Chapter

Cybercrime: Victims' Shock Absorption Mechanisms

Obinna J. Eze, John Thompson Okpa, Chukwuemeka Dominic Onyejegbu and Benjamin Okorie Ajah

Abstract

The development of technology creates opportunities for businesses, seamless communications and leisure activities to thrive. However, it also propels crime. In Nigeria, cyber threat continues to evolve rapidly with rising number of victims on daily bases. This necessitated the present study that examines the shock absorption mechanism of the cybercrime victims in Nigeria. The data for this study came from a variety of sources, including books, articles, essays, tabloids, and journal publications; a content analysis approach was used to evaluate the data and present using certain words, themes, concepts, or codifications. The study found that the peculiarity of cybercrime lies in the fact that the victims willingly land themselves into it without being forced to do so. It starts with what seem to be a friendly conversation and exchange of correspondences and pleasantries which turns into a scamming spree. To this end, victims are left battered and shattered, and could act irrationally against own-self before state actors set out to track the offender(s). Thus, victims of cybercrime could absorb shock by spending quality time with significant others. This enables them feel the love and moral supports from close associates, other than wallow in loneliness and isolation which can breed unpleasant stimuli.

Keywords: cyber-attacks, cybercrime, law enforcement agencies, shock absorption mechanisms, victims

1. Introduction

Cyber-attacks are growing in multiple dimensions globally. Malicious cyber activity poses a danger to public safety, national security, and economic stability. The global cyber threat continues to evolve at a rapid pace, with a rising number of people falling victims on daily bases. The development of technology creates opportunities for people, such as business and leisure activities, but also enables criminals to commit crimes [1–3]. Research conducted by Pew research center (PEW) in 2014, reveal an astonishing 40% of all adult internet users admit to experience cyber victimization of different variants [4]. Most often, cyber-attacks such as hacking, phishing, business email compromise (BEC) malware attacks, password attacks, man-in-the-middle attacks, insider threats, and crypto-jacking are the most frequently suffered by victims [5]. Cybercriminals have access to a wide variety of psychological manipulation techniques. For instance, phishing emails are the most typical means through which hackers distribute ransomware. Fake emails are also used by hackers to deceive victims into opening dangerous attachments or clicking on hazardous links. Cybercriminals also exploit the natural desires of humans to trust others to send unsolicited electronic mails to unsuspecting victims, as though they originated from legitimate sources [6–8].

The betray of trust is very common technique used by dating fraudsters, they engage in the purposeful creation of trust with their victim, often over a period of weeks or months, with the goal of betraying them after extorting money from them. To learn later that a relationship that seems to be based on openness, closeness, and trust is really built on deceit is especially upsetting when it occurs in the context of a dating scam. In addition, the possibility that the event would become public, exposing the victim to scorn or sympathy, can generate profound emotions of shame. In the aftermath of a such crime, victims may be hesitant to confide in others who may otherwise provide practical and psychological help. For fear of being ridiculed or believing the police would do nothing, victims may not report such crimes. Interpersonal cyber-crimes constitute a breach of trust, and the emotional repercussions of "virtual betrayal" may be as devastating as those of physical betrayal. Victims have expressed feelings of sadness, anxiety, powerlessness, and rage. They may become despondent, even suicidal, and lose faith in other people [7, 9].

Green, Streeter and Pomeroy [10] reveal that the emotional effects of a crime and the selected coping technique rely on how well the chosen strategies meet the situational needs. "For example, if the situation resulting from a crime is perceived by the victim as somewhat controllable, he or she would be more apt to have positive emotional outcomes from using a problem-focused coping strategy as opposed to an avoidance-oriented strategy" [10, 11]. Holohan and Moos [11] further reveal that as the intensity of a stressful event grows, so does the significance of coping mechanisms. Against this backdrop, this chapter set out to foster coping mechanism, i.e. shock absorption mechanisms for dealing with cybercrime trauma while awaiting the protracted orthodox criminal justice outcomes in Nigerian setting, and by extension, other climes similar to Nigeria across the globe. The following research questions were put forward:

i. What is the classification of cybercrime?

ii. What are the patterns of cyber-crime?

iii. What are the shock absorption mechanisms adopted by victims?

