“LUCRATIVE AND HIDDEN”: FACTORS INFLUENCING CYBERCRIME INVOLVEMENT AMONG YOUTH IN METROPOLITAN LAGOS.

ADEDEJI OYENUGA (PhD)
Department of Sociology
Lagos State University
adedeji.oyenuga@lasu.edu.ng
+2348037269268

ABSTRACT
Increasing access to the Internet. Although there have been studies on cybercrime, studies from within the subculture have remained mostly unexplored. This study, therefore, examined factors responsible for youth involvement in cybercrime. The study adopted diffusion of innovation and space transition theories. The study design was exploratory involving the use of qualitative methods of data collection. Four localities with a preponderance of cybercrime in Lagos State were purposively selected: Surulere, Ikotun, Badagry and Bariga. Ten In-depth Interviews and two case study were employed to collect data from youth involved in cybercrime that were chosen through guided referral in each locality. Through participant observation, youth involved in cybercrime were interacted with repeatedly over four years. Data were also collected from secondary sources such as EFCC and police records and periodicals. The data collected were content analysed. Access to the Internet and peer influence were the significant factors affecting youth involvement in cybercrime. However, other factors are economic, social, and psychological. Youth involved in cybercrime has been encouraged by the complexity and sophistication of the Internet. Therefore, stiffer regulations are necessities for adequate control of the virtual environment among others.

Introduction
Cybercrime has become an issue of concern in the global community. The fact that the world is becoming more dependent on online transactions has increased the vulnerability of all. Earlier beliefs were woven around the weakness of the western world as put forward by Furnell (2002); Howard (2001); and Kshetri (2010), but the widespread of the Internet has put more nations in danger. The recent enforcement of cashless transactions in Nigeria has equally placed within the danger zone. Literature has suggested that one of the significant reasons people engage in cybercrime is the anonymity within the Internet environment (Williams, 2005). Moreover, beyond questions of “who” is misbehaving in “which” ways via the Internet, the question of “why” people may be misbehaving while online also remains under-researched despite ongoing conjecture among media commentators. For some authors, the types of online misbehaviours like hacking website defacement, (or)bot-herding, website cloning and credit card theft constitute new forms and patterns of behaviour. Thus, it is argued that:

The Internet has allowed for the creation of a new environment within which novel types of crimes are engineered (Williams, 2005:3).
Indeed, for some, the Internet does nothing less than increase the likelihood that even ‘good kids’ who are ordinarily unlikely to commit crimes such as robbery, burglary or assault, may not be disinclined to commit an online crime (DeMarco, 2001:2).

In attempting to account for the apparent novelty of online crimes, discussions have tended to concentrate on the socio-structural features of the cyber-space (Selwyn, 2008). In this way, the facilitation of new patterns and forms of deviant behaviour is seen to stem from different structural and organisational features of the Internet and Internet use, with cybercrime guided by the Internet’s “own ontological and epistemological structures, interactional forms, roles and rules, limits and possibilities” (Yar, 2005:422). Thus, Freestone and Mitchell (2004) have highlighted the “unparalleled opportunities” for anonymously
accessing information and people as allowing “aberrant behaviour to remain “faceless.” Similarly, the seemingly remote nature of the online action is also seen to lift individual acts “out of local contexts of interaction and restructuring them across indefinite periods and space” (Wall, 2005:77). Thus, the disembodied nature of online interaction with other users and online organisations, coupled with the digital immateriality of online exchanges, is felt to lead users to explore a new sense of disinhibition and, it follows, a higher propensity to commit a crime (Denegri–Knot, 2006).

Highlighting the emergence of the ‘new’ forms and patterns of deviance acknowledges the potentials of the Internet to also promulgate preexisting crimes and malpractices (Selwyn, 2008). Freestone and Mitchell (2004) also contend that the Internet has paved the way for many new forms of aberrant behaviour, of which some are entirely new, and others are technologically updated versions of long-standing ethical debates. Thus, the point has been made that the Internet is perhaps more likely to extenuate existing behaviours rather than prompt novel behaviours, with online miscreants more often than not merely succumbing to “electronic opportunism” to engage in crime (Rocco and Warglien, 1995:14). Therefore, it may be more accurate to describe the maturing and transmutation rather than transformation of misbehaviour (Patchin and Hinduja, 2006).

