

# SOCIO-ECONOMIC DETERMINANTS OF CYBER CRIME: IMPLICATION FOR SUSTAINABLE DEVELOPMENT

*Osayi, Kelechi K. & Opara, Ejimofor*

## **Abstract**

*The emergence of the cyber space has given rise to a new face of social relationship characterized by increased interaction among young people. This like, the physical space, has given rise to a peculiar form of criminality inimical to societal development. It is against this background that this paper aimed at examining the socio-economic determinants of cybercrimes among young people and its implications for sustainable development in Nigeria. This study was anchored on the premise of Differential Association and Space Transition Theories. It was conducted in Owerri Municipal Local Government Area with a sample size of two hundred and fifty (250). The 250 participants were chosen through simple random and purposive sampling techniques. The Questionnaire and In-depth Interview Schedule were the major instruments for data collection. Quantitative data collected were analysed using Statistical Package for Social Sciences (SPSS), while narrative quotes were used in the analysis of qualitative data. Findings from the study revealed that unemployment, crave for quick money, low income, bad company and poverty were the major determinants of cybercrimes. The study showed a Significant relationship between level of educational attainment and being a victim of cybercrime. It was therefore recommended among many others that the government should capitalize on the opportunities that abound in the cyber space to create job for the teeming number of young people in the country as well as help initiate, together with other stakeholders, sensitization programmes to educate people on the implications of cybercrimes to societal development in Nigeria.*

## **Introduction**

Each phase of societal development has been characterized by a unique pattern of crime. The breakthrough in digital technology has carried communication and commerce across the globe. This breakthrough has led to explosions of crime and criminality in the cyber space, therefore posing novel challenges to societal development. The prevalence of cyber-crime and its threat to Electronic commerce (E-Commerce) and critical infrastructure systems and indeed sustainable development have elicited serious global concerns (Ndubueze, 2009), equally of global concern is the ability of law enforcement to keep pace with its prevalence and sophistication. A consensus seems to be emerging

among researchers that existing legislations are not enough to effectively prosecute cyber criminals (Daramola, 2008; Jaishanker, Pang and Hyde, 2008; Kyungshick, 2006; Nayak, 2008).

As the criminal justice system grapples with the challenges of bringing within its purview cyber mis-conduct hitherto uncovered by law; the scope and dimensions of cyber-crimes keep increasing changing. Cyber-crime raises very critical security issues. Mansel (2005) observes that the cyber space raises issues that are fundamental to individual and collective human society and security. Brenner (2007), elaborating on the concept of cyber-crime noted that just like traditional crimes, for there to be cyber-crime, four (4) elements must be present; actus reus (The prohibited act or failing to act when one is under obligation); Mensrea (a culpable mental state); Attendant circumstances (the existence of certain necessary conditions); and harm resulting to person or property. The variants of cyber-crime are many, most common being phishing, hacking, identity theft, cyber stalking, securities fraud, online gambling etc. (Ndubueze, 2009). "Cyber-crime is emerging as a major criminological issue (Roberts, 2008: I). The first conference entirely devoted to cyber criminology also referred to as "virtual criminology" was held in Spoken Valley, WA, United States in October, 2006 (Jaishanker, 2007). Cyber-crime represents a new phenomenon in criminal activity, the globalisation of criminal conduct (Brenner, 2001). This globalization of criminal conduct as stimulated by the globalisation of the new information and communication technology (ICT) which created borderless free market, where cyber-crime has international repercussion (Foggeti, 2003). Li (2007: 22) opined that, "The network context of cyber-crime makes it one of the most globalized offences of the present and the most modernised threat of the future".

Furthermore, McAfee Virtual Criminology Report (2007) found that governments and allied groups were using the internet in cyber spying and cyberattacks Critical national infrastructure network systems such as electricity, air traffic control, financial market and government computer networks are targets. About 120 countries now use the internet for web espionage operations. Cyber assaults have progressed from initial curiosity probes to well-funded and well organized political, military, economic and technical espionage (Ndubueze, 2009). Concerns on the use of the internet for cyber terrorism are rising. There are hundreds of terrorist websites on the internet (Weimann, 2004). Terrorist groups frequently use the internet to communicate, raise funds and gather intelligence on future targets (Hydes, 2007). Evidence suggests that terrorists used the internet to plan their operations on September II, 200 I against the United States of America (USA). Mohammed Atter who led the attack made his ticket reservation online (Wilson, 2003). Peter Cheriff, a French citizen, was recruited by AI Qaeda over the internet while resident in France (Powel, Carsen, Walt, Gibson and Gerlin, 2005). Consequently, the proposal for the restructuring of the U.S Federal Bureau of Investigation (FBI) provoked by the September II, 200 I terrorist attack had its top priorities for the future as counterterrorism, counter-intelligence and cyber security as well as hi-technology crimes (Muller in Etter, 2002).