2. Conceptualization of cyber crime

The concept of cybercrime is vast and the high-tech nature of the field has made it difficult for scholars in various field of cyber-criminology to agree on a particular definition for the concept. It has been suggested that since cybercrime may entail various types of crime, a definition of cybercrime has to place an emphasis on the specificity, the expertise, or the use of computer technology [12, 13]. Accordingly, Ajayi [14] observed that the above situation has made it difficult for scholars to come up with a universally accepted and recognized definition of cybercrime. Although, the definition of cybercrime varies slightly from one individual to another, there is a consensus among scholars on the important role of networked technologies in enabling this type of criminal activity. One frequently adopted definition of cybercrime describes it as any action in which computers or networks are a tool, a target or a place of criminal attack [15, 16]. The International Telecommunication Union (ITU) [17] defined "cybercrime as a criminal offence involving a computer as the object of the crime (hacking, phishing, spamming), or as the tool used to commit a material component of the offence (child pornography, hate crimes, computer fraud)". As the name suggests, this phrase appears often when computers or associated technology is employed in a criminal offence. Traditional crimes like distributing child pornography, illegal substances, and hate crimes may be considered cybercrimes since they can be perpetrated via the internet [12, 15].

Innovative Dynamic Networks (IND) [18] defined "cybercrime in a contracted sense to imply unlawful acts directed by means of electronic operations that targets the security of computer systems and the data processed by them". Cybercrime in a broader sense according to Innovative Dynamic Networks (IND) [18] refers to "prohibited activities committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network". United Nations Office on Drugs Control (UNODC), [19] defined "cybercrime as a cluster of unlawful behaviour such as offences against the confidentiality, integrity and availability of computer data and systems, computer-related offences, content-related offences and offences related to infringements of copyright and other related rights".

Cybercrime differs, according to McConnell International in Tamarkin [12], from most conventional deviant behaviours in four ways: the criminal act is relatively easy to learn, the cost of committing the crime is never proportional to the damages caused, it is a borderless crime and fourthly, the act, most times are not clearly prohibited. It is important to note that e-crime is perpetuated in the virtual environment. The virtual environment is designed in such a way that data about individuals, things, realities, proceedings, phenomena or events are depicted in mathematical symbol or any other way and transmitted through local and global networks. From the foregoing, the term 'cybercrime' can be applied in explaining, as well as, describing widespread destructions on computer data or networks through interception, interference or damage of such data or systems. It can also be used to explain and describe crime committed against computer systems or the use of the computer in committing crimes. The definitions, although not completely definitive, and perfect, provide a recognised and good framework for explaining cybercrime at the international level and within the context of this chapter.

3. Methods

This study is a narrative research that relied heavily on secondary research methodologies and examined only articles written in English. The data for this study came from a variety of sources, including books, journal essays, articles, tabloids, magazines, and scholarly materials from the internet in the areas of cybercrime. Google scholar and the Google search engine were used in the online search. This study therefore summarizes the data collected from these current research publications. After extensive research and evaluation of the available materials online, the major themes reported in this study were identified. The main ideas were selected and reported based on the frequency of their reporting in the literature. The literature focus was on reports and research findings on the curbing strategies of victims of cybercrime.

4. Classification of cybercrime

Ayofe and Irwin [20], and Poonia [21] broadly classified cybercrime into four primary taxonomies: "crime against persons, cybercrimes against property, cybercrime against organisations and cybercrimes against society".

4.1 Cybercrime against persons

In the cyber world, crime against persons manifest in form of transmitting child pornography, cyberbullying and harassment of cyber users [22].

4.2 Cybercrime against property

The second type of cybercrime includes offences committed against any and all kinds of property. "These crimes include unauthorized computer trespassing through cyberspace, Salami Attacks, computer vandalism, intellectual property crimes, transmission of harmful programs and unauthorized possession of computerized information".

