Cybercrime Schemes and Search by the Police

Osagioduwa Lucky Ogbomo & Olawole Wisdom

University of Benin

ABSTRACT

This study provide an empirical vision of cyber policing with it sectional comparative philosophy. The research therefore seeks to determine the extent of relationship between search by the police force and reduction in CBCE in Nigeria. Also, the study further seeks to investigate the degree to which CBCE suspect are prosecuted by the police force. The study embraces the interpretivism philosophy with the deductive theoritical approach. Methodological choice was mono quantitative method. Copies of similar questionnaire were administered to both youths in Edo State and personnel of the Nigerian Police Force in the state. Survey strategy was adopted in this research. The opinions of respondents were sought. Cross sectional time horizon was employed. The study sought the views of two distinct sections with peculiar interpretation of cyber crime operationality namely, the youth (section A) and the police force (section B). the non-probabilistic sampling methodology was further embraced in the study. The responses from both sections were analyzed comparatively in the study. Fifty-six (56) documents were retrieved from both sectional respondents. The analysis was was done using response Comparative- Percentage- Techniques (COPTA).

Keywords: cybercrime, search, police, scheme, cyber policing, internet fraud.

Classification: FOR Code: 391401p

Language: English

Cybercrime Schemes and Search by the Police

Osagioduwa Lucky Ogbomo[α] & Olawole Wisdom[σ]

ABSTRACT

This study provide an empirical vision of cyber policing with it sectional comparative philosophy. The research therefore seeks to determine the extent of relationship between search by the police force and reduction in CBCE in Nigeria. Also, the study further seeks to investigate the degree to which CBCE suspect are prosecuted by the police force. The study embraces the interpretivism philosophy with the deductive theoritical approach. Methodological choice was mono quantitative method. Copies of similar questionnaire were administered to both youths in Edo State and personnel of the Nigerian Police Force in the state. Survey strategy was adopted in this research. The opinions of respondents were sought. Cross sectional time horizon was employed. The study sought the views of two distinct sections with peculiar interpretation of cyber crime operationality namely, the youth (section A) and the police force (section B). the non-probabilistic sampling methodology was further embraced in the study. The responses from both sections were analyzed comparatively in the study. Fifty-six (56) documents were retrieved from both sectional respondents. The analysis was was done using response Comparative- Percentage- Techniques (COPTA). Findings indicates that a good number of teenager driving expensive cars are usually first suspect of CBCE activities.It was also discovered that 3.5 percent of the youth will engage in CBCE even when the government plans and ensure high standard of living for its young adult. Furthermore, result pointed that only 11.25 percent of Nigeria police are knowledgeable of the various techniques employed in perpetuating CBCE in Nigeria. The author recommends that police officers should be expose to both local and global training.

Keywords: cybercrime, search, police, scheme, cyber policing, internet fraud.

Author α: PhD in view, University of Benin) Bursary Department Lighthouse Polytechnic,Edo State Nigeria Olawole Wisdom.
σ: Police Office, Edo State.

I. INTRODUCTION

Development of internet technology had made the general populaces more at the mercy of on Internet which is a breeding field of nasty activities like cybercrime (CBCE). The origination of the World Wide Web (WWW) in the year 1989 has accelerated digital communication and interaction in the globe (Hunton, 2011). Thi-s occurrence of the Internet has significantly impacting upon and reinforcing several essential facets of contemporary civilization and critical public and social infrastructures. Directly, CBCE is a demanding concern for state and intercontinental police institutions to react to CBCE, together with the multifaceted diminuendos of CBCE networks'(Harkin et al, 2018). Importantly, cyber policing envisions mammoth challenges to condense victimization. Privatization of policing CBCE is critical (Yar, 2013b; Boes and Leukfeldt, 2017; Finn, 2019).

Weighing strategically the actuality of CBCE Brenner (2001, 2004) asserted that CBCE is a divergent category of criminality from a law perception. All form of CBCE has a counterpart crime in the physical world. For example, vandalism can be seen as the tangible world correspondence of hacking (Petee, Corzine, Huff-Corzine, Clifford, and Weaver, 2010). However, disjointedness exists between real-life Yar (2005) criminalities and cybernetic crimes. Yar (2005) further debated that computer-generated space builds exceptional openings for the commission of the novel category of criminalities; such crime cannot be executed in the physical world. Furthermore, Wall (2017a,

2017b) disputed that the internet machineries did not just produced newfangled chances for CBCE, but have also transformed the landscape of real-world criminalities. Distinguishing between CBCE and real-world crimes, CBCEs are definite variety of innovative criminalities, which cannot to be discharged and perpetrated in the absenteeism of Internet machineries.

A number of researchers (Ruddell, Thomas, and Patten, 2011; Joh, 2019; Lam, 2019 Yar, 2013b; Boes and Leukfeldt, 2017; Finn, 2019) argued that CBCE policing should be a private sector affairs. In the same direction, Yar, (2013) and Button, (2019) contended that policing should not be restricted to public police bearing in mind that CBCE as a new-fangled category of criminality has specific significant implications for policymakers in the country. Also, Yar (2013b) highlighted that a number of private organization and players for example Internet services providers, social network services (i.e. Twitter, Facebook) and non-governmental organization (NGOs) (i.e. The SANS Institute or Internet Watch Foundation 'IWF') may well have quite a few tasks in controlling and administering the Internet.

Pieces of literature indicate that studies on CBCE was conducted by Sumanjit, D. & Tapaswini, N, (2013), Azah, A. A. (2020) Ajayi, (2016), Ahmet, (2014), Olusi, Aguele, Ihumuaibvi, &Edobor, (2009), Cameron, (2015), Maitanmi, Ogunlere, Ayinde, & Adekunle, (2013), Maziah, (2016; Igba, Elizabeth, Aja, Simon, Egbe, & Ogodo, (2018); Vishi, & Shruti, (2018); Farzana, (2019); Andrea, Florian, Bernhard, Jo, Emmanouil, & Max, (2018); Paek, Nalla, Chun, & Lee, (2021), UNODC, (2021); Anca, Claudiu, Mara, Lucian, Leonardo, & Catalina (2021) respectively. However, studies on cyber policing known where conceptual and narrow. This study provide an empirical vision of cyber policing with it sectional comparative philosophy. The research therefore seeks to determine the extent of relationship between phone search by the police force and reduction in CBCE in Nigeria. Also, the study further seeks to investigate the degree to which CBCE suspect are prosecuted by the police force.

II. CYBERCRIME

Alkaabi, Mohay, McCullagh and Chantler, (2010) highlighted that professionals, police, attorneys, criminologists, and state security specialists fathom the concept of CBCE differently. Researchers like Gordon & Ford, 2006; Wall & Williams, 2001; Snyder, 2001; Yar, 2005 attempted to tailor the essential features of CBCE but was with limited unanimity. Goodman and Brenner, (2002) defined CBCE as the deliberate manipulation of ICTs by crooks. Association of Chief Police Officers (ACPO) noted that CBCE or "e-Crime" involves the usage of linked computer or Internet technology to commit or assist the commission of e-criminality (Association of Chief Police Officers, 2009). On the contrary, the Australian Institute of Criminology (AIC) regards CBCE as the commontag for all offenses committed employing an e-data storage or communications instruments" (Australian Institute of Criminology, 2011).

It is usually deliberated that there is a absence of harmony around a standard definition of the cybercrime in the literature (Wall, 2008; Anderson, Barton, Böhme, Clayton, Van Eeten et al., 2013; Williams and Levi, 2015)

Network Crime (NETCRY): NETCRY is the deliberate use of a computer instrument to carry out or performs illegal activities, such as committing fraud, trafficking in child etc. (www.britannica.com, nd.).

Telecommunications Fraud (TELFR): TELFR means the act of a third party gaining entrance to and using the Insured Organization's telephone line in an illegal manner and method (www.lawinsider.com).

Cyberbullying (CBBULL): National Bullying Prevention Centre (NBPC) debated that CBBULL is the engagement of information technology to continually and purposefully pester, hurt, embarrass, demean, or intimidate an individual. Furthermore, CBBULL include revealing individual or secret information about somebody, initiating embarrassment or disgrace. Some CBBULLs are criminal conduct (*StopBullying. gov). Also, Hinduja and Patchin, (2019) in*

agreement with NBPC submission *noted that* CBBULL is when an individual constantly and calculatedlyteases, mistreats, or makes amusement of a targeted person online, employing cell phones or automated garget.