On July 30, 2009 relevant stakeholders in Nigeria gathered in Abuja to review an international convention on cyber-crime. The treaty was the first on the issue that deals with infringement of copyright, computer-related fraud, child pornography and violation of network security (Anuforo, 2009). Foggetti (2003) distinguishes cyber-crime from other criminal activities and underscores the nature of cyberattack. He observes that the distinguishing feature of cyber-crime is basically its cross-border nature. It is usually difficult to identify the *Locus Commissidelicti* (the place where the offence was committed) when the offender uses information and telemetric means to commit the offence. He further noted that the attackers may violate several computer systems with just one illegal access and carryout several unlawful operations on computers which are interconnected, but physically located in different countries or territories.

Internet Crime Complaint Centre (IC3) statistics graphically depicts the international trends of cyber-crime from January 1, 2004 to December 31, 2004; according to the source, IC3 websites received 207,449 complaints submission. This is a 66.6% increase over 2003 when 124,509 complaints primarily related to the internet were received. Internet auction fraud was the most reported offence constituting 71.2% of the reported fraud complaints (IC3, 2005). The latest report released by IC3 (2008) shows that it possessed more than 219,553 complaints in 2007. The total dollar loss from all reported cases of fraud was \$680.00 per case.

This was an increase from \$198.44 million in total reported losses in 2006. Statistics from other sources tend to support the increasing incidence of cyber-crime. Puliam (2005) found that attack on the government, financial services, manufacturing and health care industries cost over 50% in 2005. This exposes societies to the negative consequences of underdevelopment, especially the third world countries in the 21<sup>st</sup> century. In December, 2004 one in every 52 e-mails contained a malicious security threat, such as virus attack. By June, 2005, it increased to one in every 28 e-mails. (eBay, 2006). The average annual loss reported by US companies more than doubled, from \$168,000 in 2004 report to \$350,424 in 2005 survey. Security survey (2007) found that financial fraud overtook virus attacks as the source of the greatest financial loss. Insider abuse of network access or e-mail (such as trafficking in pornography or pirated software) edged out virus incidents as the most prevalent security problem with 59% and 52% respondents reporting each respectively.

Furthermore, in the analysis of prosecution of network attack from 1999-2006, the Economic and Financial Crimes Commission (EFCC) found that individual attacks caused as much as \$10 million in damages to individuals. Organizations suffered the greatest financial loss and damage, more than \$1.5 million per occurrence; this is very inimical to the country's drive to her vision 2020:20. However, 84% of these crimes could have been prevented if the identity of the computers connecting to the web were checked in addition to user I.Ds and passwords (EFCC reports, 2007). A survey of 1,150 internet users in Lagos revealed that 94% of the respondents felt that identity theft is a serious problem. The survey reinforced the fact that the much bigger story was the amount of

money that is not getting spent. As stories of identity theft became more common, internet users are becoming less confident about making purchases online. It also found that a majority (50%) of internet users avoided making purchases on the internet because they were afraid that their financial information could get stolen. Almost half (49%) of internet users who were worried about their financial information getting stolen said that they did not make purchase on the internet (SIA digital Confidence Index Survey, 2006).

The internet has also witnessed an influx of sexual predators that use the platform to lure and victimize vulnerable children. A study on virtual (cyber) sex offending conducted in the United States involving 22 clients seen through a centre for online addiction revealed that all the clients were men who were arrested for engaging in sexual misconduct with minors using the internet. They aged 34 to 48 with mean of 38.5% who were employed in white-collar jobs mainly as engineers, doctors or lawyers, 17% were blue collar workers mainly working in factories, 15% were unemployed and 10% had some disabilities. In all cases, clients partook in paedophilic themed adult client rooms, unknowingly chatting with a Federal agent or police officer who posed online as a minor (Young, 2008).