4.3 Cybercrime against organisations

Organisations are seriously threatened and attacked by the activities of cybercriminals. Such attacks and threats have resulted to loss of sensitive information, money, and intellectual property. The activities of these criminals have also made consumers to lose confidence and trust in the services provided by these organisations. Cyber-terrorism is one of the most remarkable forms of cybercrime against organisations. Another form of cybercrime against organisations is cyber-warfare. Simply put, it refers to politically motivated hacking to conduct sabotage and espionage, especially, among nations.

4.4 Cybercrime against society

Cybercrimes against society may take the form of "forgery, cyber-terrorism, web jacking, polluting the youths through indecent programming, financial crimes, sale of illegal articles, net extortion, cyber-contraband, data diddling, logicbombs, etc". This type of crime also includes; revenue stamps, forgery of currency notes, certificates, mark sheets, among others, high grade scanners and printers may be used to forge these documents. Web jacking hackers obtain access to and control over the website of others, and they may even modify the content of the website to accomplish political aims or to make financial benefit.

5. Patterns of cybercrime in Nigeria

Cybercrime entails the application and manipulation of the internet to fraudulently derive benefits from unsuspecting users. Some of these crimes includes, spoofing/phishing, spamming or escrow services, web jacking and scam messages. Different authors have varying views but in simple terms, cybercrime encompasses all illegal activities carried out by a single or more individuals most times referred to as scammers, hackers, fraudsters, "419ners", using the internet through the medium of networked computers, telephones and other ICT equipment. Thus, the acts of cybercrime originated from the emergence of computers, telephones and other ICT inventions. Numerous conventional crimes are being perpetrated with the use of ICT inventions, they include:

Auction fraud: This is the misrepresentation of a product advertised for sale through an internet auction site, or the non-delivery of the products purchased through an internet auction site. The seller posts the auction as if he resides in the United States, then responds to victims with a congratulatory email stating he is outside the United States for business reasons, family emergency etc. They often post the auction under one name, and ask for the funds to be transferred to another individual or directly to him via Western Union, Money Gram or bank to bank wire transfer.

Huckstering: This is a process of obtaining email address from the internet access point using email harvesting software called web spiders (such as email Extractor Lite 1.4) to send a large number of messages to each harvested spam-trapped addresses and typical product based Spam (i.e. Spam selling an actual product to be shipped or downloaded even if the product itself is fraudulent).

Piracy: This is the act of illegally making access to people's soft copies such as, books, games, movies and CDs or DVDs, etc and make copies of same to disseminate for some gains which is usually financial gains [23]. Example, the use of pirated Microsoft Windows to install newly acquired computers; pirated home movies; and pirated MP3 music installed in phones, Ipads and other gadgets.

Hacking: This is the act of cracking firewalls or security codes with the use of computers, laptops and sophisticated phones in order to gain access to people bank accounts, data or any other profitable information.

Phishing/spoofing: This is the act of faking or forging digital information or documents [24]. Spoofing/phishing specifically connotes the fraudulent acts of forging a website to make it look like the original one to deceive persons having legitimate transactions with such websites or the harvesting of people's e-mails, and after consuming their contents, use same to defraud other people, who somehow feels the information received is authentic.

Ponzi/pyramid: This is a kind of money doubling scam. It is usually initiated as an investment for never to be receive profits. Because it a bogus and attractive investment proposal, desperate individuals often fall victim. The victims of these scams neither receives dividends nor their initial capital. Example, the 2009 money doubling scam in Calabar, Ikom and Ogoja in Cross River State.

Nigeria letter or "419": This named after a section in the Nigerian Criminal Code. 419 combines impersonation, obtaining by false pretence or advance fee fraud. The major trick for this scam is calculated persuasions. Victims are usually hooked with sensible persuasions after the fraudsters have anticipated their thoughts for every step to be taken. Victims who are charmed by these well added lies end up losing huge sums of cash or divulging their credits cards numbers or Automated Teller Machine pins.

Credit card fraud: This involves illegal or unauthorised use of people's credit/debit cards to steal their money. Out of carelessness or negligence, victims usually compromise their credit/debit cards numbers to fraudsters, who actually get same from close observation or outright theft, sometimes on gun point. In Nigeria, such numbers are obtained in ATM withdrawal terminals or robbery at any location and pins are obtained on gun point.