In the academic Internet research community, there is a debate on the “cause” and “continuation” explanation of online crime. These two have accounted for the altered norms and ethical framework of cyber-space. Indeed, as with general discussion of deviance, the issue of who determines what is acceptable and to whom is itself subject to debate (Fullertone and Punj, 1997), a topic most evident in the prominent libertarian discourse since the early 1990s, which has stridently celebrated unfettered, unregulated and “outlaw” behaviour on the Internet (Thomas, 2005). In this sense, the negative discourse of cyber-deviancy and Internet-based misbehaviour are challenged by the “egalitarian undertones of a discourse sustained on the web’s being the freest of spaces” (Denegri-Knot, 2006:91). Thus, cyber–theorists have forcibly stated that the emerging norms and values of the Internet are quantitatively and qualitatively different from those of the “real world.” From this perspective, online behaviour is inherently disinhibited self-absorbed, and on occasions, transgressive, with Internet users, therefore, feeling “entitled and more willing to challenge offline norms of acceptable behaviour” (Denegri-Knot, 2006:86). Thus, Freestone and Mitchell (2004) have concluded:

The idea of cyberspace exists as a separate realm to the physical world and may have developed an ethnical culture of its own, or “Netiquette” and has a set of beliefs or standards, shared by a group of people, which help the individual decide what is, what can be, how to feel, what to do and how to go about doing unethical things on the net (Pg. 126).

Cybercrime remains elusive and ever strives to hide in the face of development. As measures and techniques for detecting crimes and criminals advance, criminals also look for means of hiding from these measures. The Internet currently serves as a hiding place for fraudsters who have simply migrated from the streets to an electronic platform offered by the World Wide Web. Different nations have adopted different strategies to contend with crimes, depending on their nature and extent. Certainly, a nation with a high incidence of crime cannot grow or develop. That is so because crime is the direct opposite of development. It leaves a negative social and economic consequence (Sylvester, 2001). For Nigeria, a nation in the process of saving her face regarding cybercrimes, efforts are now being directed at the sources and channels through which cybercrimes are perpetrated, with the most popular one being Internet access points (Longe and Chiemeke, 2006). Given the above, this study investigated the factors responsible for youth involvement in cybercrime with various specific focus on Lagos State.

Methods
The study utilized qualitative techniques in data generation. As already established, the qualitative method allows the researcher to gain valuable insights through the subjective narratives of the respondents by giving us clearer understanding from the participants’ perspectives. This ensures that data are rich in narratives and experiences.
The study was conducted in Lagos State as a primate state in Nigeria. Four localities were purposively selected from the stratified localities in Lagos State based on the digital divide. The study, therefore, selected Surulere, Bariga, Ikotun, and Badagry in this regard.

The youth involved in cybercrime is the unit of analysis. The study categorised youth involved in cybercrime as individuals who were aged between 15 and 30 years and engaged in cybercrime. A total of 48 were selected through guided referral method that was aided by other youth and cybercafé managers.

40 In-depth interviews (IDI) were conducted with youth involved in cybercrime (including those in the nests of the enforcement agencies). The 40 youth involved in cybercrime were selected through snowballing, informal personal interaction and observation. The selection of the 40 respondents was based on the fact that the population of youth involved in cybercrime is not readily known. The choice of the selection process was based on the fact that a familiar and conducive environment must be created for youth involved in cybercrime for them to divulge relevant information aside from the establishment of a relationship of trust.

Eight case studies each of successful youth involved in cybercrime were also conducted. In addition to the above. The secondary source of data were scam e-mails collected from potential victims of Internet scam and email correspondences with youth involved in cybercrime.

The qualitative data generated through IDI and case studies were analyzed with the use of content analysis and ethnographic summary that was enhanced with computer analysis.

Findings

Factors Encouraging Youth Involvement in Cybercrime

The survey shows that there are various factors responsible for the involvement of youth in cybercrime. These factors are poverty, defective socialization, access to the Internet, peer pressure, frustration and covetousness among others.