In their study of the role of internet access points in the facilitation of cyber-crimes in Nigeria Longe and Chiemeké (2008), used statistical and simple random sampling to select a total of 50 cyber cases across four locations in South-Western Nigeria and analyzed a total of 232 validly filled and returned questionnaires. The study revealed that spamming activities remained prevalent among Nigerian internet users and that cyber cafes, more than any other internet access point, had facilitated cyber-crime. The study also found a steady increase in the use of the internet for news, travel information and sports and a decline in pornographic viewing which they attributed to content future used by most cyber cafes.

A survey conducted by IT news Africa in December, 2008, with subjects drawn from information and communication technology comprising, Christian society, policy makers, and the general public, revealed widespread concern over Nigeria's battered image across its borders because of high level and sophisticated incidences of cyber-crime. The respondents were worried that internet pornography, abuse of online visa application and online banking, among other felonies were on the increase in the country (IT news Africa, 2009). Cybercrime incidences and statistics from some African countries, most Particularly, Nigeria, Ghana and South Africa have damaging impact on images and economies of these countries.

### **The Problem**

One of the first publicised cyber-crimes occurred in November, 1988 in the United States. A 23years old student, Robert Morris, launched a virus (Morris worm) on the internet. Over 6,000 computers of the estimated 60,000 systems linked to the internet at that time were infected. It cost about \$100 million (US Dollars) to repair the infected systems. Morns got a sentence of 3years probation and a \$10,000 fine (StanBaugh, Beaupre, Icove, Baker, Cassedey and William, 2001). In 2008, companies worldwide lost more than 1

trillion, U.S dollars on intellectual property due to data theft and cyber-crime (McAfee 2009).

Cyber-crime is a widespread and growing global problem. According to the 2008 world internet crime report released by the internet crime complaint center (IC3, 2009); internet related criminal activities resulted in about \$264.4 billion reported losses, showing a significant increase from \$239.1 billion in 2007. A majority of the 72,940 cases referred for investigation by IC3 involved 'alleged fraud and had a median financial loss of \$931.0. Again, there is an increase from \$239.1 billion in 2007. The details of the report showed that; perpetrators were predominantly males (77.4%). The majority of the reported perpetrators were from the United States, but a significant number were located in the United Kingdom (UK), Nigeria, Canada, China and South Africa. The United States with 61.1 % of reported cyber-crimes, top the list of cyber-crime prone countries, followed by the U.K (10.5%) then Nigeria (7.5%), Canada (3.1 %), China (1.6%), South Africa (0.7%), Ghana (0.6%), Italy (0.5%) and Romania (0.5%). Males comprised 55.4% of the complainants nearly half were between the ages 30-50. While most were from the United States, the IC3 received numerous complaints from Canada, United Kingdom, Australia, India and France. Male complainants reported losing more money than females at a ratio of \$1.69 to every \$1 lost per female. Electronic mails (E-mail) at 74.0% and web pages at 28.9% were the two primary vehicles for the fraudulent contacts.

Studies show that over 80% of all E-mail is spam (Dickson, 2008). Children are not exempted from cyber-crime victimization. According to the Iowa Internet Crime Against Children Taskforce (2009), 1 in 7 children between the ages 10-17 are sexually solicited online. Child exploitation occurs in all income groups and cultural backgrounds (Ndubeze, 2009). The internet contains about 372 billion online pages of pornography (Mach and LiederBach cited in Mears, Manichi, Gertz and Bratton, 2008).

Cyber-crime has joined the list of problems plaguing Nigerian, and impeding her growth and development; Culminating in the listing of Nigeria as the third on the roll of top ten cyber-crime host spots in the world by a 2008 internet crime report (IC3, 2009). The enormity of this problem can be better appreciated when we consider the fact that in spite of several interventions made by the Nigeria Government in tackling cyber-crime, Nigeria has for three consecutive years (2006, 2007 and 2008) ranked third on the list of world cyber-crime perpetrator countries. Again, the latest IC3 data released recently showed a rise in cyber-crime in Nigeria 5.7% in 2007 to 7.5% in 2008 of world reported cases (IC3, 2009).