Identity theft: This is the act of impersonation for the purpose of committing theft. Individuals and organizational fake identities are used by fraudsters to dupe persons operating legitimate businesses.

Data dadding: This is a kind of attack which involves altering raw data just before it is processed by a computer and then changing it back after the processing is completed.

Salami attacks: These attacks are prevalent in the financial institutions. It is an alteration that is so insignificantly made such that in a single case it would go normally unnoticed. For instance, Salami Attack occurs where a bank employee inserts a program such as 'logic bomb' into the bank servers, that deducts small amount of money from the account of every customer and deposits it in another account opened and owned by the staff but with a different account name.

Internet time thefts: This is the act of manipulating or circumventing servers of network service providers in order to hack their passwords and gain login access. Fraudsters usually steal airtime from Internet Service Providers or GSM service providers, like the case that affected MTN Nigeria in February 2009.

Web jacking: This is the process of fraudulently gaining access into individual's, corporate organisation or government websites or e-mails and completely taking charge or control of it. This is done by breaking through the passwords and other unique features, and editing same whereby the original owner may not be able to gain access again.

Phone phishing: Phishing attack also extends to phones such that messages claimed to come from a bank may tell users to dial a phone number regarding problems with their bank accounts. Once the number (owned by the phisher, and provided by a voice over IP Service) has been dialled, prompts would tell users to enter their account numbers and Personal Identification Number (PIN) which the Phisher would use in defrauding the victim.

Pornography: This is the act of using ICT gadgets to illegally publish pornographic images, or the use of internet to download pornographic contents illegally. Most people still have the understanding that pornography does not amount to crime, but they forget to know that most pornographic images are illegally produced, and so everybody benefitting from such content is a criminal, while those less than 18years are delinquents.

Sale of illegal articles: This is the process of selling contrabands or illegal products such as hard drugs or weapons of mass destruction through the use of internet websites, e-mails, short message services and other means of digital communication. .

Employment/business opportunity fraud: On the Internet different websites and most often ‘pop-ups’ on web pages have been design to advertise lucrative employment opportunities and businesses with the aim of defrauding unemployed persons.

Forgery: This is the act of counterfeiting an original document, made possible and easy by the emergence of information and communication technology. It is the act of faking an original money note or coin, or any other document to make it look similar or almost the same as the legal or original one. In Nigeria, there are a lot of forged certificates and naira notes.

Cyber defamation: Character defamation as crime has also migrated from the verbal physical world into the digital world. This is an act of making mails, faxes, text messages, etc, slaying somebody's character and distributing same to acquaintances of the target victim. This is usually done for some selfish and fringe benefits.

Cyber theft: Any form of criminal activity that involves the use of information and communication technology is called cyber theft. Cyber theft is synonymous to cybercrime except that it is narrowed to issues that are outright theft such as, embezzlement with the use of ICT, stealing people's passwords and pins or hacking.

Cyber laundering: This is the process of illegally transferring monies or currencies with the use of ICT. This is usually done by fraudsters with the intention of concealing the source and destination of this monies or currencies. It is a common form of cyber criminality in Nigeria, where corrupt government or public officials cyber launder stolen money to other parts of the world in order to avert the wrath of EFCC and ICPC.

Key logging: This is the act of using software called key logger to stroke someone's computer keyboard in order to digitally monitor the activities taking place on that computer, and capitalizing on such information to defraud the computer owner.

Spam message: This is fake messages or e-mails directed at harvested e-mails or random numbers with persuading and attractive contents aimed at defrauding unsuspecting victims.

Malware: Malware short for malicious software, (sometimes referred to as pest ware) is a software designed to secretly access a computer system without the consent of the owner.

Lotteries fraud: Some corporate organizations in Nigeria garner millions of viewers to send text messages or to call in answers to a displayed question on TV or answer a question through SMS. The amount charged for such calls or text message (SMS) from the viewers amount to millions of Naira while the amount to be won might just be N10,000.00.

