SOCIALLY STRUCTURE AND THE PRODUCTION OF YOUNG CYBER CRIMINALS IN NIGERIA

Edward Omeire U.
Federal University of Technology Owerri, Imo State, Nigeria

Charles Omeire O.
Michael Okpara University of Agriculture, Umudike, Abia State, Nigeria

ABSTRACT
The advent of information and communication technology (ICT) and the ensuing diffusion of internet in sub Saharan Africa have ushered in a new form of criminality commonly referred to as Nigerian scams or yahoo-yahoo. In recent times, there has been an upsurge in the number of youths involved in cybercrime. Using Robert Merton’s Social Strain Theory as a theoretical premise, the paper posits that socio-cultural pressure on youths to achieve pecuniary success and frustration arising from a sense of discrepancy between individual aspirations and legitimate means to realize these ambitions lead to the emergence of yahoo boys sub-culture in Nigeria. The paper recommends among other things value re-orientation, the enactment of appropriate legislation and job creation to cater for the army of frustrated youths who are easily recruited into this criminal enterprise owing to unemployment and structural inequality in the Nation.

KEYWORDS
Yahoo Boys, Cybercrime, Social Strain Theory, Internet.

1. INTRODUCTION
The advent of information and communication technology (ICT) in Africa and the ensuing diffusion of the internet in Nigeria have given rise to improved productivity, increased efficiency and improved livelihood to many disadvantaged communities.

ICT applications, such as, e-commerce, e-learning, e-health and e-government, are potent tools for accelerating development. This is because they can be deployed in delivering a wide spectrum of basic services in remote and rural areas. They can stimulate rural development, accelerate poverty reduction, improve health and increase agricultural production in developing countries.
Contrary to the general view that the internet will facilitate the much need development across the world, recent trends and development in the cyberspace have shown that the relationship between technology and society has proved not to be metaphysical but quite materialistic instead (Kalathil and Boas, 2003). The positive consideration of ICT often ignores the odds that the varied uses can constitute a threat to its rightful use (of technology) thereby undermining social relationship and progress (Carey, 1988). One of such threats is the emergence of a new form of criminality commonly referred to as Cybercrime. Cybercrime represents the ugly alley of information society.

Cybercrime refers to any unlawful behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network. It represents all activities done with criminal intent in cyberspace (Karofi & Mwanza, 2006). Cybercrime has been given local nicknames across West Africa. For instance, in Ghana, Cameroon and Nigeria, it is referred to as ‘Sakawa’, ‘Faymania’, and Yahoo Yahoo respectively. (Adeniran 2008; Longe and Chimeke 2008). Cyber criminals take advantage of system weakness, anonymity, ignorance and gullibility on the part of users to commit their wicked crimes.

Cybercrime or Yahoo-Yahoo as it is called in Nigeria is an offshoot of advance fee fraud which became trendy in the early 90s. It is closely linked to early days of internet diffusion in Nigeria when yahoo mail and yahoo Instant Messenger was the most popular means used by these individuals to send unsolicited bulk e-mails to gullible victims.“Yahoo-Boys” thus became the derogatory tag given to young boys (sometimes girls) who engage in internet fraud (Asokhia, 2010). They are also known as Guymen. Their operations are usually well structured and organized. As an organized crime network, reciprocal engagement, joint endeavour, and shared repertoire of best practice and techniques are key attributes (Oludayo & Ibrahim, 2011).

Furthermore, the variety of scams perpetrated by the Yahoo boys combined with their innovation and technique in many ways make them out as “entrepreneur” although used negatively (Carter and Jones-Evans, 2012).

Cybercrime has become a global problem and has caused immense loss to both businesses and individuals globally. Several studies and documents (McAfee, 2013; Norton, 2013 and Ponemon, 2011, 2012, 2013;) have examined the costs and losses caused by cybercrime. Between 2006 and 2007, financial losses occasioned by cybercrimes in the United States alone increased dramatically from $52.5 million in 2006 to $67 million in 2007 (Richardson, 2008). Per Norton Cybercrime Report (2011) over 74 million people in the United States were victims of cybercrime in 2010. These criminal acts resulted in $32 billion in direct financial losses. In 2015, Lloyd’s a British insurance company estimated that cyber-attacks cost businesses as much as $400 billion a year, this includes direct damage plus post-attack disruption to the normal course of business. Forecasts by some IT experts and vendor over the past year put the cybercrime figure as high as $500 billion and more.

The most significant loss from cybercrime is in the theft of IP and business private information. IP theft is not just a cybercrime, rather it is a fundamental problem for the information society. Per US Department of Commerce report (2011) IP theft costs US companies $200 to $250 billion annually. On the other hand, the Organization for Economic Development (OECD) estimated that
counterfeiting and piracy costs companies as much as $638 billion per year (US Department of Commerce report, 2011).

2. LITERATURE REVIEW

Cybercrime is not indigenous to any country rather it is a global citizen. It cuts across national borders, producing a new area of illicit human enterprise and undermining the prospect of applying laws based on geographic boundaries. McConnel (2000), noted that cybercrimes differ from most terrestrial crimes in four ways namely: they are easy to learn; they require few resources relative to the potential damage caused; they can be committed in a jurisdiction without being physically present and they are often not clearly illegal. As such, cybercrime has become one of the major security issues for law enforcement agencies and the world in general.

Ribadu (2007), stated that the prominent forms of cybercrime in Nigeria are cloning of websites, false representations, internet purchase, fraudulent electronic mails and other e – commerce kinds of fraud. Salkowitz (2010) identifies three forces driving the world in this present age and these include the youth, ICT and entrepreneurship. These forces generate massive impact and drive the global economy in new directions and at very high velocity.

