CYBERCRIME AWARENESS AMONG POLICE PERSONNEL IN LAGOS, NIGERIA

[1]**Philip N. Ndubueze; [2]Ukasha Ismail**

[1]Department of Sociology, Federal University Dutse, Jigawa State, Nigeria, Email: pnndubueze@gmail.com, philip.n@fud.edu.ng [2]Department of Sociology, Federal University Dutse, Jigawa State, Nigeria, Email:ukashai17@gmail.com

Abstract

The study investigated cybercrime awareness among police personnel in Lagos, Nigeria. One hundred and thirty (N130) police personnel were selected from Lagos police command through multistage sampling that involved the use of cluster, simple random, convenience and purposive techniques. This paper adopted a combination of space transition theory of cybercrime and gap theory of policing as theoretical framework. The study found that the police personnel are aware of online advance fee fraud (also called *yahoo-yahoo* in Nigeria) among other forms of cybercrimes perpetrated in Lagos metropolis. Cybercrime are frequently reported to the police. However, individuals report few cybercrime victimization to the police in Lagos compared to managers of commercial banks. Also, majority of the respondents believed that training and retraining of police personnel on Information and Communication Technology (ICT) can improve their awareness of cybercrime. Result of Chi-square test showed that there was no significant relationship between level of education and cybercrime awareness among police personnel in Lagos (P>0.06). The study recommends that, members of the public be massively sensitized on the importance of reporting cybercrime victimization to the police. More so, online platforms should be created by the Lagos state police command to enable cybercrime victims report their victimization easily and get feedback on action taken.

Keywords: Awareness; cybercrime; internet; police; Lagos; *yahoo-yahoo*.

Introduction

In the olden days, crimes were solely committed in the physical space, which police organizations are traditionally familiar with and oriented to. However, technological advancement in the past two decades or so has broadened and dramatically altered the landscape of crime. The proliferation of information and communication technologies (ICTs) as well as the progressive development in digital transactions and communications have created new opportunities and opened up new windows which have resulted in the emergence of new forms of criminal behaviors. Therefore, technology savvy criminals have migrated from the physical space to cyberspace and are perpetrating diverse forms of cybercrimes. Cybercriminals take undue advantage of vulnerabilities of the internet technology to carry out a wide range of criminal activities on the cyberspace.

Olayemi (2014) posited that, the society is increasingly depending on modern information technologies and the internet to carry out almost all activities that have to do with social life. This advancement paves way for criminals to victimize the unsuspecting and gullible internet users. The extent of cyber victimization depends on the level of awareness of the dynamics of cybercrime by the victim. Cybercrime victimization can be victim precipitated. Therefore, awareness of the variants of cybercrime can assist potential victims to protect themselves from victimization.

In the same vein, awareness of the changing patterns of cybercrime is key to the law enforcement fight against cybercrime. Increase in cyber-related threats have necessitated paradigm shift in policing. Cyber policing is increasingly gaining prominence in contemporary security architecture. Judicial evidence are increasingly being collected, stored and transmitted during proceeding in electronic form. Whereas countries

of the global north have since leveraged on internet technology to improve the efficiency of their police forces, the same cannot be said of the countries of the global south. However, efforts are been made by developing countries, including Nigeria to catch-up with the rest of the world.

Although numerous governmental and private initiatives have been deployed to deal with cybercrimes in Nigeria (Adesina, 2017), reasonable successes seemed not to have been achieved. Ehimen and Bola (2010) also observed that, the Nigerian law enforcement agencies that are responsible to combat the crimes are not adequately prepared to prevent and control cybercrimes. Majority of them are not educated on computer and the internet. Stol and Jansen (2013) opined that few victims report cybercrime to the police. This attitude may have been influenced by the victims' perceived lack of confidence on the police.

Aggarwal (2015), Balogun and Obe (2010), Ehimen and Bola (2010), Jaishankar (2011), Lewis (2015), Ndubueze, (2017), Ndubueze, et al. (2013) related cybercrime victimization among internet users to lack of cybercrime awareness. However, a few studies that investigated the role of police in combating cybercrime (Brown, 2015; Police Executive Study Forum, 2014; Stol & Jansen, 2013; Leukefedt, et al. 2013; Mitchell, et al., 2005) did not focus on their cybercrime awareness. Therefore, in order to fill the above gap, this study investigated awareness on cybercrime among police personnel in Lagos, Nigeria.

Research Questions

This research attempted to answer the following research questions: (1) What is the level of awareness on cybercrime among police personnel in Lagos, Nigeria? (2) What are the best possible measures to improve awareness on cybercrime among police personnel in Lagos, Nigeria? (3) How frequent do people report cybercrime victimizations to police in Lagos, Nigeria?

Hypothesis

H_1: Tertiary educational attainment determines cybercrime awareness among police personnel in Lagos, Nigeria.