The erstwhile EFCC Boss in Nigeria, Ribadu (2007: 15) traced the origin of cyber-crime and criminality in Nigeria, when he declared in West African sub-regional meeting on advanced fee fraud that:

*In no time the traditional Nigerian value of honesty, integrity and hard work faced its rudest challenge as this new culture of dishonesty eroded all that was admirable and noble about us*

*especially in our urban conurbation. Scammers became the new Princes of achievement and the symbol of excellence, living well on stolen funds. In the face of tepid law enforcement environment, the late 90s announced a curious interface where crime and technology became engaged in an incestuous intercourse with the emergence of mobile telephone and the internet around the year 1997. Suddenly, the problem escalated faster and cheaper in the face of masked identities of the perpetrators who found cosy shields in the anonymous ambience of the cyber space.*

The phenomenal growth in the number of internet users around the world has increased the number of potential vulnerabilities of cyber attacks. Internet world statistics (2009) puts the number of internet users around the world at 1,574,313,184 (approximately 1.5 billion) as at December 31, 2008. The statistics further showed that in Nigeria, internet users grew from 200,000 (two hundred thousand) in 2000 to 10,000,000 (ten million) in 2008. Moritz (2008) observes that Nigerians access the internet in many ways; 53% through Very Small Aperture Terminal. (VSAT)-link, 19% through wireless microwave links and 14% through Digital Subscriber Line (DSL). Many of these sessions are through cyber cafes as very few Nigerians own personal computers (Ndubueze, 2009).

Awareness of cyber security in Nigeria started with the press and covered all crucial areas (Udotai, 2008). As a critical intervention, the Federal Government of Nigeria in 2004-established a cyber-crime working group known as the Nigeria Cyber Working Group (NCGW), comprised all key law enforcement, security, intelligence and information communication technology (ICT) organizations. Consequently, former President, Olusegun Obasanjo on June 5, 2006 signed a new law (Advanced Fee Fraud and other related act, 2006) to combat cyber-crime and fraud related offences in Nigeria (E-Nigeria, 2006).

Former EFCC Chairperson, Mrs. Farida Waziri, in 2008 stated that the commission arrested 136 cyber-crime suspects in 28 raids across Nigeria. She noted that 60 suspects were arrested in the South-West, 39 in the South-East, 26 in the South-South and 11 in the Entire North (Olapu, 2008). This breakdown indicated that the South-East ranked second behind the South-West, as region prone to the activities of cyber criminals than the rest of the zones in Nigeria. Recently, the EFCC arraigned 58 suspects in court for various cybercrimes. Out of this number, seven (7) were charged with operating cyber cafes not registered with the commission and for failing to obtain the particulars of their customers, required by law (Nwosu, 2008). The war against cyber- crime is far from being over. Uwaje (2009:27) projects that "Cyber-crime and cyber security activities will increase by about 53% in the next decade (2010-2015) worldwide." Despite government's intervention, the problem of cyber-crime has continued to escalate. Olapu (2008) opines that cyber-crime is at an all-time high rate in Nigeria, as cyber cafe owners sometimes collaborate with fraudsters. He further stated that, internet services being offered by

Starcomms, Zoom mobile, Visa phone, Multi-links and other telephone operators also provide venue for cyber-crime commission. Some cyber fraudsters aged between IS. 25years also carryout these illegal activities in their homes and hotel rooms (Ndubueze 2009).

The former speaker of the Nigerian House of Representatives, Mr. Dimeji Bankole warned that the high incidence of online fraud involving Nigerians could delay the Country's vision to rank among the best 20 economies of the world by the year 2020 (Ameh, 2009). Despite the fact that cyber-crimes have become a serious problem in Nigeria, there is no available statistics on its patterns and trends. There is not reliable data on the social and economic determinant of cyber-crimes. This study will therefore, attempt to fill the gap in the study of cyber-crimes in Nigeria by focusing on the Social and economic determinants of cyber-crimes and its implication for sustainable development in Owerri Municipal Local Government Area of Imo State. .

### **Objectives of the Study**

Consequent upon the foregoing, the major objectives of the study include:

1. To ascertain the types of cyber-crimes in Owerri Municipal Local Government Area of Imo State.
2. To ascertain the economic factors that necessitates the occurrence of cyber-crimes in Owerri Municipal Local Government Area of Imo State.
3. To discover the social factors that give rise to cyber-crime in Owerri Municipal Local Government Area in Imo State.
4. To ascertain the most effective and efficient ways to curb the incidence of cyber-crime in Owerri Municipal Local Government Area of Imo State.