Phreaking: This type of crime involves the theft of telecommunication services, instances of which have involved using cereal box toy whistles to imitate telephone call signals, and more recently cloning mobile SIM cards. Many homes in Nigeria are now connected to DSTV products through a self made cord, which when attached to a video player, has the capability of connecting to several statements in DSTV television.

6. Victim susceptibility

Cyber criminals definitely have targets to explore. Likely cybercrime victims include;

The naive/gullible: There are certain persons who are easily deceived. This is because they trust almost everybody who comes their way. Even in the cyberspace, they try to be helpful to those they have never met. Cyber criminals prey on such individuals who are naive and slow about knowing much of the internet gimmicks. Older people usually fall into this category because they trust easily, and the intricacies of the computer are not of their generation.

Desperados (for money or "items"): So many youths wants to build sky scrapers within a twinkle of an eye and through any means, they easily fall victims to online pop-ups that read "Get rich fast". This desperation makes fraudsters to have their way with them. In many instances, these youths are cajoled into bogus and attractive business proposals, and even life-changing advertisements. In these businesses, investors who are invariably the victims never recover their initial capital, let alone make profits. The sole benefactors are the initiators of the businesses who are the perpetrators. On the other hand, students are the major victims of cyber stalkers because of their desperation to meet people online and make friendship. Sometimes, this online friendship is sought by students to boost their self-esteem or personal ego.

Unfortunately, they become victims of internet hoodlums who either manipulate them for the satisfaction of their sexual appetite or other rituals.

The inexperienced: So many people have frivolous attitude towards ICT. They are mostly contented with just making calls and sending text messages or checking e-mails, without the desire for requisite knowledge on the detail use or application of digital devices. Such persons cannot protect their phones or computers from malicious damage and intrusion. Even when they have information that such crimes exist, they still fall victims because of their inexperience.

Unlucky people: These are people who are very unlucky in life. They fall victim of cybercrimes as a result of their fate which has made them to be found at a wrong place, at a wrong time. For example, malicious viruses can be circulated in the cyberspace and only unlucky people's computers and phones will be infected, which will result to serious damage and destruction of their systems and data. In this case, it does not matter how knowledgeable or proficient you are in protecting your data, you can just be unlucky.

7. Target hardening

Cyber criminality is a phenomenon tied to the daily routine of individuals. To this end, Cohen and Felson in 1970 articulated the Routine activities approach which derives from the fact that elements of a criminal or deviant act come together in normal, legal, and routine activities [25]. At the heart of routine activities are three premises often referred to as the crime triangle; a likely offender, a suitable target, and the absence of a capable guardian. Routine activities theory posits that criminal victimization increases when motivated offenders and suitable targets converge without let or hindrance [26].

Within the cyber space, the massive spread of global system of network provides the fertile ground for the absence of a capable guardian, the internet user then becomes the suitable target, waiting to be devoured by scammers who are the motivated offenders in this regard. However, from the routine activities approach, if internet users adopt target hardening strategies like; two-step security code authentication, periodic password change, firewall settings, anti-virus definition update, One Time Password (OTP) validation, etc., online criminal victimization will decline.

Thus, target hardening ensures that online users take the responsibility to police their own activities on the internet. The stipulations of the routine activities approach is best suited to guard internet users in the sense that people are supposed to guard their login details securely from un-trusted sources. This includes ensuring that websites being accessed are well secured with the inscription “https” or “locked padlock”. In another light, parental control should be activated in computer and internet gadgets used by underage children to guard them from cyber stalking and pornography. Put succinctly, the watchword to target hardening as posited by the routine activities approach with regards to cyber criminality refers to all deliberate authentication and security efforts adopted by the internet user to ensure that online activities are protected from scammers.

