ANTIDOTES TO THE MANY FACES OF CYBERCRIME

SUBMITTED BY:

CHIMA, OGBA R.: PG/19/0096

MSc. COMPUTER SCIENCE (ELONGATED)
IN PARTIAL FULFILLMENT OF THE COURSE:
RESEARCH SEMINARS (MASTERS) – GEDS870

LECTURER: PROF. AWODELE, O.
DECEMBER, 2021

IJASR 2022
VOLUME 5
ISSUE 1 JANUARY – FEBRUARY **ISSN: 2581-7876**

Abstract: Definition of cybercrime has defied globally acceptable definition. However, this paper will discuss the concept of cybercrime in line with what it is, what motivates people to take that course of action, it's forms, various ways it manifests and the various ways to mitigate against it to protect individuals, organization's reputation, ensure non-repudiation, business growth and continuity, while still enjoying the use of technology.

Keywords: Cybercrime, Cybersecurity, Malware, Hacking, Child exploitation, Zapping

BACKGROUND TO THE PROBLEM

The growthof computers and the internet has opened a wide dimension of possibilities for everyone world over to have access to the Internet from the comfort of their homes, offices, cyber cafes and so on. Nowadays, smart phones and other devices have made Internet access easier and faster. Not so long ago, computers were large, cumbersome devices utilised primarily by government, research and financial institutions. For the most part, computer related crimes was possible only for those who have access and cognate know-how. Today, the ubiquitous availability of the technology and its increasingly easy to use features has made iteasily accessible to both cybercriminalsand their victims (Clough, 2010).

The rapid growth of digital technology, and the converged telecommunications infrastructure (computing and communication technology), has completely changed the way we communicate and carry out business. Interestingly, while overwhelmingly positive, there has also been a murky side to these developments. Almost every step of advancement in technological growth has been followed by a corresponding opportunity to be exploited criminals (Clough, 2010). One major consequence of this unlimited access to the Internet has been a corresponding increase in the spate of cybercrimes. Different types of countless crimes are committed daily on the cyberspace across the world.Cybercrime is knows no boundaries, it is nondiscriminatory, andit's dramatically on the boundless increase. Countless dollars are beingsiphoned from innocent individuals and large corporateentities alike. Numerous numbers of people are recruited into this crime owing to little or no know-how requirements coupled with fantastic financial rewards.(Team CYMRU, ACM QUEUE 2016, p.5). Furthermore, Majid (2020, pp.3-4) expressed it thus:

> *Businesses blame threats to economic performance, stability, on vandalism, and cybercrime (e-fraud and piracy); while governments talk of cyberwarfare and cyberterror, especially in the wake of the September 11 attacks; parents fear for their children's online safety, as they are told of perverts and pedophiles stalking the Internet's "chat rooms" looking for victims; hardly a computer user exists who has not been subjected to attack by "viruses" and other forms of malicious software; democratic rights and freedoms advocates see a threat from the state itself, based on conviction that that the Internet provides an enabling environment for surveillance and control of citizens, an electronic web with which "Big Brother" can watch us all. The development of the Internet and related communication technologies thus appears to present an array of new challenges to individual and society.*

Therefore, in consideration of the foregoing, the cyberspace became hostile as new breakthroughs are being achieved in Information technology making it very difficult to carry out activities for online communities. Despite

the enhanced countermeasures that have been adopted in recent years, it has remained on the increase. Manifestations of cybercrime include the reason for economic losses, service disruptions, loss of critical data, intellectual property losses, threat to National security. Cybersecurity provides secure and safe cyberspace. To mitigate the above, effective and properly articulated cybersecurity policies and frameworks need to be developed and implemented for business growth and continuity.

The role cybercrime play in foreign relations is important and has increasingly become strategic. This has led to the formation of major international bodies. Various treaties and bilateral, regional and international agreements among jurisdictions of the world have been made (Kshetri, 2013). A major one is the Council of Europe Convention on Cybercrime. This was either ratified, accessed or signed by about 52 countries by September 2016. The above developments have triggered further formations in developing countries including the Commonwealth Model Law on Computer and Computer-related Crime (2002). The African Union followed with the Convention on Cyber Security and Personal Data Protection, adopted in June 2014. There are also initiatives at the European level.