Knowledge and Accessibility of the Internet

From the data gathered, results showed that accessibility of technology is one of the major factors responsible for youth involvement in cybercrime. All of the respondents stated that accessibility to technology, especially through the computer, is a valid factor. According to one of the respondents,

"Of course, a farmer cannot go to the farm without the necessary tools such as hoe, and cutlass. Well, this is not what a farmer can do, and this is certainly not for those that are not educated. Better put, those who are not computer literate. This is for only very few people. The Internet teaches you a lot of tricks, even when you are not perpetrating crime: It teaches you how to change IP address, how to become invisible on the network, how to access the websites that ordinarily cannot be accessed from within your network or country and others. We simply take advantage of all of this. With our own lap-top connected to the Internet, we are good-to-go (IDI/23/YICC, June, 2012)."

Poverty

Common to the responses of all the respondents is poverty. Almost all of the respondents affirmed that poverty is responsible for their involvement in cybercrime, while very few claimed that it was not responsible for their involvement in cybercrime. The entire studied population however said that poverty may be one of the factors, but it is not always solely responsible for youth involvement in cybercrime. According to one of them:

"Poverty did not cause it in all cases because there are people who are not poor, yet they are into yahoo. I, for example, have a good background, but I have chosen to do this on my own (IDI/23/YICC/June, 2012)."
According to Zembroski (2011), people in impoverished environment may gain success by perpetrating illegal acts, but poverty is merely a risk indicator of crime. It may create a condition where the youth may be unable to resist temptations posed by cybercrime or the Internet.

Unemployment
In the course of the interview, a little less than half of the respondents mentioned that unemployment is also a factor responsible for youth involvement in cybercrime. The researcher probed further on this since the respondents claimed to be students. One of the respondents thus replied:

Even as a student, I still need a source of income. I need money to do fine-boy. In America and Europe, there are employment opportunities everywhere, people go to school and work per hour (part time job). That way, they will not lack. They still send money to “Naija” even as students (CS/28/YICC/December, 2012).

It was also revealed that it is not only students that are involved in cybercrime; even graduates are into it. Most of the respondents who subscribed to unemployment as a factor blamed the government for not providing enough employment opportunities.

Family Background
Data collected also showed that family background is one factor responsible for youth involvement in cybercrime. There is a close interplay among family background and occupation of parents. Almost all the respondents strongly agreed that family background is one of the factors responsible for their involvement in cybercrime.

It can therefore be explained here that it is easier for a youth with a disadvantaged family background to be socialized into involvement in cybercrime by friends than youth who are well-do and better monitored. Such a youth may consider cybercrime as an option, opportunity or even an escape route from the prevailing suffering within his family.

Poor Parental Supervision
Another factor identified to be responsible for youth involvement in cybercrime is poor parental supervision, which may be associated with the profession of parents. A majority of the respondents subscribed to profession of parents as a factor responsible for the involvement of youth in cybercrime. In this regard, many of the parents work far away from home regardless of what they do and most times, till late hours of the day. This way, the child is at liberty to do whatever he wants till any period of the day. When the earning is poor, the parents provide less for the children and these children are easily cajoled by others into cybercrime. This suggests that the occupation of the parent can contribute to youth involvement in cybercrime in two ways: if the parent spends less time at home and/or if they earn less. These suggest that poor supervision owing to the occupation of parents is a strong determining factor of how much provision and time the children get from the parents.

One respondent said:

My mum is a very busy businesswoman that earns enough money, but with this, I earn my own money. Majority of us are not as lucky as I am, but in this jungle, we survive together (IDI/23/YICC/December, 2013).

Another said:

With what my parents do for a living, I will rather not disturb them. When I make enough, I even give them a part of it. I know of a guy whose parents made it through his online adventures (IDI/19/YICC/March, 2014).
Defective Socialization

Results also revealed that defective socialization is not considered a causative factor of involvement in cybercrime by the youth involved, but the fact remains that socialisation is a lifelong process that is initiated by the family and complemented by others within the society and larger world as the child grows. The finding affirmed that primary socialisation is not faulty, but secondary socialisation outside of the family is where the defect is rooted. A significant proportion of the respondents asserted that they were involved in it by choice as parents would never teach their children to steal. One respondent said:

Nigerian parents are really trying. They do their best in nurturing children, but when these children derail morally, the parents still get a share of the blame. I was not taught this at home; I chose to learn it and it has nothing to do with home training (IDI/20/ YICC/December, 2013).