Literature Review

Awareness of Cybercrime among Police

The complexity of policing online activities and the challenges associated with technology use, monitoring, reporting and enforcement has been elaborately discussed (Holt, 2020). It is much more difficult to investigate and solve cybercrime than street crimes (Graham & Smith, 2020) and police departments that rely on traditional approaches to crime control may not be able to effectively track many cybercrime offences (Willits & Nowachi, 2016). Georgieva (2020) argued that the adoption of new intelligence techniques in cyberspace has made security and intelligence agencies major actors in cybersecurity sector.

The growing spate of cybercrime is a major challenge for law enforcement agencies. Moore (2015) argued that persistence of high technology crime constitutes a problem to law enforcement personnel because of the training and equipment needed. Similarly, Holt and Bossler (2016) opined that cybercrimes and advances in technology create unique challenges for the response of policing agencies to them. They also observed that given that technology is always evolving makes digital evidence management a major challenge that confronts law enforcement in the field.

Several studies have investigated the level of awareness of cybercrime among the general public. For instance, a study conducted by Pradeep and Arjun (2018) found that youth in Udupi district, India are not aware of cybercrime and that the lack of awareness is manifested mainly in cases that has to do with the protection of personal computers and laptops. Tibi, et al. (2019) assessed the level of cybercrime awareness among students at a teachers' training college in Israel and found that the level of cybercrime awareness among participants was inadequate. Furthermore, a study by Nzeakor, et al. (2020) that examined the pattern of cybercrime awareness in Imo State reported that majority of

the respondents claimed to be aware of cybercrime. However, the study found that their knowledge of cybercrime seemed to be superficial since majority of the respondents were only aware of computer-related/assisted forms of cybercrime such as e-fraud, while few of them were aware of computer-focused crimes such as business e-mail compromise, spam mail, denial of service attack etc. This is perhaps because most empirical studies on cybercrime as well as media reportage on it in Nigeria is skewed towards online advance fee fraud. The fact that the police are also a part of the public and they also use the internet, the findings of the above studies apply to them.

Reporting of Cybercrime Victimization to Police

Under-reporting of cybercrime and the fact that only a few cybercrimes are prosecuted raises questions about public perception of the effectiveness of the police to combat cybercrimes. This is the finding of study conducted by Weijer et al. (2019) when they examined attitude of reporting cybercrime victimization among internet users. They discovered that there is wide discrepancy between intended and actual cybercrime reporting behaviour of people. This implies that cybercrime victims want to report their negative experience to police, but they do not frequently do so. In line with the above, Stol and Jansen (2013) observed that most victims of cybercrime do not report their complaint to law enforcement authorities. And, even if the victims reported to the police, there is no certainty that they will register the report and swiftly act upon it. This means, people may be afraid and may accuse the police of not taking action. It may be attributed to feeling of shame and upset by the victims, which deter them from reporting their victimization experience (Whitty & Buchanan, 2012). Olayemi (2014) discovered that the Nigeria Police Force (NPF) mostly become aware that cybercrime is committed through complaints lodged by victims. Police over-reliance on a single source of information about an emerging phenomenon of cybercrime is inadequate. To address this shortcoming, Ndubueze (2014) underscored the role of Internet Service Providers (ISPs) in safeguarding the Nigerian cyberspace. To him, they can play gate-keeping functions and are also required by law to detect, prevent and report any of their criminal-minded clients to relevant law enforcement authorities.

Theoretical Framework

A combination of space transition theory of cybercrime and gap theory of community policing formed the theoretical framework of this study.

Space Transition Theory of Cybercrime

Space transition theory which was developed by Jaishankar (2008) explains the dynamics of criminal behaviour in the cyberspace. It posits that:

1. Persons with repressed criminal behaviour (in the physical space) have a propensity to commit crime in cyberspace, which, otherwise they would not commit in the physical space, due to their status and position.
2. Identity Flexibility, dissociative anonymity, and lack of deterrence factor in the cyberspace provide the offender the choice to commit cybercrime.
3. Criminal behaviour of offenders in cyberspace is likely to be imported to physical space, which, in physical space may be exported to the cyberspace as well.
4. Intermittent venture of offenders in the cyberspace and the dynamic spatiotemporal nature of cyberspace provide the chance to escape.
5. (a) Strangers are likely to unite in cyberspace to commit crime in the physical space, (b) Associates of physical space are likely to unite to commit come in cyberspace.
6. Persons from closed society are more likely to commit cybercrime than persons from open society).
7. The conflict of norms and values of physical space with the norms and values of cyberspace may lead to cybercrimes (Jaishankar, 2008, pp. 293-296).

