

CrossRef DOI of original article:

1 Scan to know paper details and author's profile

2

3 *Received: 1 January 1970 Accepted: 1 January 1970 Published: 1 January 1970*

4

5 **Abstract**

6

7 *Index terms—*

8 **1 INTRODUCTION**

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

17 Weighing strategically the actuality of CBCE Brenner ??2001, ??004) asserted that CBCE is a divergent
18 category of criminality from a law perception. All form of CBCE has a counterpart crime in the physical world.
19 For example, vandalism can be seen as the tangible world correspondence of hacking (Petee, Corzine, Huff-
20 Corzine, Clifford, and Weaver, 2010). However, disjointedness exists between real-life Yar (2005) criminalities
21 and cybernetic crimes. ??ar (2005) further debated that computergenerated space builds exceptional openings
22 for the commission of the novel category of criminalities; such crime cannot be executed in the physical world.
23 Furthermore, Wall (2017a, agreement with NBPC submission noted that CBBULL is when an individual
24 constantly and calculatedlyteases, mistreats, or makes amusement of a targeted person online, employing cell
25 phones or automated garget.

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

31 YahooYahoo (YAYO): YAYOentails perpetrating online frauds scheme that range from identity credit card
32 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
33 defraud others nationally or internationally using various means largely the Facebook handle.

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

38 Cyber SEX (CBSXXX): Nicola (2000) debated CBSXXX is same as Internet sex, computer sex, netsex and,
39 cyber or cybering, colloquially, is a computer-generated sex happenstance in which more than one individual
40 inkeddistantly via computer system exchange sexually unambiguous messages unfolding a sexual involvement.
41 Furthermore, CBSXXX is a sub-type of technology-mediated sexual interactions. Eventually, ??arley (1996)added
42 clearly that CBSXXX also involves real life masturbation. ??arley (1996) added that the quality of a CBSXXX
43 encounter classicallyis contingent upon the participants' emotional capacities to arouse a glowing, intuitive
44 mental picture in the thoughts and Imagination of their buddies. CBSXXX can arisebetween lovers who are
45 physicallydistant or among persons with no erstwhile knowledge of each other and meet in virtual spaces and
46 may even be unknown to each other. In some environments,CBSXXX is heightened by the use of a webcam to
47 diffuse real-time video of the partners.

6 MONEY LAUNDERING AND TAX EVASION (MLTA):

48 Cyber Trafficking (CBSXXT): IJM, (2020) and CNN (2013) asserted that CBSXXT is the live streaming of
49 forced sexual performances and or an outright rape. Targets are kidnapped, threatened, or mislead and conveyed
50 to CBSXXX dens. The Philippine Star, (2020), ASEAN Post (2019) and Manila Bulletin (2020) noted that the
51 CBSXXX dens can be in several setting where the CBSXXX traffickers have access to the tablet, computer, or
52 phone with internet network. IJM(2020) added firmly that players use pornographic video sharing websites, social
53 media connections, videoconferences, online chat rooms, dating pages, dark web sites (NBC, 2018), and other
54 platforms. Also, Philippine, (2019) remarked that they use online payment systems (NBC News, 2018& Reuters
55 2019) and cryptocurrencies to hide their personalities. Furthermore, South China Morning Post ??2019] added
56 that Loads of reports of CBSXXT happenings are referred to authorities yearly. Meanwhile, VOA,(2017) and
57 the South China Morning Post (2019), highlighted vividly fresh regulations and constabularies procedures are
58 needed to fight this type of CBCE.

59 2 Vishing (VSH):

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

64 3 Smishing (MSH):

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

68 4 Phishing (PSH):

69 PSH involves the practice of sending emails purporting to be from reputable London Journal of Research in
70 Management and Business establishments with the intent to induce targeted persons to expose and secret
71 particular information, such as passwords, PIN, and credit card information. Furthermore, PSH is the trick of
72 hoodwinking Internet users through deceptive email messages into revealing private or personal statistics which
73 can then be used dishonestly(<https://www.merriam-webster.com/dictionary>).