Another said:

I don’t think so! (Further explaining) People from good home, brought up by parents with high moral standards are even into this business. As far as I am concerned, it is personal choice (IDI/23/YICC/June, 2012).

Another respondent then said:

It is not inadequacy of socialization, but by peer group influence and being too ambitious (CS/27/YICC/March, 2014).

Peer Influence

The results of the interview also showed that peer group influence is another factor that influences youth involvement in cybercrime. In the course of the interviews, almost all the respondents said peer group influence is one of the factors responsible for youth involvement in cybercrime. A majority of them claimed friends aided their involvement in cybercrime directly and indirectly.

One of the respondents said:

If you see your friend looking good, wearing good clothes, using an expensive phone, riding cars when you are not riding a bicycle, you will be forced to go his way (IDI/18 years/YICC/November, 2011).

Another corroborated thus:

I walked into the cyber cafe myself, but I learned the tricks from my friends. Peer influence is very strong, because they introduce one to cybercrime gradually. They teach you how to capitalise on the weaknesses of others and the opportunities provided by the Internet (CS/26 years/YICC/June, 2012).

Another further said:

At times, the peers may not teach you directly; you will learn indirectly by observing them. Majority of us started from dating and those who did not have the intention of cybercrime, would realise that chatting was not easy. Each time they try, they fail, but the young guy on the next system is chatting freely. Then, he asks and he is made to know that he should not bear his name and live in Nigeria. He is put through and it becomes a new identity and a new lifestyle altogether (IDI/24 years/YICC/November, 2011).

Frustration

Frustration has been viewed as a psychological process which comes as a result of the inability of an individual to achieve certain goals. This study explicitly showed frustration is another active factor responsible for the involvement of youth in cybercrime perpetration. A majority of the respondents strongly agreed to the fact that frustration could lead to consideration of cybercrime, especially where the parents are poor and the child is finding it hard to make ends meet on his own. Only a few of the respondents were
indifferent in their opinion about frustration being a factor to their involvement in cybercrime. One of the respondents said:

When a young man is frustrated as a result of lack of money, and cannot get simple things done, he might go into yahoo if he sees the opportunity (IDI/19/YICC/March, 2014).

Another respondent complemented this by saying:

When the condition one finds himself is unbearable, it is easier for other children to help one find a way out. They may not need to say a lot before one is convinced. This is easy to do, but requires plenty of time. If money would flow in, there will be time to spend online (IDI/24/YICC/Junecountry 2012).

Majority of the respondents were however of the view that frustration is a product of poverty; that is, frustration is connected to poverty.

**Covetousness and Greed**

The study further revealed that socio-psychological factors like covetousness and greed are other factors that may encourage involvement in cybercrime. While covetousness refers to wanting what belongs to others, greed means taking more than one needs. Invariably, the two point towards the absence of contentment. Only a few of the respondents agreed that these are strong indicators of youth involvement in cybercrime.

According to one of the respondents:

Youth of now-a-days want to have everything and when there is no means to achieve all they wish to have, they look for options. Cybercrime is a very attractive option in the sense that people can never know what you do, unless you tell them (IDI/23 years/YICC/December, 2013).

Another said:

When you are not contented with what you have and you compare yourself with other people, you will do yahoo oh… (IDI/19 years/YICC/November, 2011).

According to him:

Youth do yahoo to elevate their social status and they are usually too desirous and ambitious to achieve material things. They always want to have in excess and would go extra mile to achieve this as a youth involved in cybercrime (CS/28 years/YICC/December, 2014).