Cyberstalking (CBSTAL): CBSTAL is typology ofCBCE in which somebody harasses or stalks a target by means of electronic or digital device, such as email, social media, instant messaging (IM), or communications forwarded to a chat group. Intentionally, CBSTAL take advantage of the facelessness and anonymity provided by the internet to trunk or harasses their victims, occasionally without being discovered, punished or even identified(Rahul,nd).

YahooYahoo (YAYO): YAYOentails perpetrating online frauds scheme that range from identity credit card tricks, prevarication and larceny, counter feitcheque and money order transactions, and online shopping (https:// www.nairaland. com/71121/y). Yahoo boy in the Nigerian context is juvenile (young male or female) who defraud others nationally or internationally using various means largely the Facebook handle.

Yahoo Plus (YAPLU): Premium Times (2022) distinguishing between YAYO and YAPLU revealed that YAYO is the consistent and frequent internet scam, but YAPLU involves rituals and the use of human parts and renewable sacrifices rituals in other to charm and easily influence the targets.

Cyber SEX (CBSXXX): Nicola (2000) debated CBSXXX is same as Internet sex, computer sex, netsex and, cyber or cybering, colloquially, is a computer-generated sex happenstance in which more than one individuall inkeddistantly via computer system exchange sexually unambiguous messages unfolding a sexual involvement. Furthermore, CBSXXX is a sub-type of technology-mediated sexual interactions. Eventually, Harley (1996)added clearly that CBSXXX also involves real life masturbation. Harley (1996) added that the quality of a CBSXXX encounter classicallyis contingent upon the participants' emotional capacities to arouse a glowing, intuitive mental picture in the thoughts and Imagination of their buddies. CBSXXX can arisebetween lovers who are physicallydistant or

among persons with no erstwhile knowledge of each other and meet in virtual spaces and may even be unknown to each other. In some environments,CBSXXX is heightened by the use of a webcam to diffuse real-time video of the partners.

Cyber Trafficking (CBSXXT): IJM, (2020) and CNN (2013) asserted that CBSXXT is the live streaming of forced sexual performances and or an outright rape. Targets are kidnapped, threatened, or mislead and conveyed to CBSXXX dens. The Philippine Star, (2020), *ASEAN Post (*2019) and Manila Bulletin (2020) noted that the CBSXXX dens can be in severalsetting where the CBSXXX traffickers have access to thetablet, computer, or phone with internet network. IJM(2020) added firmly that players use pornographic video sharing websites, social media connections, videoconferences, online chat rooms, dating pages, dark web sites (NBC, 2018), and other platforms.Also, Philippine, (2019) remarked thatthey use online payment systems (NBC News, 2018 & Reuters 2019) and cryptocurrencies to hide their personalities. Furthermore, South China Morning Post (2019] added that Loads of reports of CBSXXT happenings are referred to authorities yearly. Meanwhile, VOA,(2017) and the South China Morning Post (2019), highlighted vividly fresh regulations and constabularies procedures are needed to fight this type of CBCE.

Vishing (VSH): VSH is the fraudulent activities of calling or leaving voice notes claiming to be from trustworthy establishments in order to persuade the targeted individuals to disclose private financial information, such as bank particulars and credit card statistics. Simply, Vishing (voice or VoIP phishing) is an automated fraud scheme in which persons are deceived over the phone. (https://www.techtarget.com/searchunifiedcomm unications/d).

Smishing (MSH): MSH is a the fraud scheme of sending text messages alleging to be from dependable and reliable corporations in order to convince the focused individuals to divulge private information, such as PINs, or credit card information (www.google.com/search?cli).

Phishing (PSH): PSHinvolves the practice of sending emails purporting to be from reputable

establishments with the intent to induce targeted persons to expose and secret particular information, such as passwords, PIN, and credit card information.Furthermore, PSH is the trick of hoodwinking Internet users through deceptive email messages into revealing private or personal statistics which can then be used dishonestly(https://www.merriam-webster.com/dictionar).

Hacking (HAKI): HAKI is the useof computer device to access personal and confidential information kept on a different computer system without authorization, or to spread a computer virus.(https://dictionary.cambridge.org/dictionary/english/hacking).

Spamming (SPNG): SPNG simply means sending or dispatching "junk" mails to other internet users or participants of a delivery list (https://www.lawinsider.com/dictionary/spamming).

Access Crime (ACCE): ACCE means gaining access into another person computer without awareness (Osagioduwa 2022).

Cyber Theft (CTT): CTTis carried out by way of computers or the internet. (www.google.com/search?cli)

Money Laundering and Tax Evasion (MLTA): Money laundering entails concealing the source and quantity of income. Money laundering is an endeavor to camouflage illegitimate earnings from prearranged criminality as genuine income or to delete evidence of earnings altogether (www.google.com/search?cli).

Cyber Vandalism (CVDM): CVDM is the destructive cyber-attacks devoid of any understandable profit or ideological motivation. Cyber vandals can mar websites, interrupt an enterprise's services, or obliterate databases and important files (https://nordvpn.com/cyber security/glossary/c).

Online Gambling (ONGA): ONGA involves betting on casinos, gaming club or sports over the internet. Well, ONGA is also termed Internet Gambling or e-gambling. Generally, credit cards are used to place the gamble and landslide or sufferers are determined thereby (https://indian legalsolution.com/online-ga).

Network Sabotage (NESAGE): NESAGE is the modification, expurgation or destruction of computer documents or programs, or meddling with computer systems, with the motiveof hindering the working of a computer or a telecommunication system (www.google.com/search?cli).

Salami Attack (SATA): SATA is same as Salami slicing tactics, salami tactics, salami slicing, and the salami-slice strategy is the scheme of breeding a chain of numerous small actions to yield a much greater action or consequence that is impossible or illegitimate to carry out at on one occasion(www.google.com/search?cli). Salami Slicing Attack" or "Salami Fraud" is a practice by which Cyber-criminals steal fund a little or a bit at a time so that there's no conspicuous dissimilarity in the total amount (https://howtoin fosec.com/2021/06, 2021)

Telecommunications Piracy (TEPI): TEPI is the manipulation of telecommunications products (principally handsets and cell phones) or services with the objective of criminal obtaining cash from a communication service provider or its patrons(www.google.com/search?cli).

Virus Dissemination (VIDIS): VIDIS is a deliberate practice of sending malicious software that fastensand join itself to target software. Trojan horse, Virus, Time bomb, Logic Bomb, worms, Rabbit and Bacterium are samples of malicious software that damages the computer software of the victim.(http://alphasquad blogging.blogspot.com/2016/12/vi)

Pharming (PAMI): PAMI is the fraudulent exercise of pointing internet users to a counterfeit website that has the form of a genuine website, in order to acquire delicate figures such as passwords, PINs, account numbers, etc. furthermore, abroadly used PAMI description is cyber fraud that comprises the engagement of malicious program to connect victims to hoaxed websites in an effort to collect their relevant and personal information, credentials, and data. (https://www.fortinet.com/resources/cyberglossary/pharming)

Network Snooping (NETPI): NETPI is the mugging of special information when

communicating over a network by a computer system, smartphone, or a different linked device. The scheme takes opportunity of unguided network communications to get information as it is being sent or received by its user (https://www.google.com/search?client).

Credit Card Fraud (CCFD): CCFD is a king of identity theft that encompasses an unconstitutional taking of target's credit card statistics with the intention of charging procurements to the victim's account or does away with resources from the account (https://www.google.com/search?client).

Salesand Investment Fraud (SIFAD): SIFAD ordinarily involve fraudsters communicating individuals unexpectedly and convincing the people to participate financially in schemes, investment, coins, or products that are insignificant or do not exist. Unfortunately, upon the receipt of payment by the criminals, they terminate connection with the prey (https://www.google.com/search?client).

Child Pornography (CHIPO): CHIPO is any pictorialdescription of sexually openbehavior involving a minor (anyone below 18 years).These compriserepresentations across different social media, including: Videos, Immature film. Photographs, Digital pictures or videos, Computer generated images indistinguishable from a concreteminor(https://www.robertmhelfend.com /criminal-defense/sex-crimes/what-is-child-porn ography/).