The theory is very useful in the understanding of some salient issues around cybercrime and its control. Essentially, how people move from the physical space to the cyberspace and vice versa and how they can operate unanimously. The theory not only underscore the nature of cybercrime, it also provides insights into the driving forces behind cyber criminality and modus operandi of cyber criminals. Police personnel need to understand the changing patterns of crime and criminality in the digital age and the modus operandi of cyber criminals to be able to effectively prevent or control cybercrime. Therefore, awareness of the dynamics of space transition is a critical to the success of the police in their efforts to combat cybercrime.

Gap Theory

Gap theory was coined by George J. Thompson in 2006. The theory is used to understand police-public partnership in crime prevention and control. The basic tenets of the theory are as follows: there is growing gap between the police and members of the public; those who are maltreated by the police will less likely assist the police with vital information on crime; crooks and criminals benefit from the 'gap' between the police and the people; and the better the police treat the people, the safer the people feel and the more the 'gap' closes (Arisukwu, 2017).

In the context of this study, gap theory provides insights on why victims of cybercrime are reluctant to report their victimization experience to Lagos state police personnel in particular and Nigeria Police Force in general. When people report cybercrime complaints to the police they need urgent attention from the police. In situations where such attention is not accorded to them at all or with the urgency it deserves, the victims may not bother to report in the future. Again, they may discourage others from reporting their victimizations as well. Consequently, people are likely to lose confidence in the police and this will affect the frequency of cybercrime reportage to them. Moreover, the police may possibly not determine the spate of cybercrime in Lagos due to inadequate intelligence (information) on cybercrime victimization. This gap may create the opportunity for some cyber criminals to continue to operate with impunity in Lagos metropolis.

The Study Area

This study was conducted in Lagos state police command partly because it is the largest police command with most complex policing mandate in Nigeria. The strength of police personnel attached to the command was put at 29,122 (www.npf.gov.ng/zone2.php). The police command, which is headed by a Commissioner of Police, has its headquarters in Ikeja. The command has thirteen (13) Area Commands who control no fewer than one hundred and seven (107) Police Divisions of the command. Lagos state police command was chosen for this study because it is housed in Lagos; a cosmopolitan city that is populated by people from diverse ethno-religious and economic backgrounds. Adesina (2017) suggested that the Lagos metropolis has the highest presence of cyber criminals in Nigeria.

Methods

The study used survey design to investigate awareness of cybercrime among police personnel in Lagos command. A sample size of one hundred and thirty (130) police personnel was selected using multi-stage sampling techniques. Lagos state command was clustered into thirteen (13) Area Commands namely: Area A - Lagos Island, Area B – Apapa, Area C – Surulere, Area D – Mushin, Area E – Festac, Area F – Ikeja, Area G – Ogba, Area H – Ogudu, Area J – Elemoro, Area K – Morogbo, Area L – Ilashe, Area M – Idimu, and Area N – Ijede. Three (3) area commands namely: Area A - Lagos Island, Area J– Elemoro, and Area C – Surulere were selected using simple random sampling. One hundred and twenty (120) police personnel were conveniently selected and voluntarily completed structured questionnaires. Researcher's administrative approach was adopted to explain the content of the questionnaire during the field survey. Another ten (10) police personnel were purposively selected and participated in the in-depth interviews. The data generated through questionnaires were analyzed using Statistical Package for Social Sciences (SPSS). The findings are presented in a tabular form. The qualitative data were

transcribed, analyzed and presented as excerpts. Chi-square (X^2) was used to test relationship between level of education of the police personnel and their level of cybercrime awareness.

Results

Table 1: Socio-Demographic Distributions of the Respondents

Variables	Frequency (n)	Percentage (%)
Gender		
Male	71	70.3
Female	30	29.7
Total	**101**	**100.0**
Age Grades (Years)		
20-24 years	03	2.8
25-29 years	06	5.9
30-34 years	16	15.8
35-39 years	23	22.8
40 years and above	49	48.5
Total	**101**	**100.0**
Educational Attainment		
Primary	01	1.0
Secondary	44	43.6
Tertiary	56	55.4
Total	**101**	**100.0**
Rank		
SPO(ASPII-IGP)	20	19.8
Inspector	31	29.0
Sergeant	41	38.3
Corporal	05	4.7
Constable	04	3.7
Total	**101**	**100.0**
Income		
N45,000-N54,999	60	59.4
N55,000-N64,999	04	3.7
N65,000-N74,999	23	22.8
N75,000-N84,999	04	3.7
N85,000 and above	10	9.9
Total	**101**	**100.0**

Table 1 presents the socio-demographic characteristics of the respondents. It reveals that 70.3% were males, while 29.7% constituted females. This is because the staff strength of male police personnel is significantly higher than their females' counterpart in Nigeria Police Force. On age of the respondents, 48.5% aged 40 years and above, 22.8% were between 35-39 years,(15.8% represented 30-34 years, 5.9% were between 25-29 years, and 2.8% accounts for those between 20-24 years of age. This indicated that there are least young police personnel in Lagos police command and Nigeria Police Force as a whole. Respondents with tertiary education constituted the majority (55.4%). This is followed by 43.6% of the respondents who possessed secondary school qualifications and 1.0% had first school leaving certificate. This reveals that a significant number of police personnel acquired tertiary education.