Significant steps towards cybersecurity cooperation has also been taken by the Shanghai Cooperation Organization (SCO). This body has Kazakhstan, China, the Kyrgyz Republic, Russia, Tajikistan and Uzbekistan as its members. Furthermore, many countries have signed either multilateral and bilateral treaties and agreements to institutionalize cybersecurity relations. Instances abound. For example,China and Malaysia signed an MoU to combat trans-border crimes. The importance of regional and international cooperation was highlighted by the two countries with the engagement of who possess regional and global networks (Kshetri, 2019). Furthermore, laws are rapidly being enacted to control cybercrime. As much as one hundred and seventeen countries, eighty-twoof them developing and transition economies, had passed such laws, and additional twenty-six countries had drafts underway (UNCTAD, 2015).

Locally, Nigeria joined the league of the countries that have enacted laws to control cybercrime by enacting Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015 and the Nigeria Data Protection Regulation regulations.

According to a 2011 World Bank survey, out of the top ten countries in the world with a high level of cybercrime prevalence, four of these countries come from Africa (Cameroon, Ghana and South Africa and Nigeria, in no order of prevalence).Top five hotspots for cybercrime are, first, the Russian Federation, followed by China, Brazil, Nigeria and Viet Nam, according to another study (*Time*, 2014). Also, the 2010 Internet Crime Complaint Center Report ranked Nigeria third in the hierarchy of nations with the highest prevalence of cybercrime (IC3 Report, 2010). From this report, Nigeria is considered one of the major global centers of cybercrime.

Meaning of Cybercrime

Inconsistent definition of cybercrime has constituted a major hindrance to its study. This has also affected decision-making by the law enforcement agencies tackle the crime. Various definitions have come up in order to try to find a solution. For example, the Council of Europe (COE) Convention on Cybercrime, says that cyber-crime isall "action directed against the confidentiality, integrity, availability of computer systems, networks, data as well as the misuse of such systems, networks and data" (Council of Europe, 2001). The Federal Bureau of Investigations (FBI) defines cybercrime as spanning across a diverse scenario including;

- crimes against children;
- Plagiarism (intellectual properties and/or publications), phishing, intentional dissemination of malware to cyberterrorism.

To (Casey, 2004), cybercrime is considered to be any crime that are computers related and non-computer related. Cybercrime is considered by Thomas and Loader (2000, p.3) as those "computer-mediated activities which can be conducted through global telecommunications networks".

Cybercrimes are offences that can only be committed using a computer and related technology (McGuire, M. 2013). In general, cybercrimes are activities primarily carried out using computers. For example, the intent to hack into email account may yield unplanned datathat may be used to commit a fraud in future. To (McGuire and Dowling, 2013), offences 'against' computers and networks are what should be considered as cybercrime.

Forms of Cybercrime

Cybercrimes can be classified in several diverse ways. One, those crimes committed by violent orpotentially violent criminals, and two, nonviolent crimes. The violent types include Cyber terrorism; Assault by threat.

Cybercrimes include three main offending patterns (Wall, 2008). One patterncan be the integrity of the system (hacking). Second, the computer. Thirdly, the content of the computer itself can be the objectof cyberattack.

Details of the main forms of cybercrime are outlined below:
Malware:a malicious software that spreads from one computer device to another and affects computer operations (Kirwan and Power, 2012). It can lead to the deleting of files or causing system 'crashes'. It can also be used to steal personal data. Different forms of it exist, namely:

• *Viruses* can cause mild to severe effects in terms of damaging or deleting software or files, thereby making the hardware useless. Viruses are self-replicating programs, which can spread within a computer and across computers. Hosts are important for the propagation of the spread like a file or diskin a computer to act as a 'carrier'. Viruses can only spread when there is the human action to execute the infected file (Moir, 2008).

• *Worms* are programs that can also self-replicate, but they may not require a human intervention to spread, within a computer or across computers. Worms can be more harmful than virusesso much that they can destroy networks (Beal, 2011). Worms can be vehicles for spreading Trojans.

• *Trojans* are a form of malware that that hides its real content thereby fooling the user to think that it's not harmful. It tries to initially to hide its true intentions, but it is actually a vehicle that delivers a variety of destruction to computer data.