Hoaxes (HES): Pournelle (2004) noted that there are two straightforward classifications of Internet deceptions: frauds, where the purpose is to defraud others, and HES, where the prime objective is simply to pull the chain, but with abroad consequences. HES give the criminals ego gratification as they see their scheme grow through the Internet. Frauds give the culprit's savings of the target, and years of hassle. Meanwhile, HES are shared by mails and come in an infinite assortment of guises. (Pournelle, 2004)

Data Diddling (DID): DID is a form of CBCE in which data is changed as it is typed into a computer system, usually by a data entry official or a computer virus. Computerized processing of the altered data results in a fraudulent benefit (https://www.google.com/search?client)

Illegal Interception of Telecommunications (IITE): IITE involves gaining access to the signal, collecting the signal, and exfiltration of the signal (Purpura, 2013).

Cybersquatting (CUT): CUT is the practice of registering, trafficking in, or using an Internet domain name, with bad faith intent to profit from the goodwill of a trademark belonging to someone else. (https://www.google.com/search?client).

Email Crime (EMAC): EMAC is same as email scam. It is the premeditated trick for either individual advantage or to hurt a targeted target through mails. Immediately email became generally adopted, EMAC instantly began to be employed as a channeland tool by fraudsters to swindle people of their assets and resources. Similarly, EMACoften take the shape of a "con game", or scam (https://www.google.com/ search?client).

Cyber-Terrorism (CYTI): CYTI is the engagement of network system and related information technology with the goal of initiatingimpairment or damage, with the purpose of compelling the resident population and influence policy of target government or otherwise affect its conduct (https://www.google.com /search?client).

Aiding and Abating Cybercrime (AIDAC): AIDAC involves helping, covering, sheltering, sponsoring, assisting (directly or indirectly),and encouraging cyber scammers. Furthermore, AIDAC entails aiding and abetting the crook in his getaway in relation to e-crime.

Defamation (DAMAT): DAMAToccurswhenan individual has circulated a statement about an individual or a targeted enterprise which injure the reputation or disparages of the organization.(Bloomsbury-law.com › defamation, 2022).

Cyber Espionage (CYEN): Kurt (2022), believes that CYEN is same as cyber spying. CYENis a form of cyber-attack whereby an illegal user endeavors secretly to access delicate or confidential documents or intellectual property (IP) for monetary,advantage, competitive,and political

motives(Kurt, 2022). Espionage also involves collecting information secretly by spying and individual, organization, or country strategy with the intention of selling same to another party for economic gain. CYEN can be grouped into:

- *Spyware (SPY):* SPY is computer software that is engineered to collect illegitimately someone's data without their permission. SPY is often contracted through defective network browsers or by being downloaded without the target being aware of doing so (Kurt, 2022).

- *Tracking Cookies (TRAT):* TRAT is usually involves trailing someone's internet service so that advertisers target that victim with ads tailored to their benefits.

- *Key logging (KEY):* This is when a program records a person's keystrokes, which can be used to steal secret pin and social numbers (Kurt, 2022).

Cyber Attack (CATA): CATA entails gaining unauthorized entrance to an individual or organization computer with the primary objective of causing damage to the computer system, files, and network (Pratt, 2022).

Man-in-the-Middle (MITM): MITM result when cyber hackers secretly insert themselves between more than one parties, for instance spying individual computer users and their financial institutions. MITM is same as monster- in-the-middle attack (MDA), man- in- the-browser attack (MBA), eavesdropping attack (EVA), machine-in-the-middle attack (MMA), (Pratt, 2022).

Distributed Denial of Service (DDoS): DDoSoccurs when crackers bombard an establishment's servers with enormous volumes of concurrent information demands, thus making the company's servers incapablein managing any legitimate needs (Pratt, 2022).

Structured Query Language (SQL) Injection (SQLI): SQL Iinjection arises when hackers input malicious code into servers employing the SQL programming language to get the server to divulge and collect sensitive personal or organizational information (Pratt, 2022).

Zero-Day (ZED): ZED exploit occurs when cyber hackers first exploit a newly noticed and identified weakness and vulnerability in IT structure (Pratt, 2022).

Domain Name System (DNS) Tunneling (DNST): DNSTis a refined attack wherein hackers launch and then use untiringly, existing access or a tunnel into their targets' systems (Pratt, 2022).

Drive-By or Drive-By Download (DDD): DDD arises when an internet user browses a website that, in turn, infects the innocent person's system with malware (Pratt, 2022).

Credential-Based Attacks (CBA): CBA occur when cyber attackers steal the credentials that ITpersonnel uses to open, operate and administers a computer system and then use the stolen data to illegally access the victim computers to collect secret data, disrupt an entity, and its processes(Pratt, 2022).
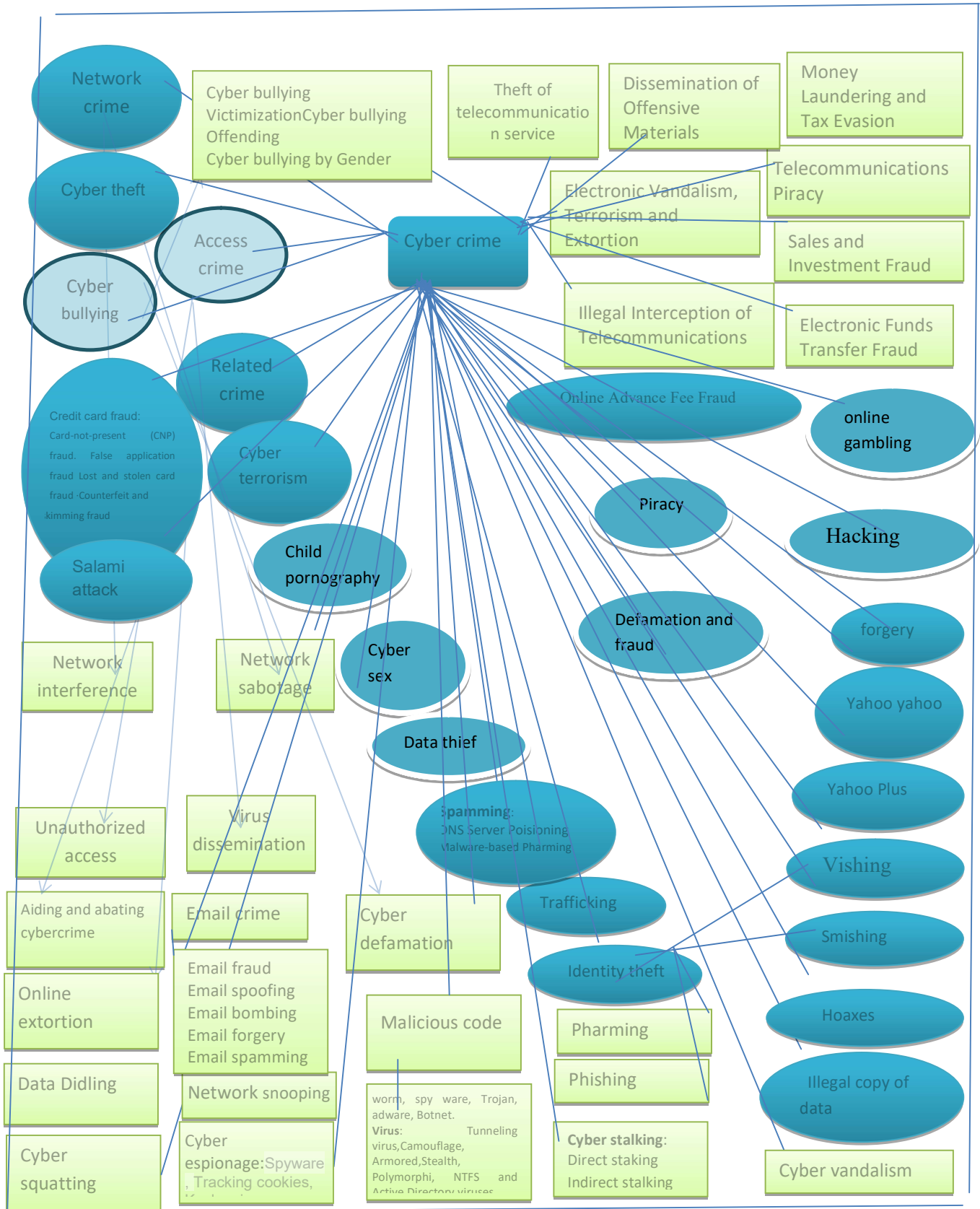
Credential Stuffing (CRS): CRSresults when cyber intruders employs compromised login permits, for instance email and password to access a targeted systems (Pratt, 2022).