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

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

79 5 Access Crime (ACCE): ACCE means gaining access into 80 another person computer without awareness (Osagioduwa 81 2022).

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

83 6 Money Laundering and Tax Evasion (MLTA):

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

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

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

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

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

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

104 **7 Virus Dissemination (VIDIS):**

105 VIDIS is a deliberate practice of sending malicious software that fastens and join itself to target software. Trojan
106 horse, Virus, Time bomb, Logic Bomb, worms, Rabbit and Bacterium are samples of malicious software that
107 damages the computer software of the victim. (<http://alphasquadblogging.blogspot.com/2016/12/vi>)
108 (PAMI): PAMI is the fraudulent exercise of pointing internet users to a counterfeit website that has the form of a
109 genuine website, in order to acquire delicate figures such as passwords, PINs, account numbers, etc. furthermore,
110 abroundly used PAMI description is cyber fraud that comprises the engagement of malicious program to connect
111 victims to hoaxed websites in an effort to collect their relevant and personal information, credentials, and data.
112 (<https://www.fortinet.com/resources/cyberglossary/pharming>)

113 **8 Hoaxes (HES):**

114 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 abround
115 consequences. HES give the criminals ego gratification as they see their scheme grow through the Internet. Frauds
116 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)
117 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
118 processing of the altered data results in a fraudulent benefit (<https://www.google.com/search?client>)
119 Illegal Interception of Telecommunications (IITE): IITE involves gaining access to the signal, collecting the signal, and
120 exfiltration of the signal (Purpura, 2013).

123 **9 Cybersquatting (CUT):**

124 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>).

125 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.

126 Similarly, EMACoften take the shape of a "con game", or scam (<https://www.google.com/search?client>).

127 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>).

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

136 **10 Aiding and Abating**

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

138 ? 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).

139 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).

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

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

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

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

155 **11 Domain Name System (DNS) Tunneling (DNST):**

156 DNSTis a refined attack wherein hackers launch and then use untiringly, existing access or a tunnel into their
157 targets' systems (Pratt, 2022).

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

160 Credential-Based Attacks (CBA): CBA occur when cyber attackers steal the credentials that ITpersonnel uses
161 to open, operate and administers a computer system and then use the stolen data to illegally access the victim
162 computers to collect secret data, disrupt an entity, and its processes (Pratt, 2022).

163 **12 Credential Stuffing (CRS):**

164 CRSresults when cyber intruders employs compromised login permits, for instance email and password to access
165 a targeted systems (Pratt, 2022).

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

169 **13 Malware (MAW):**

170 MAW refers to viruses, Trojans, worms and other software that gets onto your computer without your knowledge.

171 LogicBombs (LOBO): LOBOcommands the computer system to implement a particular command at a definite
172 date and time or under certain speculated situations. The specified commands or orders might require the
173 computer to reveal a verification technique on the screen;LOBO can instruct the computer to start deleting its
174 files. LOBO often works similar to viruses. While a virus contaminates a given computer program after which
175 reproduces when the computer program begins to run, the LOBO does not replicate. LOBO simply waits for
176 some predetermined occasion or time to do its Azah, (2020) shared the view with (Alhaji, 1985) that search,
177 connotes simply the procedure adopted by officers to recover and regain from an individual or group of persons,
178 belongings, buildings, resources belonging to another person, or organization compulsory for the purpose of
179 Law enforcements. Hence the police can make use of the process to recover criminal evidence, in course of
180 their investigation, where necessary, in order to forestall the commission of crime ??Alhaji, 1985). Persons and
181 properties search by police officers (POF) is directed on a suspected person to retrieve relevant information and
182 evidence to be consulted during trial (Afolanya, nd). Legally, the authority and right of the POF to embark or
183 individual or property search is engrained in a number of valid legislations. Specifically, the current Police Act
184 (PAT), precisely in section 28 sub-sections(1) and section 29 respectively (PAT Cap P19 LFN 2004).