8. Shock absorption mechanisms

Cyber crime triggers emotional bankruptcy on victims. Most time, victims of cyber crime commits suicide upon the reality of the extent of loss they suffered in the hands of scammers. Therefore, most victims of cyber crime could have lost their sanity or life moments after reality of being duped. Shock has been found to have helped individuals regulate their emotional response mishap [27]. The aim of this chapter is to proffer possible shock absorption mechanisms which could help victims to go past the emotional scam associated with cyber crime, owing to the fact that only the living, or the sound mind can logically seek for justice and retribution for a crime committed against them. Thus, the following shock absorption mechanisms are posited:

a. Talk to someone about the situation, a problem shared is a problem half solved. There is tendency for a victim of cybercrime to reach out to someone immediately; this is to avoid being blamed. But rather than bottling up the emotion, it is better to let it out and lessen the burden in the heart.

b. Spend quality time with significant others. This will enable the victim to feel the love and moral support from close associates, than wallow in loneliness and isolation which can breed unpleasant stimuli.

c. Approach daily tasks with care. In the midst of clouded thoughts, accidents are more likely to happen after severe stress. Thus, the need to undertake activities with care. It is most appropriate to have adequate rest for the day, until the victim gradually bounce back to normalcy.

d. It is necessary to re-establish a normal routine as soon as possible, but it should be taken gradually.

e. Exercise should be undertaken at certain intervals of the day, as this could be shuttled between periods of relaxation

f. Victims are not to take laws into their hands but rather should report to law enforcement agents to take action.

The above shock absorption mechanism require that victim avoid certain behavioural tendencies such as: alcohol or drugs for the purpose of relieve from emotional pain, making substantive life decisions at the moment, withholding emotions and self-blaming. It is pertinent to note at this juncture that cybercrime could leave victims with a feeling of emptiness, and a trigger of emotion even after several years. However, in this midst of these, it is impossible to undo what has happened but life can be good again in time. In the light of the forgoing, significant others to the victim have traditional roles to play to promote the integral efforts of shock absorption. This includes spending time with the victim, offering assistance where necessary, giving listening ear, avoid triggering negative emotions on the victim, showing empathy, and any other humanistic gesture.

9. Conclusion

Cybercrime since its inception has left its victims shattered and demoralized to the point of taking their own life or loosing total sanity to the point of no recovery, in a word, cyber crime has left its victims in a state of Robert Merton's "anomie". The peculiarities of cybercrime lie in the fact that the victim willingly lands him or herself into it without being forced to do so. It starts with what seem to be a friendly conversation and exchange of correspondences and pleasantries which turn into a scamming spree. Unlike other criminal ventures, cyber criminality stem from betray of "trust" but unfortunately "false trust". To this end, victims are left battered and shattered, and could act irrationally against own-self before state actors set out to track the offender. For this, this chapter outlined shock absorption mechanisms to deal with the rising and dynamic trend of cyber criminality to save the victim prior to state intervention to bring the perpetrator to book.

Acknowledgements

The authors appreciate Ifeoma Nuela Arinze who typeset the initial draft of the paper.

Conflict of interests

The authors declare no conflict of interest.

Notes/thanks/other declarations

The authors sincerely appreciate sources cited in this intellectual output.

Author details

Obinna J. Eze[1], John Thompson Okpa[2], Chukwuemeka Dominic Onyejegbu[3]
and Benjamin Okorie Ajah[1]*

1 Department of Sociology and Anthropology, University of Nigeria, Nsukka, Nigeria

2 Department of Sociology, University of Calabar, Calabar, Nigeria

3 Social Sciences Unit, School of General Studies, University of Nigeria, Enugu, Nigeria

*Address all correspondence to: okorie.ajah@unn.edu.ng

References

[1] Alawari BM, Ajah OB. Understanding the Gender Dimensions of Cyberbullying among Undergraduates in Nigeria. Zaria: Ahmadu Bello University Press Limited; 2017

[2] Reep-vanden Bergh CMM, Junger M. Victims of cybercrime in Europe: A review of victim surveys. Crime Science. 2018;**7**(1):5

[3] Okpa JT, Ilupeju AA, Eshiotse E. Cybercrime and socio-economic development of corporate Organisations in Cross River State, Nigeria. Asian Journal of Scientific Research. 2020;**13**:205-213

[4] Lenhart A. Teens, Social Media, and Technology Overview. Washington, DC, USA: Pew Research Center; 2015