Brute-ForceAttack (BOFA): BOFA is a situation in which cyber fraudsters uses trial-and-error attempts to crack login details such as usernames, passwords and encryption keys, trusting that the several tries pay off with an accurate guess (Pratt, 2022).

Malware (MAW): MAW refers to viruses, Trojans, worms and other software that gets onto your computer without your knowledge.

LogicBombs (LOBO): LOBOcommands the computer system to implement a particular command at a definite date and time or under certain speculated situations. The specified commands or orders might require the computer to reveal a verification technique on the screen;LOBO can instruct the computer to start deleting its files. LOBO often works similar to viruses. While a virus contaminates a given computer program after which reproduces when the computer program begins to run, the LOBO does not replicate. LOBO simply waits for some predetermined occasion or time to do its

destruction. (Peter, Kenneth, Lucasz& Michael, 2006).

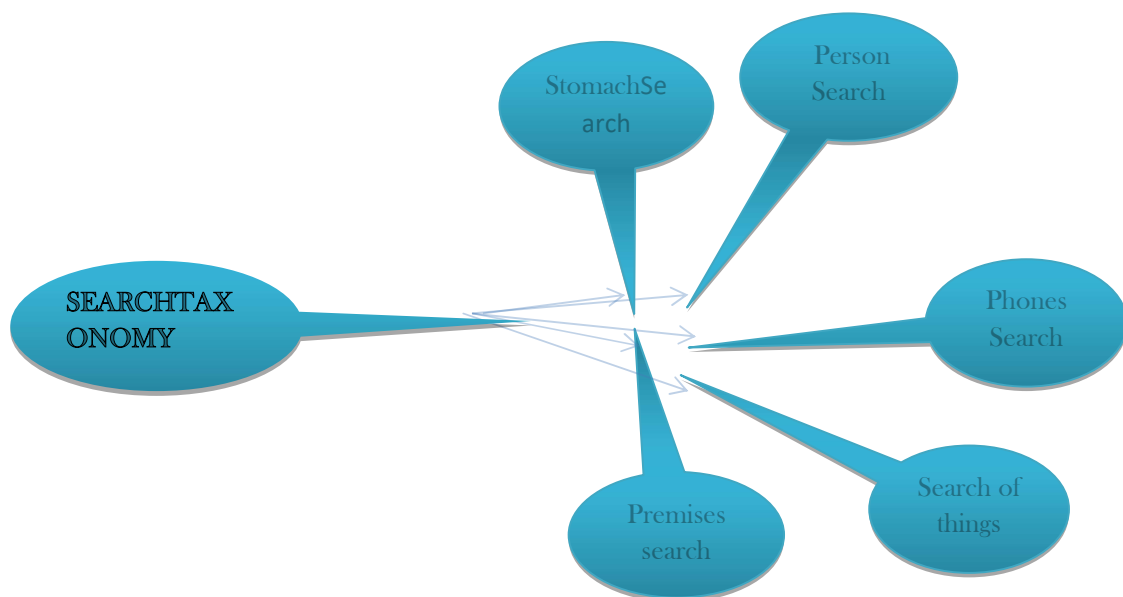Source: (author's conceptualization and compilation, 2022)

III. SEARCH AND THE POLICE

Azah, (2020) shared the view with (Alhaji, 1985) that search, connotes simply the procedure adopted by officers to recover and regain from an individual or group of persons, belongings, buildings, resources belonging to another person, or organization compulsory for the purpose of Law enforcements. Hence the police can make use of the process to recover criminal evidence, in course of their investigation, where necessary, in order to forestall the commission of crime (Alhaji, 1985). Persons and properties search by police officers (POF) is directed on a suspected person to retrieve relevant information and evidence to be consulted during trial (Afolanya, nd). Legally, the authority and right of the POF to embark or individual or property search is engrained in a number ofvalid legislations. Specifically, the current Police Act (PAT), precisely in section 28 sub-sections(1) and section 29 respectively (PAT Cap P19 LFN 2004).

Section 28 subsections (1) PAT Cap P19 LFN 2004 states that "a higherPOF possibly by power under his control empowered a POF to enter suspected apartment, stores,,buildings, other areas in quest for missing assets, and search with the intention of seizing, and securing identified property the POF deems to have been collected and possessed unlawfully. Furthermore,the POF would be authorized to embark on persons or property search upon obtaining a search warrant (SEW), and the property recovered, if any, matched the belongings labeled in such SEW. It is probable that a good number of Nigerian laws have loopholes. While section 28 mandated and provided that the POF must obtain a SEW, section 29 of the same constitution did not make compulsory a POF securing a SEW before embarking on any search. Directly, section 29 provides that a POFcan detain and search any one whom the POF reasonably suspected (RES) of possessing in his custody or carrying in any way anything which he has cause, or reason to believe to have been stolen or legitimately acquired (PAT Cap P19 LFN, 2004; Azah, 2020).However, on the contrary, professional effort had been made in explaining the component of the term reasonable suspicion. In the case between *Sarkin Kinkiba Tsoho Ladan v. Zaria Native Authority, it* was established that the term reasonable suspicion is a suspicion based on proofs, facts and evidences and not just an ambiguous notion based on traditions. Henceforth any search done on an individual lacking reasonable explanation in agreement with the act will result in an unlawful search. Justifiably, whenever anyone feels personal, premises, or phone (PPP) search carried out on him was not reasonable, the victim can seek for justice in the Court of Law.

Security Search Typology

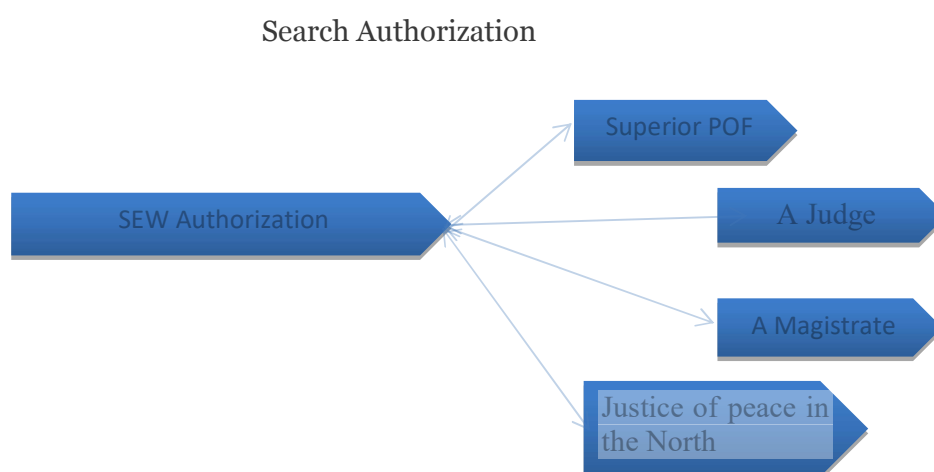*Source: (author's conceptualization, 2022).*

Exceptionally, *Body Search* is done on anyone detained and apprehended by the security agencies in association of acrime, in this context, the law permits such examination to be stretched to the suspect being medically inspected. In the same vein, *Stomach Searches* carried out on a suspect arrested in relation with being in illegal custody of hard drugs.The suspect could be exposed to stomach medical scrutiny to discover if the suspect has swallowed to his stomach some hard substances.

However, the constitutional and legislative provision appears to have fashioned a lacuna. The Sections did not explain or give an understanding to the term "Reasonable", and consequently, it is unfortunate to note that, what was preordained to be a security has unexpectedly become an opening for abusing human rights. Evidentially, the Nigerian police resulted in molesting and harassing the populace particularly the youth suspected to be a Yahoo boy. Unfortunately, the POF sometimes do probably request the suspect to transfer funds to their personal account without any reasonable suspicion.