### **Theoretical Framework**

The Differential Association Theory of Sutherland (1939) and the Space Transition Theory of Jaishanker (2007) provide analytical framework for this study. A combination of the two provides an ideal context in which one can understand the Socio-economic determinants of cyber-crime. Cyber technology is complex and requires some expertise to manipulate. An individual needs to learn beyond the basics of computer programming to manipulate the cyber space. Cyber-crimes take place in the cyber space where the offenders are less likely to be tracked.' The differential association theory enables us understand fully the process involved in learning and reinforcement of the techniques of cyber-crime and how these constitute, to a reasonable extent, a "push factor to cybercrime commission: In Nigeria where there is no serious pro-active mechanism to checkmate cyber-crime, cyber criminals still hit their targets, amass wealth and receive the approval of their admirers.

The Space Transition Theory tends to cover some aspects not captured in the Differential Association Theory. Space transition basically involves the movement of persons from one space to another. Cyber criminals behave differently when they move from the

physical space to the cyber space, the relative anonymity the cyber space offers as well as the relative speed with which a target could be hit are strong motivations for cyber-crime commission. Some terrorist groups are known to recruit and train their members online to carryout attack in the physical world. Some criminal groups in Nigeria who operate in the physical space may conflict with those of the cyber space. For example, one may be lured easily into disclosing some personal information on the internet by an impersonator than when the person comes physically, Therefore, the differential association and space transition theories were adopted as the theoretical framework to guide this study, because both of them are the most relevant, suitable and appropriate theories for this nature of study.

### **Study Hypotheses**

The following hypotheses were formulated to guide this study;

- i. There is a significant relationship between respondents' occupation and their perception of people's involvement in cybercrime
- ii. There is a significant relationship between respondents' level of educational attainment and their tendency of being victim of cybercrime.

### **Methodology**

The area of this study was Owerri Municipal Local Government Area of Imo State. Owerri Municipal is one of the three (3) councils in Owerri Imo State. It is located in South-East Nigeria with an area of 58 square kilometers (km<sup>2</sup>). The 2006 Nigerian census indicated that there are 62,405 males and 64,807 females in Owerri Municipal Local Government Area of Imo State. Thus, there are 127,212 persons in Owerri Municipal Local Government Area (NPC, 2009:834 & 835). The target population for this study included persons between the ages 18 and 64. Besides, the age category covers majority of cyber cafe users in Owerri Municipal Local Government Area. It is very rare to find people over the age of 65 years patronizing cyber cafes. The sample size was 250.

The purposive sampling technique and the simple random sampling technique were used for this study. The purposive sampling is a variant of the non-probability sampling technique (Oranye, 2003) was employed in choosing two (2) cyber cafe's from each of the five (5) communities that make up Owerri Municipal Local Government Area. Bringing the total number of cyber cafes surveyed to ten (10). The simple random sampling is a type of probability sampling technique (Aniekwe, 2005). The balloing method of the simple random sampling technique was adopted in selecting twenty-five (25) cyber cafe users from each of the ten (10) cyber cafe's earlier chosen to make up 250 respondents to whom the questionnaires were administered. While ten (10) cyber cafe operators were selected for the in-depth interview, bringing the total number of respondents for the study to 260.



## Findings

A uniform set of 250 questionnaires were administered out of which four (4) were wrongly filled. Thus, bringing the total number of correctly filled and returned questionnaires to 246. Also the in-depth interviews were successfully conducted with ten (10) cyber cafe operators. Therefore, 246 correctly filled and returned questionnaires and data gotten from the IDI were used for analysis in this study.

### Types of Cybercrimes in Owerri Municipal Local Government Area

TABLE 1: Distribution of Respondents on the Most Common Type of Cyber Crime

| Response      | Frequency  | Percentage |
|---------------|------------|------------|
| Hacking       | 55         | 22.4%      |
| Cracking      | 8          | 3.3%       |
| ATM Fraud     | 88         | 35.8%      |
| Pornography   | 59         | 24.0%      |
| Fake Identity | 20         | 8.1%       |
| Virus Attacks | 4          | 1.6%       |
| Don't know    | 12         | 4.8%       |
| <b>Total</b>  | <b>246</b> | <b>100</b> |

*Source: Field Survey, 2011.*

The above table indicates that 35.8% of the respondents identified ATM fraud as the most common types of cyber-crime. The table further shows that 24.0% of the respondents affirmed that pornography is the most common type of cyber-crime in Owerri Municipal Local Government Area. An IDI respondent responds thus;

*There are different types of cyber-crime in Owerri, but the most common I think, is ATM fraud. One thing you must understand is that everybody has his own format. It all depends on how smart you can be. (Male, Educated, 26 years).*

This is however at variance with submission of another IDI respondent who stated that, "the most common type of cyber-crime in Owerri is pornography. Even many adults come to this cafe to embarrass themselves, watching naked men and women on the internet". It can be extrapolated from the data presented above, that ATM fraud and internet pornography are the most common types of cyber-crimes preponderant in Owerri Municipal Local Government Area.