The table indicates that 38.3% of the respondents were sergeants, 29.0% were inspectors, then senior police officers (SPOs) constituted 19.8%, 4.7% were corporals and 3.7% were constables. The finding revealed that majority of police personnel in the sampled areas were sergeants who are, in most cases, at the middle of their lengths of service. Also, the table indicates that more than half of the respondents (59.4%) earned N45, 000-N54, 999 per month, 22.8% earned N65, 000-N74, 999; 9.3% were those with monthly income of N85, 000 and above, 9.9% earned between N55, 000-N64, 999, and 3.7% of the respondents earned between N75, 000-N84, 999. This shows that members of the rank and file in the Nigeria Police Force earn lower compared to Inspectors and Senior Police Officers.

Table 2: Cybercrime Awareness among the Respondents

Response	N	%
Yes	89	88.1
No	12	11.9
Total	**101**	**100.0**

Table 2 presented respondents' awareness of cybercrime. It reveals that majority of the respondents (88.1%) were aware of cybercrime, while 11.9% were not aware. Likewise, some police personnel interviewed revealed how police become aware of cybercrime in the study area. An indent-interview participant stated that:

> It is hard to find police personnel in Lagos that is not aware of online advance fee fraud (*Yahoo-Yahoo*). The activities of *Yahoo-Boys* have received serious attentions of popular media and law enforcement agents. In short, it has reached a point where any youth seen with Laptop is interrogated by police personnel and most crime bulletin on the media involves *Yahoo-Yahoo*. These are good sources of

> enlightenment on cybercrime in Lagos (IDI/male/Constable/Lion Building Division/2018).

This suggests that most police personnel in Lagos are aware of cybercrime. Although to them, cybercrime is synonymous with *Yahoo-yahoo*. This implies that they may not be aware of other emerging cybercrimes that are perpetrated daily. For example cyberstalking, cyber hate speech, cyber defamation, online child grooming and so on.

Another in-depth interview participants narrated thus:

> I am aware of cybercrime in Lagos because I acquired computer skills and I visit the Internet more often. But, frankly, I do not think 30% of police personnel in Lagos are aware of cybercrime because majority of us [police personnel] are not computer literate (IDI/male/SPO/Onikon Division/2018).

The above quote seems to suggest that the Lagos state police command does not routinely train and retain its personnel to acquire skills on computer and related technologies. Those interested in personal development perhaps have to enroll themselves in computer training centres.

Table 3: Respondents' Views on Forms of Cybercrimes Frequently Perpetrated

Forms of Cybercrime	Yes (%)	No (%)	Total (%)
Digital Piracy	11 (10.9)	90 (89.1)	101 (100)
Spamming	21 (20.8)	80 (79.2)	101 (100)
Cyber-stalking	7 (6.5)	94 (93.5)	101 (100)
Phishing	15 (14.9)	86 (85.1)	101 (100)
Hacking	21 (20.8)	80 (79.2)	101 (100)
Cyber Terrorism	13 (12.9)	92 (91.1)	101 (100)
Online Advance Fee Fraud (*Yahoo-Yahoo)*	89 (88.1)	12 (11.9)	101 (100)

Table3 shows respondents' views on forms of cybercrimes frequently perpetrated in Lagos. It indicates that majority of the respondents (88.1%) said online advance fee fraud (*Yahoo-yahoo*) is most perpetrated cybercrime, while 11.9% did not think so. Furthermore, 20.8% of the respondents were of the view that hacking is the most perpetrated cybercrime in Lagos, while majority (79.2%) had a contrary view. Similarly, 20.8% of the respondents said that spamming is most perpetrated, while 79.2% said no. Moreover, 14.9% of the respondents believed that phishing is the most perpetrated cybercrime, whereas 85.1% did not think so. Also, 12.9% of the respondents reported cyber-terrorism as frequently perpetrated and 91.1% disagreed, 10.9% of the respondents were of the view that digital piracy is the most perpetrated cybercrime in Lagos, while (89.1%) did not believe so. Lastly, 6.5% of the respondents indicated that cyber-stalking is the most perpetrated cybercrime, while majority (93.5%) did not think so. Majority of the respondents agreed that online advance fee fraud (*Yahoo-yahoo*) is most perpetrated cybercrime in Lagos. A senior police officer interviewed corroborated the above findings:

> In Lagos, *yahoo-yahoo* has become a household name due to its acceptance among individuals, especially youths. Majority of Yahoo-Boys are students of various tertiary institutions and unemployed graduates. In sum, online advance fee fraud is generating concerns as it continues in different magnitude (IDI/male/SPO/Ikoyi Division/2018).