Phone Search has become a major problem being that YAYO is now a household name majorly in the southern region of the country. This is singled out in this research because it has constituted critical debate and regular and routine practice by POF in Nigeria, particularly southern part of the country. Azah, (2020) in is summary, having scrutinized Section 45 of the CBCE Act, instituted that evidence gotten from electronic system for instance phones and laptops etc. are electronically generated evidence allowed and stated in the Act. He concluded considering past judgment like *Omisore vs. Aregbesola, and* Deepak*Babaria v. State of Gujarat* that search of electronic systems such as personal or organizational phones, Laptops etc. with the motive to acquire evidence for purpose of launching CBCE only becomes legitimate when it is executed upon the issuance of SEW issued by a judge.

Also, *Premises Search **(PPPSS)*** is a type of search conducted in a charge person's properties, goods, ware houses, or other premises. The goal of premises search is to seize any assets supposed to have been stolen or illegitimately gotten.A POP can only conduct *PPPSS* with a permission or SEW from a judge, justice of peace of the North, Magistrate, and a superior POF which must be in writing. A superior POFaccording to the Police Act (PACT)is any POF beyond the level of a Cadet assistant Superintendent of Police. In addition, Search of Things (SET) is search performed on items other than PPPSS o person's search.

Search Authorization

Source: (author's conceptualization, 2022).

Section 28(3), of the PACT contained that a superior police officer is endorsed to issue a SEW on premises on the subsequent conditions;one, in the last one year the premises is occupied by an individual earlier imprisoned of getting stolen assets or sheltering thieves. Two, the suspect is connected to fraud or corrupt dealings.SEW granted in breach of this provision is illegal. Failure to observe this legislature by a POF isa breach of one's right of private life,which is clearly entrenched under section 37 of the Constitution of the Federal Republic of Nigeria. Furthermore in the different legislature, particularly,the Administration of Criminal Justice Act, (2015) in section 146 of the Act, made provision for persons, authority, and judges who can issue SEW and these include; Judge, Magistrate and Justice of peace in the North.

The research is anchored on Dark Economy Theory (DAT). The theory first appeared in pieces of literature in 2022, in a paper titled "Central Bank of Nigeria and Nigerian Economy in the 21st Century". It was formulated by Osagioduwa LuckyOgbomo a PhD from the University of Benin. In the paper, the author highlighted that dark economy is not limited to an economy void of stable electricity and poor power supply, unexpected, unrestrained and progressive corruption and fraudulent activities. Several studies (Benford, 1938; Altman, 1968; Beneish, Etuk 2011; 1999; Digabriele, 2009; Enofe et al., 2017; Osagioduwa, 2019, 2020, 2022a, 2022b; Bhasin, 2016; Hegazy, 2017; Kolar, 2013; Quirin, 2014) had shown the reality of corruption. The DATa according toOsagioduwa (2021) is an economy where crime is uncontrolled and checked. Also, it is a free economy where the law is fading out in implementation and everyone does with it is good to him or her even at the expense of the nation and public good.Several numbers of children, youth particularly the female youth and adult had lost their lives due to Yahoo Plus. So many human parts and private parts have been harvested by these cyber criminals in quest for wealth. Some even uses their relatives for rituals. Others use ladies pants and brazes stolen from the girls or collected during sexual act for rituals. It is no longer news saying that some unemployed Nigerian youth are living in luxury from fortune acquired from CBCE.

$$¥‡†Æ \ Dark \ Economy^{pHfŋఴЖ}: \ \sum f(CBCE1^{β} \sum α+ \ corruption2^{β} : \sum α + unemployment3^{β} \sum α \ famine4^{β} \sum α + wickedness4^{β} \sum α+ \ uncontrolled \ killings5^{β} : \sum α + oppression^{β6} \sum α+ \ poor \ health \ care7^{β} \sum α + political \ violence^{β8} \sum α+ injustice^{β9} \sum α+ \ political \ foolishness^{β}10, \sum \infty α^{β................¥‡†ÆpHfŋఴЖ} μ) ==>^{ΞŸ⅖ƄI} پش—noitcurted^{⍟‡Ω}$$

The cyber fraudsters often fail to recollect that dark practices breed's destruction. Paul (58-60 AD) in his lettering to the Romans highlighted the cardinal benefit and profit of dark practices. These comprises $^{¥‡†Æ}$ *Dark Economy* ^{pHfŋఴЖ} such as *CBCE1^{β},α corruption2^{β}, α uncontrolled killings5, α poor health care7^{β}, α political foolishness^{β}, ainjustice^{β9}, α political violence^{β8}, α wickedness4^{β}and the constant 'a' with the unmentioned indices $\infty α^{β................¥‡†ÆpHfŋఴЖ}μ$ result in destruction and eternal damnation ^{ΞŸ⅖ƄI}پش—noitcurted$^{⍟}$ in a dark eternal home of the wicked. Considering the solution to dark economic practices,* Isaiah and Ezra (546-461 BC) emphasized that if upright people who are termed so will humble themselves and plead and turned from their dark practices and seek My help then I will hear from above I will forgive their CBCE and its relatives and cured their land. Meanwhile, Osagioduwa (2022)noted that the way out of a dark economy resides in a lightened economy.

IV. METHODOLOGY

The study embraces the interpretivism philosophy with the deductive theoritical approach. Methodological choice was mono quantitative

method. Copies of similar questionnaire were administered to both youths in Edo State and personnel of the Nigerian Police Force in the state. Survey strategy was adopted in this research. The opinions of respondents were sought. Cross sectional time horizon was employed. The study sought the views of two distinct sections with peculiar interpretation of cyber crime operationality namely, the youth (section A) and the police force (section B). the non-probabilistic sampling methodology was further embraced in the study.The responses from both sections were analyzed comparatively in the study. Fifty-six (56) documents were retrieved from both sectional respondents. The analysis was done using response Comparative-Percentage-Techniques (COPTA). The investigator hired the Cronbach's Alpha (CRAP) statistical instrument in determining the reliability of the study. copies of organized close-ended inquiry form (Five Likert Scales format. Strongly Agree, Agree, Undecided, Disagree and Strongly Disagree).

Model

Conceptual model

$$№ΫℲ^{CBCERD}ΫΫΫ = f\ (β_0ѡѡβ_1БΙΩ‡dыى^{stmsech}, \sum β_2Ϋ϶ϖϑπϫΦ^{bodsech}, \sum β_3β‡‡‡‡‡ДД^{thgsech}, \sum β_4غكنٟ₸₸№^{ppesech}, \sum β_5ϖϖϖℲℲⅅₚⅅₚ^{premisech}, \sum$$

$$.....aβ‡‡‡‡)...(1^{x})$$

Where:

$№ΫℲ^{CBCERD}ΫΫΫ$ = cybercrime reduction.................................(1^a)

$β_1БΙΩ‡dыى^{stmsech}$ = stomach search by the police.........................(1^b)

$β_2Ϋ϶ϖϑπϫΦ^{bodsech}$ = body search by the police.............................(1^c)

$β_3β‡‡‡‡‡ДД^{thgsec}$ = things search by the police............................(1_d)

$β_4غكنٟ₸₸№^{ppesech}$ = phone search by the police...............................1_e

$β_5ϖϖϖℲℲⅅₚⅅₚ^{premisech}$ = premises search..1_f

$a_{00}β‡‡‡‡$ = error term...1_g

Analytical model

$$№ΫℲ^{CBCERD}ΫΫΫ = β_0ѡѡβ_1БΙΩ‡dыى^{stmsech}, +β_2Ϋ϶ϖϑπϫΦ^{bodsech}, + β_3β‡‡‡‡‡ДД^{thgsech}, + β_4غكنٟ₸₸№^{ppesech}, +$$

$$β_5ϖϖϖℲℲⅅₚⅅₚ^{premisech}, + ...aβ‡‡‡‡)...(1_{y})$$

4.1 Descriptive Statistics

Section A

55.0 percent of the youth respondents were female while 45.0 percent of the youth respondents where male. Furthermore, 20.0 percent are in ages 16 to 20 years, while 57.50 percent were between 21 and 30 years old. Those in age range of 31 to 40 years constitute 22.50 percent of the total respondents. Similarly, 52.50 percent where student of tertiary education, 40.0 percent where self-employed students, 2.50 percent made up dependent students, and 5.0 percent represent other group of students.

Comparative Percentage Analysis (CPA)

Question 1

Large numbers of Nigerian youth are not involved in cybercrime.