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

202 **14 Security Search Typology**

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

204 **15 III. SEARCH AND THE POLICE**

205 **16 Person Search**

206 **17 Search of things**

207 Phones Search

208 18 Premises search

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

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

220 Phone Search has become a major problem being that YAYO is now a household name majorly in the southern
221 region of the country. This is singled out in this research because it has constituted critical debate and regular
222 and routine practice by POF in Nigeria, particularly southern part of the country. Azah, (2020) in is summary,
223 having scrutinized Section 45 of the CBCE Act, instituted that evidence gotten from electronic system for
224 instance phones and laptops etc. are electronically generated evidence allowed and stated in the Act. ??021) is
225 an economy where crime is uncontrolled and checked. Also, it is a free economy where the law is fading out in
226 implementation and everyone does with it is good to him or her even at the expense of the nation and public
227 good. Several numbers of children, youth particularly the female youth and adult had lost their lives due to Yahoo
228 Plus. So many human parts and private parts have been harvested by these cyber criminals in quest for wealth.
229 Some even uses their relatives for rituals. Others use ladies pants and brazes stolen from the girls or collected
230 during sexual act for rituals. It is no longer news saying that some unemployed Nigerian youth are living in
231 luxury from fortune acquired from CBCE.

232 19 ¥ ? ?? Dark Economy

233 " : ? f(CBCE1 ? ? ? + corruption2 ? ? ? + unemployment3 ? ? ? famine4 ? ? ? + wickedness4 ? ? ? +
234 uncontrolled killings5 ? : ? + oppression ?6 ? ? + poor health care7 ? ? ? + political violence ?8 ? ? + injustice
235 ?9 ? ? + political foolishness ? 10, ? ? ? ??????¥ ? ??????" μ) ==> ?İ?"??", ? ? ? noitcurtsed ? ? ?

236 The cyber fraudsters often fail to recollect that dark practices breed's destruction. Paul (58-60 AD) in his
237 lettering to the Romans highlighted the cardinal benefit and profit of dark practices. These comprises Considering
238 the solution to dark economic practices, Isaiah and Ezra (546-461 BC) emphasized that if upright people who
239 are termed so will humble themselves and plead and turned from their dark practices and seek My help then I
240 will hear from above I will forgive their CBCE and its relatives and cured their land. Meanwhile, Osagioduwa
241 (2022) noted that the way out of a dark economy resides in a lightened economy.

242 The study embraces the interpretivism philosophy with the deductive theoretical approach. Methodological
243 choice was mono quantitative

244 20 IV. METHODOLOGY

245 Model ?İ?"? CBCERD İ?"İ?"İ?" =f (?0?????1?" ? ??"????? stmsech , ? ?2İ?"????? bodsech , ? ?3? ? ? ? ?
246 ?D?"D?" thgsech , ? ?4 ??? ppesech , ? ?5 ?????? premisech , ? ?..a? ? ? ? ? ?)??????????????????????????????.(1
247 x)

248 Where: Section B: Response from the police 6.30 percent of the police respondents agreed, 12.50 percent
249 strongly agreed, 6.30 percent could not decide, 62.5 percent disagreed, while 12.50 percent strongly disagreed
250 that Large numbers of Nigerian youth are not involved in cybercrime Section A: youth responses 17.50 percent of
251 the youth respondents agreed, 35.0 percent strongly agreed, 7.50 percent could not decide, 20.0 percent disagreed,
252 while 20.0 percent strongly disagreed that Large numbers of Nigerian youth are not involved in cybercrime. ?İ?"?
253 CBCERD İ?"İ?"İ?" = cybercrime

254 Section B Response from the police 6.30 percent of the police respondents agreed, 68.80 percent strongly agreed,
255 6.30 percent could not decide, while 18.80 percent strongly disagreed that Cybercrime had become the only means
256 of livelihood of several Nigerian youth Section A: youth responses 15.00 percent of the youth respondents agreed,
257 32.50 percent strongly agreed, 2.50 percent could not decide, 30.0 percent disagreed, and 20.0 percent strongly
258 disagreed that Cybercrime had become the onl means of livelihood of several Ni erian outh .