The results from the quantitative and qualitative data seems to suggest that the awareness of police personnel on cybercrime is limited to online advance fee fraud (*Yahoo-yahoo*). This implies that their level of awareness is not high because *Yahoo-yahoo* is just a fraction of cybercrimes perpetrated in Lagos.

Table 4: Respondents' Views on Time of the Day that Cybercriminals Usually Operate

Time of the day	N	%
Day	02	1.9
Night	07	6.9
Anytime of the day	92	94.4
Total	**101**	**100.0**

Table 4 presents respondents' views on time of the day that cybercriminals usually operate in Lagos.

It reveals that majority of the respondents (94.4%) opined that cyber criminals operate at any time of the day, 6.9% said night time, and 1.9% reported day time. Respondents for qualitative category in this study believed that nowadays *Yahoo-boys* do not have specific operational hours. They usually engage their potential victims at all times of the day. This is why a respondent added that:

> Today, cybercriminals operate at any time of the day due to development in modern means of communications such as internet-enabled mobile phones, tablets, and computers. Also, increase in networking sites (such as Facebook, Instagram, WhatsApp etc.) helps *Yahoo-Boys* engage their victims at any time (IDI/male/Inspector/Onikon Division/2018).

Proliferation of internet broadband technology, digital devices and social media platforms create opportunities for cyber criminals (*Yahoo-boys*) to operate at all times of the day.

However, another in-depth interview participant opined that:

> Cybercriminals operate at night because of its serene nature. They try to woe their targets using good network at night. They do not usually operate in the day because people are at their work-places. As such, they may not respond to their messages and/or voice calls (IDI/female/Sergeant/Victoria Island Division/2018).

The above quote suggests that, cyber criminals operate mostly at night because it is more conducive to engage their targets.

Table 5: Respondents' Views on where Cybercrimes are usually perpetrated

Point	Yes (%)	No (%)	Total (%)
Cybercafé	17 (16.8)	84 (83.2)	101 (100)
At Home	79 (73.8)	22 (20.6)	101 (100)
Government Offices	13 (12.9)	88 (87.1)	101 (100)
Private Organization Network	16 (15.8)	85 (84.1)	101 (100)

Table 5 showed respondents' opinions on where cybercrimes are usually perpetrated in Lagos. It revealed that majority of the respondents (73.8%) opined that cyber criminals usually operate at home, while 20.6% did not think so. Also, 15.9% of the respondents considered cybercafe as points where cybercrimes are usually perpetrated, whereas, 78.5% said no. Furthermore, 12.9% of the respondents believed that cybercrimes are mostly perpetrated in government offices, while 87.1% said no. Moreover, 15.8% of the respondents were of the view that cybercrimes are usually perpetrated in private organization network, whereas 84.1% of the respondents said no. This finding suggests that advances in information and communication technologies along with availability of internet broadband help cybercriminals to operate from the comfort of their homes.

Table 6: Respondents' views on Frequency of reports on cybercrime victimization

Response	N	(%)
Frequent	76	75.3
Not frequent	16	15.8
Not sure	09	8.9
Total	**101**	**100.0**

Table 6 presented respondents' experience regarding complaints on cyber victimization reported at their respective areas of jurisdiction. It reveals that majority of the respondents (75.3%) frequently hear/receive complaints on cyber victimization in their areas of jurisdiction, whereas 15.8% said that they do not frequently hear/receive complaints on cyber victimization in their areas of jurisdiction and 8.9% of the respondents were not sure whether or not complaints on cyber victimization are reported in their respective Police Divisions. Again, the police personnel interviewed narrated that police often receive cybercrime complaints, especially those related to online frauds. In addition, a respondent made the following statements:

> Most complaints on cybercrime victimization reported to us are associated with activities of *Yahoo-*

> *boys* [online advance fee fraud]. Individuals do not often report cyber victimizations, but banks do. Banks whose customers report being defraud normally detect perpetrators upon withdrawal at banking halls. Subsequently, they alert police for arrest and further investigation (IDI/female/Inspector/CMS Division/2018).

The above quotation suggests that majority of cybercrime complaints are made to the police by commercial banks. The banks usually red-flag accounts suspected to have been used for fraudulent activities. A post no debit (PND) order is placed on such accounts, thereby preventing the account holder from making withdrawal or some related electronic banking transactions. Consequently, the suspect may have no option than to visit the bank to lodge complaint or try to make over the counter withdrawal. That is how some suspected *Yahoo-boys* are identified, arrested and handed over to police for investigation.