Section B: Response from the police
6.30 percent of the police respondents agreed, 12.50 percent strongly agreed, 6.30 percent could not decide, 62.5 percent disagreed, while 12.50 percent strongly disagreed that Large numbers of Nigerian youth are not involved in cybercrime

Section A: youth responses

17.50 percent of the youth respondents agreed, 35.0 percent strongly agreed, 7.50 percent could not decide, 20.0 percent disagreed, while 20.0 percent strongly disagreed that Large numbers of Nigerian youth are not involved in cybercrime.

Question 2

Cybercrime had become the only means of livelihood of several Nigerian youth

Section B   Response from the police

6.30 percent of the police respondents agreed, 68.80 percent strongly agreed, 6.30 percent could not decide, while 18.80 percent strongly disagreed that Cybercrime had become the only means of livelihood of several Nigerian youth

Section A: youth responses

15.00 percent of the youth respondents agreed, 32.50 percent strongly agreed, 2.50 percent could not decide, 30.0 percent disagreed, and 20.0 percent strongly disagreed that Cybercrime had become the onl means of livelihood of several Ni erian outh .

Question 3

Lack of government plan for the youth as increase the height of cybercrime in Nigeria society

Section B Response from the police

68.80 percent of the police respondents agreed, 31.30 percent strongly agreed that lack of government plan for the youth as increase the height of cybercrime in Nigeria society,

Section A: youth responses

57.50 percent of the youth respondents agreed, 27.50 percent strongly agreed, 7.50 percent could not decide, 5.0 percent disagreed, and 2.50 percent strongly disagreed that lack of government plan for the outh as increase the hei ht of c bercrime in Ni eria societ .

Question 4

You have been search not less than twice in the last two months by the Nigerian police.

Section A: youth responses

20.0 percent of the youth respondents agreed, 12.50 percent strongly agreed, 5.0 percent could not decide, 25.0 percent disagreed, and 37.50 percent strongly disagreed that they have been search not less than twice in the last two months by the Nigerian police.

Section B Response from the police

6.30 percent of the police respondents agreed, 12.50 percent strongly agreed, 18.8 percent could not decide, 62.5 percent disagreed, and 6.30 percent strongly disagreed that they have search an individual not less than twice in the last two months.

Question 5

Those involved in cybercrime are easily recognized by their appearance

Section B   Response from the police

6.30 percent of the police respondents agreed, 6.30 percent strongly agreed, 12.50 percent could not decide, 56.30 percent disagreed, and 18.80 percent strongly disagreed that those involved in cybercrime are easily recognized by their appearance

Section A: youth responses

37.50 percent of the youth respondents agreed, 22.50 percent strongly agreed, 2.50 percent could not decide, 27.50 percent disagreed, and 10.0 percent strongly disagreed that those involved in cybercrime are easily recognized by their appearance

Question 6

Nigerian police upon search of a cybercrime suspect phone, request for immediate transfer into his or her personal account before discharging a suspect

Section A: youth responses

35.0 percent of the youth respondents agreed, 35.0 percent strongly agreed, 17.50 percent could not decide, 5.0 percent disagreed, and 7.5 percent strongly disagreed that Nigerian police upon search of a cybercrime suspect phone, request for immediate transfer into his or her personal account before discharging a suspect.

Section B Response from the police

6.30 percent strongly agreed, 25.0 percent could not decide, while 68.8 percent strongly disagreed that Nigerian police upon search of a cybercrime suspect phone, request for immediate transfer into his or her personal account before discharging a suspect.

Cybercrime Schemes and Search by the Police

Nigerian police often stop youths on the way and demand for the phones for search

Section B Response from the police

56.30 percent of the police respondents agreed, 12.50 percent strongly agreed, 18.80 percent could not decide, 6.30 percent disagreed, and 6.30 percent strongly disagreed that Nigerian police often stop youths on the way and demand for the phones for search.

Section A: youth responses

57.5 percent of the youth respondents agreed, 37.50 percent strongly agreed, 2.50 percent could not decide, and 2.50 percent strongly disagreed that Nigerian police often stop youths on the way and demand for the phones for search.

Question 8

Nigerian police contribute to the growth of cybercrime in Nigeria

Section A: youth responses

37.50 percent of the youth respondents agreed, 15.0 percent strongly agreed, 30.0 percent could not decide, 15.0 percent disagreed, and 2.50 percent strongly disagreed that Nigerian police contribute to the growth of cybercrime in Nigeria.

Section B Response from the police

56.30 percent of the police respondents agreed, 6.30 percent strongly agreed, 6.30 percent could not decide, 18.8 percent disagreed, and 12.50 percent strongly disagreed that Nigerian police contribute to the growth of cybercrime in Nigeria.
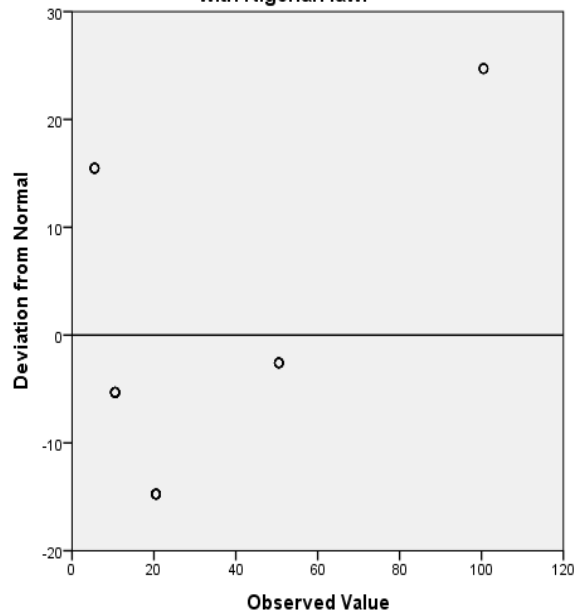
Question 9

Cybercrime suspect are usually prosecuted in line with Nigerian law.

Section B Response from the police

12.50 percent of the police respondents agreed, 12.50 percent strongly agreed, 37.50 percent disagreed, and 37.50 percent strongly disagreed that cybercrime suspect are usually prosecuted in line with Nigerian law.

Section A: youth responses

17.50 percent of the youth respondents agreed, 30.0 percent strongly agreed, 22.50 percent could not decide, 20.0 percent disagreed, and 10.0 percent strongly disagreed that cybercrime suspect are usually prosecuted in line with Nigerian law.

Detrended Normal Q-Q Plot of Cybercrime suspect are usually prosecuted in line with Nigerian law.

Question 10

Appearance of an individual usually gives the police the impression of who is a cybercrime suspect
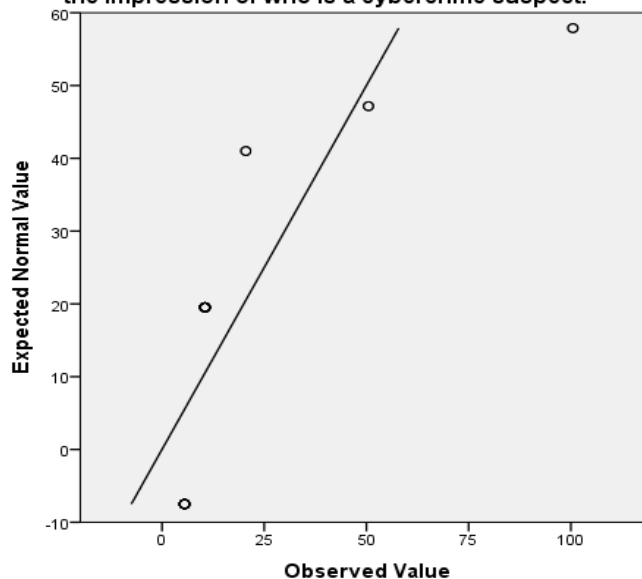
Section A: youth responses

27.50 percent of the youth respondents agreed, 57.50 percent strongly agreed, 5.0 percent could not decide, 5.0 percent disagreed, and 5.0 percent strongly disagreed that the appearance of an individual usually gives the police the impression of who is a cybercrime suspect.

Section B Response from the police

75.0 percent of the police respondents agreed, 18.80 percent strongly agreed, 6.3 percent disagreed appearance of an individual usually gives the police the impression of who is a cybercrime suspect.