259 Section B Response from the police 68.80 percent of the police respondents agreed, 31.30 percent strongly
260 agreed that lack of government plan for the youth as increase the height of cybercrime in Nigeria society,

261 21 Question 4

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

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

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

269 Question 5

270 **22 Those involved in cybercrime are easily recognized by their
271 appearance**

272 Section B Response from the police 6.30 percent of the police respondents agreed, 6.30 percent strongly agreed,
273 12.50 percent could not decide, 56.30 percent disagreed, and 18.80 percent strongly disagreed that those involved
274 in cybercrime are easily recognized by their appearance Section A: youth responses 37.50 percent of the youth
275 respondents agreed, 22.50 percent strongly agreed, 2.50 percent could not decide, 27.50 percent disagreed, and
276 10.0 percent strongly disagreed that those involved in cybercrime are easily recognized by their appearance
277 Question 6

278 **23 Nigerian police upon search of a cybercrime suspect phone,
279 request for immediate transfer into his or her personal
280 account before discharging a suspect**

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

285 Section B Response from the police 6.30 percent strongly agreed, 25.0 percent could not decide, while 68.8
286 percent strongly disagreed that Nigerian police upon search of a cybercrime suspect phone, request for immediate
287 transfer into his or her personal account before discharging a suspect. Section A: youth responses 57.50 percent of
288 the youth respondents agreed, 27.50 percent strongly agreed, 7.50 percent could not decide, 5.0 percent disagreed,
289 and 2.50 percent strongly disagreed that lack of government plan for the outh as increase the hei ht of c bercrime
290 in Ni eria societ .

291 Question 7

292 **24 Nigerian police often stop youths on the way and demand
293 for the phones for search**

294 Section B Response from the police 56.30 percent of the police respondents agreed, 12.50 percent strongly agreed,
295 18.80 percent could not decide, 6.30 percent disagreed, and 6.30 percent strongly disagreed that Nigerian police
296 often stop youths on the way and demand for the phones for search.

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

300 Question 8

301 **25 Nigerian police contribute to the growth of cybercrime in
302 Nigeria**

303 Section A: youth responses 37.50 percent of the youth respondents agreed, 15.0 percent strongly agreed, 30.0
304 percent could not decide, 15.0 percent disagreed, and 2.50 percent strongly disagreed that Nigerian police
305 contribute to the growth of cybercrime in Nigeria.

306 Section B Response from the police 56.30 percent of the police respondents agreed, 6.30 percent strongly
307 agreed, 6.30 percent could not decide, 18.8 percent disagreed, and 12.50 percent strongly disagreed that Nigerian
308 police contribute to the growth of cybercrime in Nigeria.

309 **26 Question 9**

310 Cybercrime suspect are usually prosecuted in line with Nigerian law.

311 Section B Response from the police 12.50 percent of the police respondents agreed, 12.50 percent strongly
312 agreed, 37.50 percent disagreed, and 37.50 percent strongly disagreed that cybercrime suspect are usually
313 prosecuted in line with Nigerian law.

314 **27 Searching one's personal phone by the police is necessary to**
315 **curb the rate of cybercrime in Nigeria society**

316 Section B Response from the police 25.0 percent of the police respondents agreed, 56.3 percent strongly agreed,
317 6.30 percent disagreed, and 12.50 percent strongly disagreed that searching one's personal phone by the police is
318 necessary to curb the rate of cybercrime in Nigeria society Section A: youth responses 20.0 percent of the youth
319 respondents agreed, 12.50 percent strongly agreed, 17.50 percent could not decide, 22.50 percent disagreed, and
320 27.50 percent strongly disagreed that searching one's personal phone by the police is necessary to curb the rate
321 of cybercrime in Nigeria society.