Table 7: Respondents' Views on How to Improve their Awareness on Cybercrime

Way to improve cybercrime awareness	Yes (%)	No (%)	Total (%)
Inclusion of computer appreciation courses during police basic trainings.	63 (62.4)	38 (37.6)	101 (100%)
Training and retraining of police personnel on ICT and other digital technologies.	97 (96.0)	04 (4.0)	101 (100%)
Making "cybercrime" a subject of lecture in all police lecture parades.	20 (19.8)	81 (80.2)	101 (100%)

Table 7 presents respondents' views on how to improve awareness on cybercrime among Police personnel in Lagos. It indicated that majority of the respondents (96.0%) recommended training and retraining of police personnel on ICTs and other digital devices as a strategy, whereas (4.0%) did not support the strategy. Also, 26.4% of the respondents suggested the inclusion of computer appreciation courses during police basic trainings, while 36.7% disagreed. Lastly, 19.8% of the respondents opined that making cybercrime a subject of lecture in all police lecture parades would be a good way to improve their awareness on cybercrime, whereas majority (80.2%) did not think so. In the same vein, some police personnel suggested how the level of cybercrime awareness among police personnel in Lagos can be improved. Moreover, an in-depth interview participant argued that:

> It is apparent that those police personnel that have little or no awareness on cybercrime in Lagos have not attained higher education. As such, they should be encouraged to enroll in schools and improve their level of education. Again, the management of the Nigeria Police should create an enabling environment for all police personnel to acquire computer skills given its relevance in contemporary policing (IDI/male/Constable/Lion Building Division/2018).

The above argument suggests that cybercrime awareness among police personnel in Lagos is determined by their level of educational attainment.

Hypothesis Test

H_1: Tertiary educational attainment determines cybercrime awareness among police personnel in Lagos, Nigeria.

H_0: Tertiary educational attainment does not determine cybercrime awareness among police personnel in Lagos, Nigeria.

Table 8: Relationship between Educational Attainment and Cybercrime Awareness

Educational attainment	Awareness of cybercrime		Total
	Yes	No	
Primary	01	-	01
Secondary	37	07	44
Tertiary	51	05	56
Total	**89**	**12**	**101**

(X^2=108.359, DF=6, P=0.06)

Table 8 reveals that there is no significant relationship (P=0.06) between educational attainment and cybercrime awareness among police personnel in Lagos. The result of Chi-

square test above showed that the alternate hypothesis (H_1) is rejected in favor of the null hypothesis H_0. This implies that awareness on cybercrime among police personnel in Lagos is not determined by their level of education. Thus, the finding indicates that police personnel who acquired tertiary qualifications are not more aware of cybercrime than their counterparts with secondary and primary schools leaving certificates.

Discussion

People's increased dependence on the internet and digital technologies for their daily business and recreational activities has profound implications for the rates of cybercrime. Cyber criminals in developing countries including Nigeria are exploiting people's naivety of their tricks and modus operandi to victimize them. People who are not aware of the dynamics of cybercrime are more likely to fall victim of it. Furthermore, law enforcement activities and operations have historically being physical space-oriented. To be able to effectively combat cyberspace crime, law enforcement personnel need to be fully aware of what constitute cybercrime. This paper interrogates the level of awareness of cybercrime among police personnel in Lagos; how frequent people report cybercrime victimization to the police in Lagos and the best measures to improve cybercrime awareness among police personnel in Lagos.

Results of the study revealed that majority of the sampled police personnel are familiar with the cybercrime. It also identified online advance fee fraud popularly known as *yahoo-yahoo* as the most prevalent form of cybercrime. This is hardly surprising as media reports suggest that the personnel of the Nigeria Police Force often encounter suspected online advance fee fraudsters during their routine patrol operations in Lagos. Similarly, Nwokeoma, et al. (2017) decried the upsurge in advance fee fraud cases in Nigeria. Nonetheless, online advance fee fraud is not the only variant of cybercrime that is common in Nigeria. There are other emerging types of cybercrime that citizens suffer, albeit silently for the most part. These include for example, cyberstalking, revenge pornography, cyberbullying, cyber defamation and so on. These do not often generate moral panic and have not received enough scholarly attention.