Normal Q-Q Plot of Appearance of an individual usually implies gives the police the impression of who is a cybercrime suspect.

Cybercrime Schemes and Search by the Police

Searching one's personal phone by the police is necessary to curb the rate of cybercrime in Nigeria society

Section B   Response from the police
25.0 percent of the police respondents agreed, 56.3 percent strongly agreed, 6.30 percent disagreed, and 12.50 percent strongly disagreed that searching one's personal phone by the police is necessary to curb the rate of cybercrime in Nigeria society

Section A: youth responses

20.0 percent of the youth respondents agreed, 12.50 percent strongly agreed, 17.50 percent could not decide, 22.50 percent disagreed, and 27.50 percent strongly disagreed that searching one's personal phone by the police is necessary to curb the rate of cybercrime in Nigeria society.

Question 11

Nigeria police are not knowledgeable of the various techniques employed in perpetuating cybercrime in Nigeria

Section A:youth responses

35.50 percent of the youth respondents agreed, 37.50 percent strongly agreed, 17.50 percent could not decide, 7.50 percent disagreed, and 2.50 percent strongly disagreed that Nigeria police are not knowledgeable of the various techniques employed in perpetuating cybercrime in Nigeria.

Section B Response from the police

50.0 percent of the police respondents agreed, 12.50 percent strongly agreed, 25.0 percent could not decide, and 12.50 percent disagreed that Nigeria police are not knowledgeable of the various techniques employed in perpetuating cybercrime in Nigeria.

Question 12

Cybercrime cannot be curtailed or reduce by the current Nigeria police despite all their training.

Section B Response from the police

37.50 percent of the police respondents agreed, 12.50 percent strongly agreed, 12.5 percent could not decide, and 37.50 percent disagreed that Cybercrime cannot be curtailed or reduce by the current Nigeria police despite all their training.

Section A: youth responses
37.50 percent of the youth respondents agreed, 32.50 percent strongly agreed, 17.50 percent could not decide, 2.50 percent disagreed, and 10.0 percent strongly disagreed that Cybercrime cannot be curtailed or reduce by the current Nigeria police despite all their training.

Question 13

The Nigerian police need a cybercrime unit, department or division to effectively fight cybercrime in Nigeria

Cybercrime Schemes and Search by the Police

Section A: youth responses

35.50 percent of the youth respondents agreed, 37.50 percent strongly agreed, 10.0 percent could not decide, 10.0 percent disagreed, and 7.0 percent strongly disagreed that the Nigerian police need a cybercrime unit, department or division to effectively fight cybercrime in Nigeria.

Section B Response from the police

75.0 percent of the police respondents agreed, 37.50 percent strongly agreed, 6.3 percent could not decide, and 6.3 percent disagreed that the Nigerian police need a cybercrime unit, department or division to effectively fight cybercrime in Nigeria.

Question 14

All teenager driving expensive cars are usually first suspect of cybercrime activities.

Section A: youth responses

17.50 percent of the youth respondents agreed, 47.50 percent strongly agreed, 5.0 percent could not decide, 17.50 percent disagreed, and 12.50 percent strongly disagreed that all teenager driving expensive cars are usually first suspect of cybercrime activities.

Section B Response from the police

43.80 percent of the police respondents agreed, 31.30 percent strongly agreed, and 6.3 percent disagreed that all teenager driving expensive cars are usually first suspect of cybercrime activities

IV.   SUMMARY, CONCLUSION AND RECOMMENDATION

It was discovered from the analysis that a good number of teenager driving expensive cars are usually first suspect of CBCE activities. However, 22.5 percent of teenager driving expensive cars are not usually first suspect of CBCE activities. It was further found from the analysis that the Nigerian police need a CBCE unit to effectively fight CBCE in Nigeria. Meanwhile, 11.25 percent of the total respondents do not concur that Nigerian police need a CBCE unit to effectively fight CBCE in Nigeria. Also, result revealed that Nigeria police are not knowledgeable of the various techniques employed in perpetuating CBCE in Nigeria. Just 11.25 percent of Nigeria police are knowledgeable of the various techniques employed in perpetuating CBCE in Nigeria. Further findings showed that CBCE cannot be curtailed or reduce by the current Nigeria police despite all their training. Nevertheless, product from the survey indicates that 25 percent of CBCE can be curtailed when the police officers are trained adequately.

In the same vein, outcome also indicates that appearance of an individual usually gives the police the impression of who is a CBCE suspect. But further findings expose that 8.15 percent of CBCE players are of good, moral, and generally acceptable physical appearance. In addition, further consequence of the comparative percentage analysis revealed that that Nigerian police contribute to the growth of CBCE in Nigeria. The rationale behind this finding might by probably a function of the result of 50.56 percent Nigerian police upon search of a CBCE suspect phone, request for immediate transfer into their personal account before discharging a suspect. Also, consequence from the analysis showed that Nigerian police often stop youths on the way to demand for the phones for search. Further analysis should that lack of government plan for the youth as increase the height of CBCE in Nigeria society. Similarly, it was also discovered that 3.5 percent of the youth will engage in CBCE even when the government plans and ensure high standard of living for its young adult.Sumanjit and Tapaswini (2013) highlighted the survey piloted by the Computer Security Institute (CSI)

in unification with the U.S. Federal Bureau of Investigation's International Computer Crime Squad (CSI/FBI), indicated fiscal losses resulting from computer breaches amount to over US$ 52m in 2006, an amount that is down 30% from the over US$ 141m recounted in 2004.

The study therefore recommends that

1. The police force should the educated on the 21st century cybercrime scheme. The training should be both local and global best practice.
2. The government should increase the annual budget of the police force.
3. Nigeria government should make adequate provision and economic plan for it teaming youth.

REFERENCES

1. Afolanya, A. F. (nd). 'Criminal Litigation in Nigeria' 3rd edition Chengo Law publication Limited.
2. Ahmet, N. (2014). Challenges in combating the cyber crime. Mediterranean Journal of Social Sciences .5 (19). 592-599. DOI:10.5901/ mjss.2014. v5n19p592
3. Ajayi, E. F. G. (2016). Challenges to enforcement of cyber-crimes laws and policy.Journal of Internet and Information Systems, 6 (1), 1-12. DOI 10.5897/ JIIS2015. 0089.http://www.academicjournals.org/JIIS
4. Alhaji A. A. (1985). 'Searches and seizure in Nigeria with particular reference to the Northern states' a thesis submitted to the postgraduate school, Ahmadu Bello University, Zaria. Iv
5. Anca, B., Claudiu G. B., Mara, D. B., Lucian, M., Leonardo, G. M., & Catalina, S. S. (2021).Including Sustainable Reporting Practices in Corporate Management Reports: Assessing the Impact of Transparency on Economic Performance. Sustainability, 13, (940) 1-20. https://doi.org/10.3390/su1 3020940.
6. Andrea, T., Florian, H., Bernhard,J., Jo, D.,Emmanouil, V., & Max, M. (2018).Challenges and available solutions against organized cyber-crime and terroristNetworks. Safety and Security Engineering 7 (174), 429-441. doi: 10.2495/ SAFE170391.
7. Asad, M. & Ghulam, S. (2018). Social Media and Cyber Crimes in Pakistan: Facts, Propaganda, Awareness, and Legislation. Global Political Review (GPR), Pages: 3(2), 84 – 97. From URL: http://dx.doi.org/10.31703/ gpr.2018 (III-II).09. DOI: 10.31703/ gpr.2018 (III-II).09
8. Azah, A. A. (2020). *International Journal of Law*.Effect of the cybercrime act on the police power of search in Nigeria, 6 (4), 261-263. www. lawjournals.org.
9. Cameron S. D. B. (2015). Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice. International Journal of Cyber Criminology, 9 (1).
10. Courtice, E. L., Shaughnessy, K. (2017). "Technology-mediated sexual interaction and relationships: a systematic review of the literature". Sexual and Relationship Therapy. 32 (3–4): 269–290. doi:10.1080/14681994. 2017. 1397948. S2 CID 149040678.
11. Döring, N. (2000). "Feminist Views of Cybersex: Victimization, Liberation, and mpowerment". CyberPsychology & Behavior. 3 (5): 863–884. doi:10.1089/109493100501 91845.
12. Farzana, B. (2019). Beware of Cyber Crime with Awareness - A Review. International Journal of Science and Healthcare Research, .4 (3), 135-138.
13. Hahn, Harley (1996). The Internet Complete Reference (2nd ed.). Osborne McGraw-Hill.p. 570.ISBN 0-07-882138-X.
14. Hinduja, S. & Patchin, J. W. (2019). Summary of Our Cyberbullying Research (2007-2019) Cyberbullying Research Center. Retrieved from https://cyberbullying.org/2019-cyber bullying-data
15. Igba, D. I., Elizabeth, C. I., Aja S. N., Simon, C. N., Egbe, E. U.,&Ogodo, J. V., (2018). Cybercrime among University Undergraduates: Implications on their Academic Achievement. International Journal of Applied Engineering Research, 13, (2) 1144-1154. Available from http://www.ripu blication.com

16. Maitanmi, O., Ogunlere., S, Ayinde, S., & Adekunle, Y. (2013). Cyber Crimes and Cyber Laws in Nigeria .The International Journal Of Engineering And Science (IJES), 2(4), 19-25.