Economic Determinants of Cybercrimes in Owerri Municipal Local Government.  
Distribution of Respondents on the Major Economic Determinants of cybercrime

| <b>Response</b>     | <b>Frequency</b> | <b>Percentage</b> |
|---------------------|------------------|-------------------|
| Unemployment        | 108              | 43.9%             |
| Poverty             | 98               | 39.8%             |
| Low Income          | 25               | 10.2%             |
| Electronic Commerce | 12               | 4.9%              |
| Don't Know          | 3                | 1.2%              |
| <b>Total</b>        | <b>246</b>       | <b>100</b>        |

*Source: Field Survey, 2011.*

The table above shows that 43.9% of the respondents identified unemployment as the major economic determinant of cyber-crime. Other economic determinants as revealed by the study include; Poverty (39.8%), low income (10.2%), and electronic commerce (4.9%), while 1.2% of the respondents said that they did not know the major economic determinant of cyber-crime. Data from the IDI corroborated the submission on the table that unemployment (43.9%) is the major economic determinant of cyber-crime with the following assertion:

*The major reason why people commit cyber-crime is because of no job. If there were jobs, at least they will not engage in the act. But there are also people who are into the act for the fun of it. (Male, Programmer, 30 years).*

Another respondent stated that.

*Unemployment is already a problem in Nigeria as a whole, so one can actually say that it is a major cause of even cyber-crime. (Male, Educated, 28 years).*

The data above shows, therefore, that unemployment is the major economic determinant of cyber -crime in Owerri Municipal Local Government Area.

### Social Determinants of Cybercrimes in Owerri Municipal Local Government Area

**TABLE 3: Distribution of Respondents on the Major Social Determinants of Cyber Crime .**

| Response              | Frequency  | Percentage |
|-----------------------|------------|------------|
| Crave for quick money | 125        | 50.8%      |
| Bad company           | 41         | 16.7%      |
| Poor value system     | 30         | 12.2%      |
| Parental negligence   | 25         | 10.2%      |
| Peer pressure         | 20         | 8.1%       |
| Corruption            | 5          | 2.0%       |
| <b>Total</b>          | <b>246</b> | <b>100</b> |

*Source: Field Survey, 2011.*

The table above shows that 43.9% of the respondents identified "crave for quick money" as the major social determinant of cyber-crime in Owerri Municipal Local Government Area. Other social determinants identified by the respondents include; bad company (16.7%), poor value system (12.2%), peer pressure (8.1%), and corruption (2.0%). An IDI respondent posited thus:

*Everybody wants to make money, buy good cars. Build exotic houses and all that. Crave for quick money is the reason for all these Cyber-crime and other crimes too. (Female, Educated, 25 years).*

The foregoing shows that the "crave for quick money" is the major social determinant of cyber- crime in Owerri Municipal Local Government Area of Imo State.

#### **Test of Hypotheses**

**Hypothesis one:** "There is a significant relationship between occupation and perception of the people's involvement in cybercrimes". Data on table 4 formed the basis for testing hypothesis one.

**Table 4: Distribution of respondents on whether occupation influences people's perception of cyber crimes**

| Occupation                   | Low income | Unemployment | Poverty  | Total      |
|------------------------------|------------|--------------|----------|------------|
| Unemployment                 | 4          | 2            | 6        | 31         |
| Business/Trading             | 9          | 20           | 15       | 4          |
| Artisan                      | 1          | 3            | 0        | 4          |
| Teaching                     | 4          | 12           | 5        | 21         |
| Civil/Public servant         | 8          | 17           | 10       | 4          |
| Student                      | 14         | 64           | 25       | 103        |
| Self employed                | 1          | 1            | 0        | 4          |
| <b>Socio-economic status</b> |            |              |          |            |
| <b>Total</b>                 | <b>41</b>  | <b>138</b>   | <b>6</b> | <b>240</b> |

*Field survey, 2011*

The computed value of chi-square is 9.757, while the table value of chi-square at 0.05 level of significance with a degree of freedom (DF) of 12 is 21.026. Since the calculated chi-square value is less than the critical value the researcher rejected the alternative hypothesis. It follows therefore that there is no significant relationship between occupation and perception of people's involvement in cyber crime in Owerri municipal local government area.