More so, majority of the respondents believe that cybercrime is perpetrated at anytime of the day and usually at home. This finding is contrary to the result of an earlier study by Longe and Chiemeke (2008) which found that cyber cafes constitute a major internet access point for cyber criminals. Before the proliferation of broadband internet in Nigeria, people accessed the internet mainly through cyber cafes and so did cyber criminals who were also believed to be usually involved in overnight browsing. The sampled police personnel also said people frequently report cybercrime. This is contrary to the finding of Stol and Jansen (2013) who noted that victims do not usually report cybercrime to the police. This suggests that there is perhaps an improvement in cybercrime awareness over the years. Arguably, the reporting of cybercrime will depend on the extent to which the victims are aware of their victimization. For example, a victim who is not aware that his/her identity information has been stolen online may not report same to the police. On the other hand, when identity theft is reported to the police, it will take a police officer who understands the social network of identity thieves to appreciate the potential damage that the victim may suffer and to take appropriate action. In any case, the study revealed that online advance fee fraud is the most reported cybercrime and that it is usually reported by the banks who often invite the police to arrest clients involved in fraudulent transactions. But, it would be misleading to assume that online advance fee fraud is the only type of cybercrime that is prevalent in Nigeria. Other forms of cybercrime that are not necessarily financial related are also prevalent, though hardly reported.

Likewise, majority of the respondents believe that training and re-training of police personnel on information and communication/digital technologies will help in improving their awareness of cybercrime. The gap in law enforcement knowledge and skills with reference

to cybercrime has since been recognized (Ndubueze, 2020). In the digital age, periodic training and re-training is one sure-footed way that law enforcement personnel can catch-up with the growing sophistication of cybercrime schemes. The result of hypothesis test suggested that police personnel with higher educational qualification are not more aware of cybercrime than those with secondary and primary school leaving certificates. The results from analyses of both quantitative and qualitative data corroborate the theoretical assumptions adopted in this study. The proportions of space transition theory is aligned with the finding of the study that improved police awareness of cybercrime is key to their success in the fight against cybercrime in Lagos.

Conclusion

The sampled police personnel in Lagos, Nigeria are mainly aware of online advance fee fraud (popularly known as *Yahoo-yahoo*) among various forms of cybercrime. This is not surprising given the frequency of *Yahoo-yahoo* activities in Lagos metropolis. Also, the mass arrests of *Yahoo-boys* (those who engage in *Yahoo-yahoo*) in Lagos is another factor that may have made the police personnel to be aware of cybercrime. However, other emerging cybercrimes such as cyberstalking, sextortion, revenge pornography, cyberbullying, cyber defamation and so on may not be known to non-tech savvy police personnel. There seems to be some cybercrime awareness training and re-training gaps among personnel of the Lagos state police command. This is perhaps because it lacks equipped computer laboratories with sophisticated technologies that they could use to train the personnel and sufficiently detect, trace, and apprehend various groups of cyber criminals. This may affect the decision of some members of the public to report cybercrime to the police in Lagos.

Recommendations

Based on the findings of the study, the following recommendations are made.

1. Information and communication technology-based raining and retraining of the police personnel will assist the police in improving their awareness on the ever-increasing complexities of cybercrime.
2. There is need for massive campaign by the National Orientation Agency, the Nigeria Police Force, Civil Society Organizations and other relevant stakeholders to sensitize the public on the importance of reporting cybercrime to the police.
3. Online platforms should be created by the Lagos state police command to enable cybercrime victims report their victimization easily and get feedback on action taken.
4. It is also suggested that cybercrime investigators and units be established in Lagos state police command and its various formations in order to boost the confidence of the public on the police capacity to swiftly investigate cybercrime cases.

References

Adeniran, A.I. (2008). The internet and emergence of *yahooboys* sub-culture in Nigeria: *International Journal of Cyber Criminology* 2 (2): 368-370.

Adesina, O.S. (2017). Cybercrime and poverty in Nigeria: *Canadian journal of Social Sciences* 13(4): 19-29.

Aggarwal, G. (2015). General awareness on cybercrime: *International Journal of Advanced Study in Computer Science and Software Engineering* 5(8): 204.

Arisukwu O. (2017). An Assessment of Community Policing-Oriented Training Programme in Benue and Lagos States, Nigeria. *Social Crimonol,* 5(1), 1-10.

Balogun, V.F. & Obe, O.O. (2010). E-crime in Nigeria: trends, tricks, and treatment. T*he Public Journal of Science and Technology* 11 (1): 343 – 355.

Brown, C.S.D. (2015). Investigating and Prosecuting Cybercrime: Forensic Dependencies and Barrier to Justice: *International Journal of Cyber Criminology*, 9(1):55-119 DOI:10.5281/zenodo.22387

Georgieva, L. (2020). The unexpected norm setters: intelligence agencies in cyberspace.

Contemporary Security Policy 41 (1): 33-54.

Graham, R.S. & Smith, S.K. (2020). *Cybercrime and digital evidence*. New York: Routledge: Taylor and Francis Group. Ehimen, O.R., & Bola, A. (2010). Cybercrime in Nigeria. *Business Intelligence Journal*, 3(1): 94-9.

Holt, T.J. (2020) Police and extralegal structures to combat cybercrime. In Holt, T.J. and Bossler, A.M. (eds.).*The Palgrave Handbook on International Cybercrime*. Switzerland AG: Palgrave Macmillan, Cham, pp.385-402.