17. Manila Bulletin. (May 1, 2020). Norwegian national, partner nabbed; 4 rescued from cybersex den.

18. Maziah, M. A, (2016).Determinants of Preventing Cyber Crime: a Survey Research, International Journal of Management Science and Business Administration, 2, (7), 16-24. From URL: dx.doi.org/10.18775/ijmsba .1849-5664-5419.2014.27.1002.DOI:10.18775/ijmsba.1849-5664 -5419. 2014.27.1002

19. Moga, E., Salihu, A. G., &Abdulkarim, R. (2021).A Historical Assessment of Cybercrime in Nigeria: Implication for Schools and National Development. Journal of Research in Humanities and Social Science, 9 (9), 84-94. Available from www.questjournals.org

20. NBC News. (June 30, 2018). Cheap tech and widespread internet access fuel rise in cybersex trafficking".

21. Olusi, F. I., Aguele, L.I. ,Ihumuaibvi, P.O.,& Edobor, R. I. (2009). Students Perception of Cyber Crime in Edo State: Implications for Teaching and Learning, Journal of Contemporary Research 6 (1), 90-96.

22. Osagioduwa, L. O. (2019). The effectiveness of the whistle blowing policy in combating corruption in the Nigerian public sector. *Global Journal of Arts Humanities and Social Science*. 7 (10), 77-98.

23. Osagioduwa, L. O. (2022). Assessment of challenges of public auditor's independence and report in the public sector of Nigeria.Amity Journal of management research. 5 (1), 70-87.

24. Osagioduwa, L. O. (2022b). Assessment of challenges of public auditor's independence and report in the public sector of Nigeria.Amity Journal of management research. 5(1), 70-87

25. Osagioduwa, L. O., Ese, T. E., & Ogudo, O. S. (2022). Post employment benefit: a comparative assessment of the central bank and the police force retirees. London journal of research in management and business. 22(5),1-27.

26. Osagioduwa, L. O., Mozie, E. P., Ogudo, O. S., & Uyi. N. (2022). Government anti-corrupt instruments unity and prosecution of corrupt public officers. The accounting practitioners' perspective.Nigerian journal of management science. 23(2), 29-45.

27. Osagioduwa, L. O., Ogudo, O. S., &Oloye, F. (2022).central bank of Nigeria and the Nigerian economy in the 21st century. Journal of accounting and management, 12(2), 59-76.

28. Osagioduwa, L. O., Ojiakor, I., Esenobor. E. T.,& Odiachi. L. (2022a).Fraud scheme and fraudulent accountant prosecution. *International Journal of Academic Research in Business and Social Science.*12(1), 1143-1169.

29. Osagioduwa, L. O., Uyi. N., Ogudo, O. S., &Mozie, E. P. (2022). Effective auditors, systematic corruption and the EGAD report: the way forward. Gusau journal of accounting and finance. 3(2), 1-31

30. Osagioduwa, L., O. (2019b). Treasury single account effectiveness on corruption control and public organizations efficient administration in Nigeria. *International Journal of Management Studies and Social Science Research*. 1 (5), 1-19.

31. Osagioduwa, L.O., Okeke, S. E., &Ohidoa, T. (2020).Public auditors and detection of corruption in Nigeria. *International journal of social and management science*. 3(2),49-57

32. Paek, S.-Y.; Nalla, M.K.;Chun, Y.-T.; Lee, J. (2021). The Perceived Importance of Cybercrime Control Among Police Officers: Implications For Combatting Industrial Espionage.

33. Peter, C. P., Kenneth, M., Lucasz, P. T., &. Michael, W. (2006). SPAMALOT: A Toolkit for Consuming Spammers Resources. Proceedings of the 3rd Conference on E-mail and Antispam. Available online at www. ceas.org. Police Act Cap P19 LFN 2004.

34. Pratt, M. K. (2022). What is a Cyber Attack? Definition, Examples and Prevention. Available from https://www.techtarget.com/search security /definition/cyber-attack.

35. Reuters, (April 15, 2019). "Global taskforce tackles cybersex child trafficking in the Philippines.

Cybercrime Schemes and Search by the Police

36. Reuters, (June 17, 2018). Webcam slavery: tech turns Filipino families into cybersex child traffickers.

37. South China Morning Post. (May 2, 2019). ^How the internet fuels sexual exploitation and forced labour in Asia"

38. South China Morning Post. (September 11, 2019). Cybersex trafficking spreads across Southeast Asia, fuelled by internet boom. And the law lags behind".

39. Sumanjit, D. & Tapaswini, N, (2013). Impact of cyber crime: issues and challenges. International Journal of Engineering Sciences & Emerging Technologies, 6, (2), 142-153

40. Sustainability 2021, 13, 4351. https://doi.org/ 10.3390/su13084351

41. The ASEAN Post, (October 18, 2019) Duterte's drug war and child cybersex trafficking".

42. The Philippine Star. (April 13, 2020). Senator warns of possible surge in child cybersex traffic.

43. The Philippine Star. (November 11, 2019). "Senate to probe rise in child cybersex trafficking.

44. UNODC, (2021).Report on the meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime held in Vienna from 6 to 8 April 2021. 2-11.

45. Vishi, A., Shruti, M. S., (2018). Cybercrime victims: a comprehensive study. International Journal of Creative Research Thoughts. 6 (2), 640-648.

46. VOA. (May 12, 2017). Philippines Makes More Child Cybersex Crime Arrests, Rescues"

Cybercrime Schemes and Search by the Police

London Journals Press membership is an elite community of scholars, researchers, scientists, professionals and institutions associated with all the major disciplines. London Journals Press memberships are for individuals, research institutions, and universities. Authors, subscribers, Editorial Board members, Advisory Board members, and organizations are all part of member network.

Read more and apply for membership here:
https://journalspress.com/journals/membership

For Authors

For Institutions

For Subscribers

Author Membership provide access to scientific innovation, next generation tools, access to conferences/seminars /symposiums/webinars, networking opportunities, and privileged benefits.
Authors may submit research manuscript or paper without being an existing member of LJP. Once a non-member author submits a research paper he/she becomes a part of "Provisional Author Membership".

Society flourish when two institutions come together." Organizations, research institutes, and universities can join LJP Subscription membership or privileged "Fellow Membership" membership facilitating researchers to publish their work with us, become peer reviewers and join us on Advisory Board.

Subscribe to distinguished STM (scientific, technical, and medical) publisher. Subscription membership is available for individuals universities and institutions (print & online). Subscribers can access journals from our libraries, published in different formats like Printed Hardcopy, Interactive PDFs, EPUBs, eBooks, indexable documents and the author managed dynamic live web page articles, LaTeX, PDFs etc.

JOURNAL AVAILABLE IN

PRINTED VERSION, INTERACTIVE PDFS, EPUBS, EBOOKS, INDEXABLE
DOCUMENTS AND THE AUTHOR MANAGED DYNAMIC LIVE WEB PAGE
ARTICLES, LATEX, PDFS, RESTRUCTURED TEXT, TEXTILE, HTML, DOCBOOK,
MEDIAWIKI MARKUP, TWIKI MARKUP, OPML, EMACS ORG-MODE & OTHER

support@journalspress.com
www.journalspress.com

*THIS JOURNAL SUPPORT AUGMENTED REALITY APPS AND SOFTWARES