• *Spyware* is a harmful software that can install itself on the computer. After installation, it then carries out covert spy operations such learning user's online behavior. Thereafter it starts sending such personal information like user name, address, browsing habits, interests and the downloads the user carries out. This information so gathered may then be automatically transmitted to criminal users. Spyware can sometimes wrap itself with a payload such as *adware*. Examples abound but one of them is ofspyware is *key-logging,* which captures (logs) keys struck on a computer.Through this action, sensitivedata are collected without the user knowing. One of the most dangerous forms of malware is considered to be spyware as its objective is to secretly invade user's privacy (Furnell, S. 2010).

Hacking

Hacking is a form of trespass. It takes advantage of weaknesses and vulnerabilities in a computer to steal sensitive it's data and pass them on to the wrong people.
Hacking can be used to:

- collect sensitive personal data or information for criminal intentions;
- change the visual appearance of websites or web pages; or
- carry out DoS or DDoS attacks.

DoS and DDoS is a form of cyberattack that denies intended users temporary or indefinite access a computer of network resources. Forexample, when a user clicks a malicious link, which then overloads servers causing them to freeze or crash or experience delayed response.

Spam

Spam is irrelevant or unsolicited messages sent over the internet, typically in bulk to large number of users and is often related to products advertising (e.g. pharmaceutical products) or pornography.)

Botnets

Botnets are clusters of computers infected by malicious software that allows hackers/malicious actors to control them. Cyber criminals usedthem to send out spams, phishing messages or other malicious cyber traffic automatically andrepeatedly to specified targets (Alhomoud *et. al* 2013).

Man in the Middle Attacks (MITM)

It is a method in which an attacker can make pretense to be the actual host and can deceive the client he is talking to the actual host (Varshney,ICICC 2020). Various forms of MITM include HPPTS Spoofing, IP Spoofing, DNS Spoofing, Wi-Fi eavesdropping, Stealing browser cookies, SSL hijacking and Email hijacking.

Other forms of cybercrime include:

Child exploitation: the sharing of images/videos of children being physicallyand sexually abused and thereafter using it as a bait on other children online in order to win asexual relationship in the 'real world'. This is also known as 'grooming' (Martellozzo, E., 2010).Child exploitation did not originate byInternet age at all. However, the Internet has become the new playgroundfor consumers of child pornography and a market place for those who provide it.

Harassment: Internet harassment, otherwise called cyberbullying refers to the use of the Internetto harass, bully or embarrass another person (Black andKenneth, 2010).

Digital Piracy: One of the forms of cybercrimes.Gunter, W. (2010) defined digital piracy as illegal act of copying digitalcontents without explicit permission from the copyright holder/online using computer technology.

Intentional Damage: Acompany'scommunications networks can be harmedthrough *zapping*, the process of damaging or erasing data and information, causingproblems for allusers of the data and information (Wienclaw, 2008).

Other forms cybercrimes occur in the banking and finance industry which include Credit or Debit card OTP frauds and also data theft. It is quite common to receive calls from unknown phone numbers from miscreants pretending to be bank official or insurance company official, mobile operator and so on trying to steal money using OTP and other valuable information.

Another rising cybercrime is fake news on social media. The arrests being made may not be high enough due to certain ambiguities in the cybercrime laws regarding the level of peculiarities of the offence and the difficulty in finding the real offenders.

Motivations for Cybercrime

What motivates cybercrimes may not be far-fetched afterall. This, for the most part, largely focused around personal profit orfinancial gain. Motivations for the crime can be inferred by largely examiningthe tools used. Some research outcomes suggestthat there are more motivations, e.g. satisfying intellectualcuriosity. Other unorthodox motivations include general maliciousness, boredom,or even simply poweramongst online communities(Kirwan, 2012).

Variations in cybercrimes exist, depending on the extent to which victims are targeted. One aspect could be to indiscriminately infect large number of victims with viruses. On the other hand, it refers to highly planned, sophisticated and prolonged attacks known as Advanced persistent threats (APTs)which aim to achieve aspecific goal, for example, destroying infrastructure (Symantec, 2012).

PROBLEM STATEMENT

Cybercrime has continued to be a recurring decimal despite various countermeasures deployed to mitigate it by various communities which include companies, universities and individuals. Statistics abound pointing to the advances it has left in its trace. Recent statistics show that about 3twenty-five million records were compromised or exposed every day in the first six months of 2018 and a projected USD6tn cybercrime cost in 2021 (https://www.simplilearn.com/free-cybercrime-course-for-beginners-skillup?referrer=search&tag=cybercrime).

