or network resource or making services unavailable to its intended users. Nigeria is ranked 169 out of 199 countries globally, as a non-conducive destination for carrying out business. Therefore, prevention, investigation and prosecution of cybercrime should be prioritized in Nigeria.
5.1 Recommendations
Cyberspace is a challenging environment that is fast and continuously evolving. The challenge is for those charged with the responsibility for securing critical and national infrastructures, private and public organisations and individuals to be abreast of developments in the cyber world. The economic vitality and national security largely depend on a stable, safe and resilient cyberspace.

Cybercrime can take place regardless of borders, but legislations and jurisdictions are based on a country-specific framework. Therefore, it is suggested for continuous review of Cybercrimes Prohibition ACT 2015, to address the dynamism of cybercrime. The upgrade of the Nigeria Financial Intelligence Unit (NFIU) to a full-fledged Agency (NFIA) is also a great leap to strengthen the fight against cybercrime in the country. For legislation on cybercrime to be relatively effective and efficient, government needs to empower graduates through employment and the provision of intensive training for law enforcement agencies on ICT to enable them in tracking down cyber criminals.

Victimization and vulnerability of users increased due to lack of precaution taken by online, internet and mobile devices users. Precautionary measures need to be taken to secure internet connected mobile devices that are vulnerable to cyber criminals who are looking for an opportunity to steal money and cause damages. Provision should also be made to install mobile security software which protects users against malicious online threats and enables users to lock, locate and wipe devices remotely. Cyber security can help prevent crimes before they happen, but it requires a lot of awareness of tools that can be installed on devices to ensure that the wrong person doesn't have access into user’s system to commit crime. It is important that everyone becomes cyber-security conscious by ensuring that they don't click on the wrong links. Cyber-security awareness is very important. It enables everybody knows what they are not supposed to click on certain links, understand the need to use two-step verification on their WhatsApp and other social media platforms. The investigation of cybercrime requires the service of digital forensics experts that will investigate to find out who the perpetrators are apprehend and prosecute them. A national biometric database, which the government is in the process of developing and introducing, will help to ensure that cybercriminals are brought to justice.

There is need for effective and efficient initiatives directed at protecting the interest of Nigerians in the cyberspace. The government agencies such as the National Information for Technology Development Agency (NITDA), Nigerian Communication Commission (NCC), Economic and Financial Crimes Commission (EFCC), the Nigeria police force should synergize towards curbing the menace of cyber-crime in Nigeria.

To reduce cybercrimes in Nigeria, there is the need to create job opportunities for the unemployed youths as well as the need for government, law enforcement, intelligence and security agencies to understand the technology and individuals engaged in the criminal acts in
order to be able to curb their activities. As the social impact of cybercrimes is so serious, it is suggested that the various tiers of governments come up with different programmes aimed at re-orientating the youth towards positive thinking, moral and attitude change. The rising spate of cybercrime globally and its attendant negative consequences has continued to call for immediate actions and the need to institute an effective risk management system and enhancement of the capacity to carry out forensic investigation to tackle it. Also, collaborative efforts of governments, corporate entities and the citizenry could play a vital role in checking cybercrimes.

References
Ezeji, Chiji Longinus

books.