Holt, T.J. & Bossler, A.M. (2016). *Cybercrime in progress: theory and prevention of technology-enabled offenses*. London: Routledge, Taylor and Francis Group.

Jaishankar, K. (2011). *Cyber criminology: exploring internet crimes and criminal behavior*. Boca Raton, FL USA: CRC Press.

Jaishankar, K. (2008). Space transition theory of cybercrime. In Schmallagar, F. and Pittaro, M. (eds), *Crimes of the* Internet. Upper Saddle River, NJ: Prentice Hall, pp.283–301.

Leukfldt, R., Veenstra, S. & Stol, W. (2013). High Volume Cyber Crime and the Organization of the Police: The Results of Two Empirical Studies in the Netherlands: *International Journal of Cyber Criminology,* 7(1), 1-2.

Lewis, N.O.Y. (2015). An Investigation of youth in cybercrime in the Ayawaso East constituency of greater Accra: a dissertation submitted to the University of Ghana, Legon, in partial fulfillment of the requirement for the award of Master of Arts Social Policy Studies Degree.

Longe, O.B. & Chiemeke,, S.C. (2008). Cybercrime and criminality in Nigeria: What roles are internet access points playing? *European Journal of Social Sciences* 6(4): 132-139.

Mitchell, K.J. Wolak, J. & Finkelhor, D. (2005) Police posing as juveniles online to catch sex offenders: Is it working: *A Journal OF Study and Treatment,* 17(3): 241-267. DOI: 10.1007/s11194-005-5055-2.

Moore, R. (2015). *Cybercrime: investigating high-technology computer crime* (2nd ed) London: Routledge: Taylor & Francis Group.

Ndubueze, P.N. (2014). Cyber Criminology and Quest for Social Order in Nigerian Cyberspace. *The Nigerian Journal of Sociology and Anthropology*, 14(1), 34-48.

Ndubueze, P.N. (2017). High-tech crimes, boundaryless policing and cyber security policy in digital Nigeria: a periscope: *Dutse Journal of Criminology and Security Studies* 1(1): 89-102.

Ndubueze, P.N. (2020). Cybercrime and legislation in an African context. In Holt TJ and Bossler AM (eds) *The Palgrave Handbook on International Cybercrime and Cyberdeviance*. Switzerland AG: Palgrave Macmillan, Cham, pp. 345-364.

Ndubueze, P.N, Igbo, E.UM. and Okoye, U.O. (2013). Cybercrime victimization among internet active Nigerians: an analysis of socio-demographic correlates: *International Journal of Criminal Justice Sciences* 8(2): 225-234.

Ndubueze, P.N. (2020). Cybercrime and Legislation in an African Context. In Holt, TJ, Bossler, AM (eds.). *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, https://doi.org/10.1007/978-3-319-78440-3_74.

Nigeria Police Force (2016). Zone-2-home page. Retrieved from www.npf.gov.ng/zone2.php.

Nwokeoma, B.N, Ndubueze, P.N. & Igbo, E.U.M. (2017). Precursors of online advance fee fraud in South-East Nigeria. In Ndubueze PN (ed.) *Cyber Criminology and Technology-Assisted Crime Control: A Reader* Zaria: Ahmadu Bello University Press, pp.195-218.

Nzeakor, O.F, Nwokeoma, B.N. & Ezeh, P.J. (2020). Pattern of cybercrime awareness in Imo State Nigeria: An empirical assessment. *International Journal of Cyber Criminology* 14 (1): 283-299.

Olayemi, O.J. (2014). Combating the menace of cybercrime: *International Journal of*

Computer Science and Mobile Computing 3(6): 980-982.

Pradeep, L.M.P. & Arjun, M. (2018). Cybercrime awareness among youth in Udupi District J Forensic Science & Criminal Investigation 8 (5): 555750. DOI: 10.19080/JFSCI.2018.08.555750

Stol, W.P.H. & Jansen, J. (2013). *Cybercrime and the Police*. Netherlands: Eleven International Publishing.

Tibi, M.H, Hadeje, K. & Watted, B. (2019). Cybercrime awareness among students at a teacher training college. *International Journal of Computer Trends and Technology*, 67 (6): 11-17.

Weijer, S.V., Leukfeldt, R. & Van der Zee, S. (2019). Reporting cybercrime victimization: determinants, motives, and previous experiences. *Policing: An International Journal*. DOI 10.1108/PIJPSM-07-2019-0122.

Whitty, M. & Buchanan, T. (2012). The Online Dating Romance Scam: A Serious Crime. *CyberPsychology, Behavior, and Social Networking, 15*(3), 181-183.

Willits, D. & Nowacki, J. (2016). The use of specialized cybercrime policing units: an organizational analysis. *Criminal Justice Studies* 29 (2): 105-124.