As we can see from the above discussion, we can understand the following manifestations of cybercrime:

i. economic losses
ii. service disruptions
iii. loss of critical data
iv. intellectual property losses
v. threat to National security

So, to respond to the above manifestations, I would review the forms and motivations of cybercrime and identify the various ways to mitigate against them to protect organizational reputation, ensure non-repudiation, business growth and continuity.

OBJECTIVES OF RESEARCH

The objective of the study is to find the countermeasures to the many manifestations of cybercrime in our society. It will make a foray into the meaning, forms, motivation and then provide the antidotes to the menace.

SCOPE AND LIMITATION OF STUDY

This study will focus its attention on meaning and forms of cybercrime, what motivates people to go into this crime and finally provide options that will be applicable to mitigate its occurrence.

LITERATURE REVIEW

Annamalai Lakshmanan (2019) in one of his research paper investigates the list of various cyber threats that happened around the world. So, his paper describes the list of cyber threats that happened around the world till date and its prevention mechanisms. He described the prevention techniques for cybercrimes that happened till now and also in the research he showed the cyber threat analysis and the cyber threat prognosis in the upcoming years. He found that the cybercrime activities will be increasing in the upcoming days and will be difficult to stop. He came up with the approach that data is important nowadays because it can be used to earn a huge amount of money and so there is a need to design a powerful system which can not only stop the crimes but also protect the customer's data. This data should be given higher priority and should be place with high privacy and full confidentiality by the systems and by using powerful firewall.

Sreehari et. al (2018) research paper focuses on the awareness level of cybercrime among different college and institution students of Kochi. It was found that there is a need to find out the various precautions by the users to fight against and prevent cyber-crime. They came up with so many findings about cybercrime like most users are just aware about cybercrime. Their study shows that the ratio of awareness among the respondents regarding cyber-crime is high for hacking when compared to other types. It has been figured out in their study that there lies a significant difference between the users who spent time on Internet and their knowledge about their cybercrimes.

Animesh S. et. al (2017) in their research paper have discussed Cybercrime and cyber law in broad sphere enclosing many subtopics like access to and utilization of the Internet, cybersecurity, online privacy, freedom of expressions. The main focus of their work highlights how the cybercrime spreads among the common people and the less knowledge about this cause among the people. Their research shows various reasons about the cybercrimes and the safety measures one can take.They mentioned that if anyone descends in the catch of cyberattack, one can register the case in one's law enforcement agencies.

Sukanya, K.P. et. al (April 2017) research paper well defines on the awareness of cybercrime between the youth of Malappuram district. Still they are unknowledgeable about it. Basic principles or morals and the proper usages on IT approaches must be initiate in schools. Besides, the media must provide proper details regarding cybercrime. Regarding the security measures for combating cybercrime, youth have an idea which is one of the findings of their research.

Kumar, P. (2016) published a paper which examines the growth of cybercrimes in India and assess and evaluates the measures taken by the government of India to combat the cybercrimes. The study found out the various types of

offenses registered under the IT Act, between the years 2008 to 2013. Basic ethics and no significant arrests made as compared to the number of cases registered regarding cybercrime.

Hemraj et. al (January 2012) provided the understanding of cybercrimes and their impacts on society and it's the future trends of cybercrimes. They categorized cybercrimes e.g. Data Crime, Network Crime, Access Crime. They also discussed the impact of cybercrimes as economic, market value, consumer trust, National Security and future trends. In their conclusion, they stated that that the way to overcome these crimes can broadly fall into three categories: Cyber Laws (referred as Cyber laws), Education and Policy making. However, at the time of their research, cloud computing and virtual infrastructure provisioning have not become pervasive and could only suggest their growth but could not offer ways to mitigate crimes against them.

(Ajayi, E. F. G., 2016) states that there exist relevant laws across different jurisdictions dealing with cybercrimes, but the challenge has remained the enforcement of the said laws. Furthermore, the following continues to hamper efforts to enforce the laws:

- the absence of a global general agreement on the meaning of cybercrime;
- the crisis of a global general agreement on the legal definition of cybercrime;
- the lack of uniformity of laws across boarders;
- the absence of extradition treaties and mutual legal assistance between jurisdictions.