**Discussion of Findings**

<table>
<thead>
<tr>
<th>Matrix 1: Factors Responsible for Youth Involvement in Cybercrime</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Factors</strong></td>
</tr>
<tr>
<td>Greed /covetousness</td>
</tr>
<tr>
<td>Frustration</td>
</tr>
<tr>
<td>Poverty</td>
</tr>
<tr>
<td>Parental occupation</td>
</tr>
<tr>
<td>Internet</td>
</tr>
<tr>
<td>Peer Influence</td>
</tr>
</tbody>
</table>

*Source: Researcher-Generated*

From the diagram above, technology is the pivot factor as the involvement is totally dependent on the Internet. Peer influence is equally strong because the adventurous youth may find himself in a group that would facilitate the involvement in cybercrime based on the intensity of cybercrime and frequency on the
Internet. Therefore, the factors investigated in this paper are Technological (Internet); Economic (Poverty, Family background, and Unemployment); Social (Poor parental supervision, defective socialisation, and Peer influence) and Psychological (Frustration and Covetousness and Greed).

Jaishankar (2008), in his first two postulates of the space transition theory, asserts that a person with a repressed criminal behaviour in the physical space has high propensity in the cyberspace since they have identity flexibility, dissociative anonymity and lack of deterrence. The factors that promote cybercrime, as revealed by this study, can be categorized into four, namely social, psychological, economic, and technological. The technological factor is the pivot of all of the other factors. Without the aid of the Internet, cybercrime may not exist in Nigeria. The existence of crimes close to what we have tagged cybercrime would have been found in letter scam, pornography, and piracy and their existence would have been minimal and condonable.

Adeniran (2008) categorizes the factors into two: super determinant (the Internet) and distinct factors (political, economic and social). Nykodym, Ariss and Kurtz (2008) also assert that cybercrime is one of the symptoms of computer addiction. According to Young (1998) and Kenshaw (2005), there were an estimated 5.6 million computer addicts in 1997 and 18.9 million in 2005. The signs of addiction, according to Internet/computer addiction services, include:

1. Inability to predict the time spent on computer
2. Failure in the attempt to control personal use for an extended period of time
3. Possession of sense of euphoria while on the computer
4. Craving for more time on the computer
5. Neglect of family and friends
6. Feeling restless or irritated when not on the computer
7. Lying to people about computer activity
8. Having problems with school or job performance as a result of time spent on computer

Among other things, Nykodym et al. (2008) further claim that computer and the Internet have become useful tools for criminals. All types of criminals have been able to use the computer and the Internet to facilitate and ease the procedures involved in their crimes. The Internet is attractive to criminals for the following reasons:

1. The Internet extends the reach of the criminal.
2. The Internet helps criminals to easily investigate potential victims.
3. Criminals on the Internet feel safest online due to their ability to conceal and alter their identities.

Other factors like greed, frustration, poverty, parental occupation, and peer influence do not have enough foundation to stand on their own as rationale for youth involvement in cybercrime, unless when dependent on the Internet.

Several of the youth involved in cybercrime have poor economic backgrounds, but the poor background is not applicable to all cases of involvement in cybercrime. A few are also from well-to-do families and these few individuals are even more successful than the other youth involved in cybercrime. They are more successful because they have more opportunities and they also operate from a very safe environment that has been provided by their parents. Through this medium, they gradually gain economic independence.

Aside from the above, the dominant factor that has been identified is the accessibility of the Internet. The Internet in itself is enough reason for youth involvement in cybercrime. The tendencies for breaking online laws cut across all age groups (Pease, 2004; Lee, McCann, & Messenger, 2007; UNICEF, 2011). The knowledge of cybercrime increases when youth interact with others who have had contacts with others that are involved in cybercrime and have learned the tricks. These youth do not necessarily need to meet one another all of the time before sharing knowledge; the Internet serves as the tool for both the learning and also transfer of knowledge of cybercrime.