322 **28 Question 11**

323 **29 Nigeria police are not knowledgeable of the various tech-**
324 **niques employed in perpetuating cybercrime in Nigeria**

325 Section A: youth responses 35.50 percent of the youth respondents agreed, 37.50 percent strongly agreed, 17.50
326 percent could not decide, 7.50 percent disagreed, and 2.50 percent strongly disagreed that Nigeria police are not
327 knowledgeable of the various techniques employed in perpetuating cybercrime in Nigeria.
328 Section B Response from the police 50.0 percent of the police respondents agreed, 12.50 percent strongly
329 agreed, 25.0 percent could not decide, and 12.50 percent disagreed that Nigeria police are not knowledgeable of
330 the various techniques employed in perpetuating cybercrime in Nigeria.

331 **30 Question 12**

332 **31 Cybercrime cannot be curtailed or reduce by the current**
333 **Nigeria police despite all their training.**

334 Section B Response from the police 37.50 percent of the police respondents agreed, 12.50 percent strongly agreed,
335 12.5 percent could not decide, and 37.50 percent disagreed that Cybercrime cannot be curtailed or reduce by the
336 current Nigeria police despite all their training.

337 Section A: youth responses 37.50 percent of the youth respondents agreed, 32.50 percent strongly agreed,
338 17.50 percent could not decide, 2.50 percent disagreed, and 10.0 percent strongly disagreed that Cybercrime
339 cannot be curtailed or reduce by the current Nigeria police despite all their training. Section A: youth responses
340 35.50 percent of the youth respondents agreed, 37.50 percent strongly agreed, 10.0 percent could not decide, 10.0
341 percent disagreed, and 7.0 percent strongly disagreed that the Nigerian police need a cybercrime unit, department
342 or division to effectively fight cybercrime in Nigeria.

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

346 **32 Question 14**

347 All teenager driving expensive cars are usually first suspect of cybercrime activities.
348 Section A: youth responses 17.50 percent of the youth respondents agreed, 47.50 percent strongly agreed, 5.0
349 percent could not decide, 17.50 percent disagreed, and 12.50 percent strongly disagreed that all teenager driving
350 expensive cars are usually first suspect of cybercrime activities.

351 Section B Response from the police 43.80 percent of the police respondents agreed, 31.30 percent strongly
352 agreed, and 6.3 percent disagreed that all teenager driving expensive cars are usually first suspect of cybercrime
353 activities

33 IV. SUMMARY, CONCLUSION AND RECOMMENDATION



INTRODUCTION

INARS, NETWORKING OPPORTUNITIES, AND PRIVILEGED BENEFITS AUTHOR MEMBERSHIP PROVIDED BY X T GENE S / SEMINING OPPS. AUTHENTI

SCIENTIFIC
, ACCESS
JMS / WEB
ND PRIVATE
ROVIDE
XTGEN

ARAOO 13 XIGENE S / SEMIN INGOPP S. AUTH ENTIFIC ACCESS

Figure 3: Question 13 The
INNOVATION, NEXT GENERATION TOOLS, ACCESS
TO CONFERENCES / SEMINARS / SYMPOSIA / WEB
INARS, NETWORKING OPPORTUNITIES, AND PRIVI-
LEGED BENEFITS. AUTHOR MEMBERSHIP PROVIDE
ACCESSTO SCIENTIFIC INNOVATION, NEXT GENE-
RATION TOOLS, ACCESSTO CONFERENCES / SEMIN-
ARS / SYMPOSIA / WEBINARS, NETWORKING OPP-
ORTUNITIES, AND PRIVILEGED BENEFITS. AUTH-
OR MEMBERSHIP PROVIDE ACCESSTO SCIENTIFIC
INNOVATION, NEXT GENERATION TOOLS, ACCESS