The above gaps are strongly militating against the applicability of cybercrime laws.

Sleiman M. B. (22 April 2021) researched on the topic Covid-19: a catalyst for cybercrime? and observed that cybercriminals were very active and easily adapt to the new circumstances and took advantage of it. The main reason for this pandemic of cybercrimes was that the phishing and malware methods, proved to be perfectly effective during the global pandemic situation that is as novel as it is unsettling for the global population. During this period, more people spent more time in the online space thereby increasing the number of potential victims.
The researchers' reliance on the administration of criminal legal code alone as antidote is faulty especially since cybercriminals are notoriously hard to track as they are smart in deploying various tools to cover their routes. Moreover, most researchers believe that even within a single jurisdiction, laws have not been effective to serve as antidotes to the crime.

Varshneya et. al (2020) found out that cybercrimes are becoming an increasingphenomenon. With the increase in use of the internet in web-applications such as e-commerce, net banking, etc. cybercrimes come along. There is no absolute solution for cybercrime. With the advent of new technology malicious users find out new flaws in the algorithm being used. Hence, there is a need to protect our online assets from such exploits, which can be achieved by taking counter measures against it. These counter measures are known as cyber security. Now the most important aspect of protecting our data is to protect it from outer sources and at the same time make it available for ourselves through the use of encryption technology.

They focused on the awareness level of cybercrime among different college and institution students of Kochi and relied so much on technology as countermeasures against the incidences of cybercrime. Such technology interventions include encryption, authentication, router security, elliptical cryptography curve, triple data encryption standard, Firewall, advanced encryption standard, data encryption standard and end-to-end encryption, and awareness.
The researchers' reliance on technology and awareness without any stipulation on the administration of criminal legal code as antidote is faulty. If the legal aspect will be gotten right then, convictions and punishments would convey the right messages to those who escaped the technology tightening of the network.

Kagita et. al (12 Sep 2020) observed that that Internet of Things (IoT) devices are rapidly gaining universal acceptance. The success of IoT cannot be trivialised today. Attacks on IoT devices and facilities are on the rise too. Since cyberattacks have become a part of IoT deployments and thereby affecting the life and society of users, therefore, serious steps must be taken to protect cyberspace. Cybercrimes causes havoc to government's infrastructure and global businesses in innumerable ways. Estimates have put the cost of cybercrime at 6 trillion dollars annually. Australia alone is estimated to lose 328 Million Dollar annuallyin consideration of cyberattacks. All steps taken to slow down these attacks have not yielded expected outcomes properly. Therefore, secure IoT is top

priority now. Understanding of patterns of attacks and threats in IoT structure should be a concern for study groups. Weak cyber securities could be attributed to be the reason for the rising cyber-attacks. Cybercriminals use keep using new technologies and tricks to attack which make mitigation efforts less effective.

The researchers' call for multinational treaties differed from the identified need for a global body with one law that offenders will be tried on and face the consequences of their crime. Multinational treaties could be slowed down by legal bottle-necks and finally weakened.

METHODOLOGY

This paper explains the meaning of cybercrime, forms, motivation for cybercrime and finally provides some recommendations aimed at mitigating the crime.

I will rely on secondary information gleaned from previous research work already carried out from online sources in order to attempt to provide answer to the problem of cybercrime in our society.

SIGNIFICANCE OF STUDY

Cyberspace is becoming more hostile as new technological grounds are discovered in telecommunication technology, making it **difficult** to conduct online activities for the government as well as for businesses. As a result, cybersecurity is employed to combat this hostility. Cybercrimes are on the increase even though robust measures are adopted by public and private institutions in recent years. Cybersecurity provides a secured and safer cyberspace, constituting policy framework, software requirements, and hardware components used to deter cybercrime. Effective cybersecurity policies are required for business growth and continuity (Furnell, S., 2012). Laws need to be reviewed and strengthened to support this fight against crime.
The social problems this development orchestrates makes this study very significant to help in finding lasting solutions to the menace.

Recommendations and Antidotes to Cybercrime

Success of modern day business operations depends on constant anti-cybercrimes mitigation strategies and this cannot be over-emphasised. The cost of the recent WannaCry malware attack already runs into billions of dollars, and which grievously compromised the United Kingdom's NHS. This is the latest case for coming into terms with aggressive cyber security measures.