Furthermore, peer influence has been found to also be a potent factor in the involvement of youth in cybercrime. On the one hand, it facilitates and enhances the initiation into cybercrime culture and on the
other hand, it sustains the internalisation of the cybercrime culture. In this study, peer influence supersedes the influence of poverty and even psychological factors such as greed and frustration. Peer influence becomes very prominent in the face of inadequate socialisation. Therefore, inadequate socialisation as a factor responsible for accepting cybercrime culture becomes firm only when there is direct or indirect influence of peers who are involved in cybercrime. This is in line with the differential association theory which asserts that crime is learned through the process of communication with intimate groups and that it varies in frequency, duration, priority, and intensity (Bosiakoh and Andoh, 2010). In the same vein, space transition theory, as a specific theory of cybercrime, sees the opportunity to have multiple personality online and still maintain the “good boy” personality offline as a determinant factor in youth involvement in cybercrime (Jaishankar, 2008). The innovation diffusion theory of Rogers (2003) identifies the factors responsible for the birth of the Internet itself to include the need for innovation and cosmopolitanism. The birth of the Internet provided the opportunities for people, especially young individuals to identify with norms that are either favourable to the violation of norms and values or unfavourable to the violation of the norms and values. When there is access to the Internet and young people make the choice of identifying with the norms favourable to the violation of norms, they go all the way to learn more about it in the course of interacting with others. This is when the differential association theory gets connected with the innovation diffusion and invariably the globalisation theory.

Conclusion and Recommendations

Youthful exuberance plays a role in defining what the youth perceives the Internet as. To many, it is everything that includes an environment where one can exhibit all behaviours that the society could generally frown at with hidden identities. How a youth defines the Internet can be associated with what the child is exposed to and the knowledge of sites where ordinarily children are not expected to visit. The influence of peers who are also exposed to the Internet is very strong and can affect children of all classes, although it affects children from poor backgrounds more.

Based on these findings, the study has come up with many recommendations. These recommendations are directed at parents, the government, law enforcement agencies, and teachers at all levels of education. On the part of parents, it is expected that they monitor the places their children visit and the time they leave and arrive at home by stylishly and strategically supervising the things they do at home, especially when they are communicating on the telephone. They are also expected to check the behavioural dispositions of these youth. Where the parents are rich enough to provide wireless Internet services at home, the use of the Internet should be supervised within the wireless network. Parents should maintain administrator-client interaction among the systems, such that the parents will take charge of the administrator in order to monitor the sites visited. Within the same network system, certain sites must be restricted, especially sites where potential victims are found.

The government is expected to cultivate relationship with other countries on the issues surrounding the control of cybercrime. Through this relationship, they can formulate policies that would specifically address cybercrime. The need for collaboration is hinged on the fact that the Internet environment is borderless and represents the world with the highest population. These policies must have room for expansion and accommodation of other policies. The policies must also move at the same pace or almost the same pace with cybercrime. Setting up EFCC, ICPC, and SFU in addition to the Nigeria Police Force has proven to be inadequate. As a result, the government should establish a law enforcement agency tagged with a name that states that it is established to tackle cybercrime with agents selected from these already established agencies. These agents should also be made to undergo Hi-tech training in order to have a clearer and better understanding of cybercrime. Having done all these, the government should then pronounce the content of cybercrime law and state all offences that are in these categories.

While the government is working with the recommendations above, the already established law enforcement agencies should put in place internal engineering that would increase protecting capabilities and mastery of the use of the Internet. In addition to these, international trainings should be encouraged.
so that the agencies can keep abreast of information on the global menace of Internet. The latter is founded on the belief that cybercrime is also learned online where borders do not exist. Since it is a fact that all youth involved in cybercrime have basic education, that is, they are educated enough to read, write, and speak English language to a considerable extent, teachers at all levels of education should adopt the use of Internet for educational purposes. Notes should be distributed online and materials for academic works should also be encouraged to be shared online. The point here is that if more time is spent online for academic purposes, less time would be spent for vices that may include cybercrime.

Finally, advertisements, pop ups, and other media should be used online to campaign against cybercrime openly. In fact, it should go beyond the Internet by extending to the television and radio. In addition to this, bank management and control by the Central Bank of Nigeria and individual banks should adopt stricter measures in controlling the flow of money into the banks and away from the banks. Domiciliary accounts should be created for an individual on the basis of the supply of concrete identity and letters from organisations where they have been employed.

References
Adeniran, A. I. 2008. The Internet and the emergence of yahooboys sub-culture in Nigeria. The International Journal of Cyber Criminology. 2.2: 368-381.