[5] Okpa JT, Ajah BO, Nzeakor OF, Eshiotse E, Abang TA. Business e-mail compromise scam, cyber victimisation and economic sustainability of corporate organisations in Nigeria. Security Journal. 2022;**35**(2):1-23. DOI: 10.1057/s41284-022-00342-5

[6] Ukwayi JK, Okpa JT. Critical assessment of Nigeria Criminal Justice System and the Perennial Problem of awaiting trial in Port Harcourt Maximum prison, Rivers State. Global Journal of Social Sciences. 2017;**16**:17-25

[7] Reyns BW, Fisher BS, Bossler AM, Holt TJ. Opportunity and self-control: Do they predict multiple forms of online victimization? American Journal of Criminal Justice. 2019;**44**(1):63-82

[8] Okpa JT, Ajah BO, Igbe JE. Rising trend of phishing attacks on corporate organisations in Cross River State. Nigeria International Journal of Cyber Criminology. 2021;**14**:460-478

[9] Ajah BO, Onyejegbu DC. Neo-economy and militating effects of Africa's profile on cybercrime. International Journal of Cyber Criminology. 2019;**13**(2):326-342

[10] Green DL, Streeter C, Pomeroy E. A multivariate model of the stress and coping process. Stress, Trauma and Crisis. 2005;**8**(1):61-73

[11] Holohan C, Moss R. Life stressors, personal and social resources and depression: A four year structural model. Journal of Abnormal Psychology. 1990;**11**(1):31-38

[12] Tamarkin E. Cybercrime: A complex problem requiring a multi-faceted response. ISS Policy Brief. 2014;**51**:1-3

[13] Nnam MU, Ajah BO, Arua CC, Okechukwu G, Okorie CO. The war must be sustained: An integrated theoretical perspective of the Cyberspace-Boko Haram Terrorism Nexus in Nigeria. International Journal of Cyber Criminology. 2019;**13**(2):379-395

[14] Ajayi EFG. Challenges to enforcement of cyber-crimes laws and policy. Journal of Internet and Information Systems. 2016;**6**(1):1-12

[15] Ndubueze PN, Igbo EUM. Third parties and cyber-crime policing in Nigeria: Some reflections. Oxford University Press. 2013;**8**(1):59-68

[16] Cisar P, Maravic CS, Bosnjak S. Cybercrime and Digital Forensics–Technologies and Approaches. Vienna, Austria: Daaam International Scientific Book; 2014. pp. 525-542

[17] International Telecommunication Union (ITU). Understanding

Cybercrime: A Guide for Developing Countries. Switzerland: ITU Publication; 2009

[18] Innovative Dynamic Networks (IND). United Nations' definition of cybercrime. 2016. Available from: https://idn-wi.com/united-nations-definition-cybercrime/

[19] United Nations Office on Drugs and Crime (UNODC). Cybercrime. 2018. Available from: https://www.unodc.org/unodc/en/cybercrime/global-programmecybercrime.html

[20] Ayofe AN, Irwin B. Cyber security: Challenges and the way forward. GESJ: Computer Science and Telecommunications. 2010;**6**(29):56-69

[21] Poonia AS. Cyber crime: Challenges and its classification. International Journal of Emerging Trends & Technology in Computer Science (IJETTCS). 2014;**3**(6):119-121

[22] Desai PN, Patel AM. Cyber Crime against Person. International Journal of Innovations in Engineering and Technology (IJIET). 2013;**2**(3):198-201

[23] Longe OB, Longe FA. The Nigerian web content: Combating the pornographic malaise using web filters. Journal of Information Technology Impact. 2005;**5**(2):29-50

[24] Loftness S. Responding to "phishing" Attacks. USA: Colenbrook Parnera Publishers; 2004

[25] Schaefer S. The Victim and His Criminal: A Study of Functional Responsibility. New York: Random House; 2005

[26] Brown SE, Esbensen F, Geis G. Criminology: Explaining Crime and Its Content. USA: Mathew Bender & Company Inc; 2010

[27] Pearlin LI, Schooler C. The structure of coping. Journal of Health and Social Behaviour. 1978;**19**(March):2-21