Awareness of the dangers of cybercrime amongst the owners/operators of small businesses is need to be raised. While it is such an intimidating technological problem, media reports need to share their report between large enterprises and small companies. Recently, this paradigm has shifted a bit. A recent U.K. government discovered that 90% percentage of big businesses experienced formation security breaches, while a significant 74 percent of small businesses did so as well.

However, below are some steps that will helpprotect data and mitigate against the risk of severe data breaches:

1. Risk identification should be the first step. This will identify fully what data targets the criminals are interested in. Usually, hackers will be interested in your customer database. Breaching this data will incur fines, lawsuits, and loss of trust by customers. No thoughts should be spared in identifying where company data is stored and who has access to it, including staffs using personal laptops and phones that are connected to your company business network.
2. Worry about who plans to grab your data. Knowledge of kinds of attacks your business segment is usually subjected to is worth having. Additionally, spare some thoughts give thought to disgruntled staff members or staff members who may have loyalty to some cybercriminals who may give them access to your network.
3. Identification of weaknesses/vulnerabilities in your network security follows. Off-the-shelf software tools and specialists can carry out these kinds of intrusion detection and prevention system checks. Also, a penetration test can be carried out to determine exploitable vulnerabilities in the network.

4. Determine a useful idea of whatimpact a successful cyberattack on your system would have on your system in terms of infrastructure and data loss? This business-impact analysis will guide decision-making and prioritise actions.
5. Potential risks so identified should be resolved as quickly as possible. Make a prioritised list of what needs to be done (protection ofyour data, your customers'and vendor data and start crossing things off the list.
6. Identity of cybercriminals: An easy means of identifying who is doing what and where a user of the Internet is located at any point in time is still a paradox. The world wide web is free and there is no requirement that should be fulfilledregarding what one is doing and location.
7. Laws challenging the extradition of criminals and admissibility of evidence across countries and regional jurisdictions should be reviewed and made uniform. There should also be a global platform for seamless reporting and collection of data on cybercrimes to assist prosecution.There should be a reviewwhere exists any extant laws in place of cybercrime laws to aid prosecution.

Finally, this research is of the view thata problem identified is half solved. This research has tried to put into clearer focus the meaning of the various forms of cybercrimes and the motivations behind them. Some of the challenges faced by law enforcement authorities is the understanding and application of the relevant laws. A vital recommendation offered by this article, is the need to put in place a law, that would have worldwide applicability, such that, irrespective of the fact that wherever a cybercrime is committed, the perpetrator can be brought to book, anywhere else (Ajayi, E. F. G., 2016).I also suggest the deployment of technology e.g. firewall, to block direct access to trusted network resources by intruders. Furthermore, while it is not feasible to guarantee complete and permanent safety from cyber-attacks and threats, individuals and organisations can prioritise vulnerabilities and take countermeasures based on their risk appetites.Putting mitigation strategies in place, remediation can happen more swiftly and effectively in case any catastrophes occur (**CISOMAG** -June 16, 2017).