**Hypothesis Two:** "There is a significant relationship between level of educational attainment and being victim of cybercrime". Data on table 5 formed the basis for testing hypothesis two.

**Table 5: Distribution of respondents on the relationship between educational attainment and being victim of cyber-crime.**

| Level of educational attainment | Hacking   | Cracking  | ATM Fraud | Fake Identity | Virus Attacks | Pornography | None      | Total      |
|---------------------------------|-----------|-----------|-----------|---------------|---------------|-------------|-----------|------------|
| No Formal Education             | 0         | 0         | 4         | 1             | 0             | 2           | 1         | 8          |
| FSLC                            | 1         | 0         | 2         | 0             | 1             | 1           | 0         | 5          |
| WASC/GCE/SSCE                   | 6         | 0         | 11        | 25            | 2             | 20          | 17        | 81         |
| OND/NCE                         | 4         | 6         | 11        | 7             | 4             | 3           | 10        | 45         |
| B.Sc./HND                       | 12        | 5         | 32        | 8             | 3             | 7           | 6         | 73         |
| M.Sc./Ph.D.                     | 2         | 4         | 3         | 4             | 1             | 2           | 1         | 17         |
| <b>Total</b>                    | <b>25</b> | <b>15</b> | <b>63</b> | <b>45</b>     | <b>11</b>     | <b>35</b>   | <b>35</b> | <b>229</b> |

*Field survey, 2011*

The computed value of chi-square is 68.012 while the table value of chi-square at 0.05 level of significance with a degree freedom (OF) of 30 is 43.773. Since the computer chi. square value is greater than the table value, the researcher accepted the alternatives hypothesis. It implies that there is a significant relationship between level of educational attainment and being victim of cyber crime in Owerri municipal Local Government area.

### **Discussion of Findings**

It was discovered in this study that A<sup>TM</sup> fraud was preponderant in Owerri Municipal Local Government Area. This was followed by pornography, hacking and fake identity. Earlier studies by IT news Africa (2008), Jaishanker (2009), EFCC report (2007) and Ndubeze (2009) all corroborated this finding. Pornography ranked third in the types of cyber-crimes that respondents have ever fallen victim of. This shows a decline in pornographic activities on the internet. Longe and Chiemeké (2008) corroborated this finding when they observed that there is a decline in pornographic viewing on the internet.

The study also identified unemployment as the major economic determinant of cyber- crime. This negates Chawki (2005), Pant (2008) and Long & Chiemeké (2008) who posited that the upsurge in cyber-crime can be attributed to factors such as; rapid increase in the number of internet users, high level anonymity and the growing number of computer technology. This study further reveals that, the "crave for quick money" is the major social determinant of cyber-crime. Other social determinants of cyber-crimes discovered in this study are bad company and poor value systems.

The Differential Association Theory clearly explains the social impetus mustered by cyber criminals in cybercrime commission. This is revealed in the fact that cybercrime like -other crimes is socially learnt, with the intent to amass quick money from targets. However, the space transition theory's assertion on the impact of socio-structural causes of crime in the physical space (i.e, Unemployment), similarly determines cybercrime commission. This was supported by the findings of this study, that unemployment is the major economic determinant of cybercrime in Owerri municipal Local Government Area. This is not totally different from the case with crime on the physical space, where people suffer from the austere effect of socio-structural dysfunction.

### **Conclusion**

The study has revealed that the cause of crime in the physical space is to a large extent similar to the cause of cyber-crime. The rising level of unemployment and crave for quick money have been identified as major reasons for high level of cyber-crime. Many educated people who are unemployed resort to cyber-crime, channeling their expertise and skills to cyber criminality. From the findings of this study, it is very manifest that there is an urgent need for the reorientation and resocialization of the people on the imperatives of proper conduct on the internet irrespective of the anonymity it offers them; as this has massive implication on the Society's march towards the realization of sustainable development in the 21<sup>st</sup> century.

### **Recommendations**

Therefore, the following recommendations are put forth to help mitigate the scourge of cyber-crime and to enhance the chances of the society in achieving sustainable development;

1. The Government and relevant stakeholders should capitalize on the opportunities lurking around in the cyber space to create employment opportunities for the teeming number of unemployed persons in our society.
2. Current efforts at ensuring cyber security should be enhanced to meet the increasing rate of cyber-crime. This can be realized through an advanced training of law enforcement agencies on the use of sophisticated ICT apparatuses, for the checkmating of cyber-crimes perpetrators.
3. Relevant stakeholders in the society should pool resources together to organize sensitization programs for the youth and general public on the proper use of the internet and ICT for societal development.
4. The study of cyber-crimes should be given serious attention by Nigerian scholars and relevant agencies (Governmental and Non-Governmental in order to initiate appropriate strategies in combating the menace of cyber-crimes.
5. Parents and Guardians should work together to inculcate the right values in their children, wards and young ones around them; the values of hard work, diligence, integrity and honesty. When this is done, it will definitely be made manifest in the activities of the cyber space.
6. Cyber criminals should be prosecuted in the courts and if found guilty, be convicted and sentenced to no less than ten (10) years imprisonment.
7. In the face of increasing rate of social network sites on the internet, it has become imperative that a cyber space monitoring agency be established to entrench the development policy of the country on the cyber space. This is due to the changing scope of social interaction, which is largely driven by the sophistication of ICT in the 21<sup>st</sup> century.

### **References**

- Adelakun, A. O. (2001). *State of the world children*. New York: UNICEF Publications.
- Alan, M.S. (2007). *Strutting, struggling and saving: Economic Depression in Northern Nigeria Kano*; Bayero University Press.
- Bourne, C. and Berger, B. (2000). *No guns please we are children*. New York. UNICEF publication.
- Buck, M. (1999). *Street and Working children*. Kano. Royal Lux publication.
- Chukudozie, O. (2002). Education and the Nigerian Child in the *journal of social inquiry*: 42 (2) pp. 119- 121.
- Collingsourth, C. (2007). *Child prostitution and Hawking*, New York: Awake publishers.

- Dube, C. (2002). Education revolution in Kenya *journal of African countries*: Vol. I. No. 1 pp. 20-24.
- Ebigbo, R. O. (2001). *Charter on the Rights and welfare of the Africa child* Enugu. ANPPNCAN publisher. .
- Ejiro, P.O. (2005). *Child upbringing and care*. Enugu: Royal links publisher.
- Fekayo, I.G. (2007). *Silences in NGO Discourses: the Role of NGOs in Africa*, Oxford: Fulham.
- Gelles, B. (2003). *Sharing experiences for Growth in children of Africa*. Ibadan: Spectrum books. .
- Howling, N. (2001). Child abusers get off the Hook. *Journal of child rights*: Vol. 2, NO.3, pp.110-120.
- I.L.O, (2007). *World labour report Discover S*, March: 16 - 24.
- I.L.O, (2005). *Child labour Rights*. Retrieved, February 20, 2011 from [http://en.wikipedia.org/wiki/child\\_labour\\_right](http://en.wikipedia.org/wiki/child_labour_right)
- National Population Commission (2009). *Republic Federal of Nigeria Official Gazette on 2006 population census Result*. Issued 2nd February, 2009, No.2, Vol. 96.
- Nnonyelu, AU. (2009). *Sociological insights*: Ibadan. Spectrum books.
- Obikezie, A. (2001). Children in street begging, *Journal of social inquiry*: Vol. 2, No.3, pp. 5 -6.
- Okoye, N.N. (2001). Observing and Helping the falling child. *Journal of mother Theresa foundation*: Vol. 3, No.4, pp. 50 - 55.
- Oloko, B.A (1997). *Child labour in Urban Nigeria*. Kano: Bayero press.
- Omotosho, J.A. (1990). *Sexual abuse of children in Nigeria*: Uyo: Alafin publications
- Schlemer, B. (2000). *The exploited child* London: Zeal books.
- UNICEF (2003). Child Trafficking in West Africa. *Journal of Inquiry by UNICEF* Vol. 5, No.3, pp. 10- 13.
- W.H.O, (2002). *Analysis of Nigerian Response to child trafficking journal* of world health organization. Vol. 2, No.4, pp. 7 - S.