REFERENCES

1. Clough, J. (2010). *Principles of cybercrime.* Cambridge: Cambridge University Press.
2. Council of Europe, 2001.
3. Thomas, D., & Loader, B. (2000). Introduction—cybercrime: Law enforcement, security and surveillance in the information age. In D. Thomas & B. Loader (Eds.), *Cybercrime: Law enforcement, security and surveillance in the information age*. London: Routledge.
4. Kirwan, G. and Power, A.(2012) *The Psychology of Cyber Crime.* Hershey: IGI Global.
5. Ajayi, E.F.G. (2016). Challenges to enforcement of cyber-crimes laws and policy. https://academicjournals.org/journal/JIIS/article-full-text-pdf/930ADF960210
6. Team CYMRU. (2016). Can we protect ourselves from the hazards of an online world? An Epidemic.www.acmqueue.com
7. McGuire, M.(2013). Cyber-crime: A review of the evidence Summary of key findings and implications Home Office Research Report 75, Home Office, United Kingdom, October. 30p. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf
8. Child Exploitation and Online Protection Centre (2013b). Children treated like 'slaves'to perform sexual acts.<http://ceop.police.uk/Media-Centre/Press-releases/2013/Children-treated-like-slaves-toperform-sexual-acts-/>.
9. Cybercrime (Prohibition, Prevention, etc.) Act 2015. Nigerian Data Protection Regulation, 2019.
10. Chawki, (2005). Cybercrime in France: An Overview.http://www.crime-research.org/articles/cybercrime-in-france-overview
11. Gunter et. al (2010). Pirating Youth: Examining theCorrelates of Digital Music Piracy among
12. Adolescents, International Journalof Cyber criminology Vol 4 Iss 1and2, pp 657–671 http://www.cybercrimejournal.com/whitneyetal2010ijcc.pdf/
13. Heather, N. (2008) Electronic Law: Research Starters Business http://web.ebscohost.com/ehost/pdfviewer/pdfviewer?hid=105andsid=0af3d1fb-4a5b-43b3-9a63-88c64b0d59f9%40sessionmgr114andvid=1>.
14. Casey, E. (2004). Digital evidence and computer crime. St. Louis, MO: Elsevier Press.
15. Chawki, M. (2009). Nigeria tackles advance fee fraud. https://warwick.ac.uk/fac/soc/law/elj/jilt/2009_1/chawki/#a4
16. Majid, Y. (2006). Cybercrime and society. London: SAGE.

17. Wall, D. (2001). Cybercrimes and the internet. In D. Wall (Ed.), Crime and the internet. London: Routledge.

18. Kshetri, N. (2013). Cybercrime and cybersecurity in the global south. Hampshire: Palgrave Macmillan
19. Furnell, S. (2010). 'Hackers, Viruses and Malicious Software'. In Handbook ofInternet Crime, Jewkes, Y. and Yar, M., pp 173–193. Culhompton: Willan Publishing.
20. Moir, R. (2008). Defining Malware: FAQ. Microsoft WindowsServer 2003. http://technet.microsoft.com/enus/library/dd632948.aspx>.
21. Beal, V. (2011). The difference between a computer virus, worm, and trojan horse. http://www.webopedia.com/DidYouKnow/Internet/2004/virus.asp>.
22. Symantec (2012). Internet Security Threat Report 2011 Trends. Mountain View, CA:Symantec Corporation.
23. Wienclaw, Ruth A. (2008) Internet Security -- Research Starters Business http://web.ebscohost.com/ehost/pdfviewer/pdfviewer?hid= 105
24. Gunter, W., Higgins, G. and Gealt, R. (2010) Pirating Youth: Examining theCorrelates of Digital Music Piracy among Adolescents, International Journalof Cyber criminology Vol 4 Iss 1and2, pp 657–671. http://www.cybercrimejournal.com/whitneyetal2010ijcc.pdf/
25. Kirwan, G. et. al (2012) The Psychology of Cyber Crime. Hershey: IGIGlobal.
26. Sreehari A, et. al (2018). A study of awareness of Cyber Crime among College students with special reference To Kochi, International Journal of Pure and Applied Mathematics, vol. 119 no. 16 2018, pp. 1353-1360.
27. Lakshmanan, Ac. (2019). Literature review on Cyber Crimes and its Prevention Mechanisms. 10.13140/RG.2.2.16573.51684.
28. Alhomoud, A. et. al (2013). A Self-Healing Framework for Enterprise networks tocombat
29. Botnets infections.https://www.researchgate.net/publication/327468313**cisomag** - June 16, 2017).
30. Varshney, S. (2020). Cyber Crime Awareness and Corresponding Countermeasures
31. (International Conference on Innovative Computing and Communication). https://ssrn.com/abstract=3601807
32. Martellozzo, E. (2012). Online Child Sexual Abuse: Grooming, Policing and Child Protection in a Multi-Media World (1st ed.). Routledge. https://doi.org/10.4324/9780203124116
33. Black, G. et. al (2010) Computer and Internet crimes, San Francisco, California http://www.fd.org/pdf_lib/WS2010/WS2010_Computer_Crimes.pdf
34. Gunter, W., et. al (2010) Pirating Youth: Examining the Correlates of Digital Music Piracy among Adolescents, International Journal of Cyber criminology Vol 4 Iss 1and2, pp 657–671. http://www.cybercrimejournal.com/whitneyetal2010ijcc.pdf/