Many authors posit that cybercrime is one of the dominant forms of crime that is widespread among youths in Nigeria (Adeniran, 2008; Aransiola & Asindemade, 2011; Tade & Aliyu, 2011; Aghatise, 2006). Aghatise (2006), reveals that about 80% of cybercrime perpetrators in Nigeria are students in various institutions. While Ibrahim (2006) opines that cyber criminals in Nigeria are usually within the ages of 18 and 30 years, and are youths, who are outside the secondary schools, but are either in the university or are about to be admitted into the university. Lending credence to this, a study by Zero Tolerance (2006) indicates that cyber criminals are usually within the age of 18 and 30 years and they indulge in the crime to survive and have a taste of good life. DeMarco (2001), also noted that cyberspace make young people susceptible to risk of engaging in cybercriminal activity by providing open, uncensored and unregulated sites that provide information, directives and tools about hacking, network intrusion, and phishing procedures.

Wall (2001) opines that there is a strong relationship between youth’s social environment and the development of crime related habits. Giordano et al (2002), reveals that youths living under socio-economic deprivations, acquire more personal deficits, thus raising their chances of acquiring additional acumen for antisocial behaviours.

Although cybercrime is not an exclusive preserve of Nigeria, the rising incidence and involvement of Nigerian youths in cybercrime makes it a serious social problem that requires urgent attention.

This paper therefore, seeks to explore the nexus between social structure and the emergence of Young cyber criminals in Nigeria.

3. THEORETICAL FRAMEWORK

Theories are very vital tools in sociological analysis for they help in no small way in explaining or predicting social phenomenon. This paper adopts Robert Merton’s anomie theory as its theoretical premise. This theory aptly explains the underlying factors responsible for the emergence of young cyber criminals Nigeria.
Robert K. Merton was one of the leading sociologists of the 20th century. He contributed enormously to broad sociological theory by developing the model for structural analysis. Robert Merton work on crime and deviance is an attempt to adapt Durkheim's general view about anomie to specific social situations and circumstances.

Robert Merton in explaining the cause of deviance in American society, posit that crime and deviance arise from social structure, rather than the individual. He opines that deviant behaviour is created due to conditions in social structure of a society. Merton further argued that some people or groups engage in criminal behaviour because they are responding generally to the social condition in which they find themselves (Tierney, 2006).

Per Merton, the society create conducive environment which engenders crimes and produce criminals by emphasizing on goals and values without providing matching opportunities for realizing them. Whereas the society instructs all citizens to demonstrate unrestrained individualism in pursuit of pecuniary success, the opportunities for goal-attainment are not equally distributed. He further argued that the discrepancy between socially approved goals and the availability of lawful means to achieve pecuniary success pushes individuals to commit crime.

Merton drew attention to some ways in which individuals may adjust to the strains brought by their failure to achieve socially prescribed goals. The adaptation typology also referred to as the “plus-minus paradigm” are conformity (+ +) in which goals are accepted and pursued along with the cultural approved means; innovation (+ -) in which the goals are accepted but culturally approved means are rejected, and illegitimate means are created and used to achieve the goals; ritualism (- +) here goals are rejected and the cultural means are accepted; retreatism (- -) in which the goals and means are rejected and the individual lives in isolationism and may sometimes find succour in drug or alcohol. The last adaptation mechanism identified by Merton is rebellion (+ +) here the individual or group rejects both the societal goals and means and wishes to change the social structure (Haralambos and Holborn, 2008).

Whereas the anomie theory provides the theoretical underpinning for this work, we are anchoring our analysis on innovation adaptation mode. This describes a situation in which the individual accepts the culturally defined goal of the society (+) but rejects the legitimate means to attain the goal.

As it relates to Yahoo boys in Nigeria, this theory holds that given the high emphasis on material success in Nigeria, young people and individuals who cannot achieve cultural goal may resort to illegitimate means to achieve same. Analysed from this standpoint, it could be seen that it is the socio-cultural pressure on youths to achieve pecuniary success as well as the limited opportunities for attainment due to structural inequality in Nigeria society that propel youths to engage in cybercrime.

In Nigeria, youths are encouraged and socialized to crave for the good things of life (desired ends). In other words, from infancy they internalize the "Nigerian Dream" of wealth, big houses, big cars, and wild display of opulence. Over time, Nigerian youths have come to idolize the lifestyle of corrupt public officers who impudently dot the Nigerian socio-political landscape. These officials though corrupt enjoy community endorsement and are marketed by society as role models. They are awarded premier chieftaincy titles by traditional institutions and are given high recognition in religious sphere.
Whereas Nigerian youths are tacitly encouraging to emulate these role models, the legitimate means to achieving pecuniary success are very limited largely due to structural inequality and pervasive corruption in Nigeria (Adeniran 2008; Tade and Aliyu 2011).

In summary, it is these trajectories within Nigeria’s social milieu that puts pressure on youths to engage in cybercrime. As Ritzer (2008) points out, deviants often take the option of alternate, unacceptable sometimes illegal means of achieving socially approved goals.

4. METHODS USED BY CYBER CRIMINALS IN NIGERIA

Some of the methods used by Yahoo boys to carry out their fraud are outlined below.

4.1. “Come and Carry” or Advanced Fee Fraud

This is one of the foremost methods or format (as it is called by Yahoo boys) used by Yahoo boys to fleece money from their victims. Under this scheme, the yahoo boy sends out unsolicited bulk mails to numerous potential victims who are usually known as “Mugu” within the yahoo subculture. In the e-mail, the fraudster will claim to be a banker of a late expatriate or a vulnerable relative of a late head of state whose millions of dollars are trapped in a secret bank account known only to him (the banker). The e-mail recipient is promised a fortune if he acts as the next of kin of the dead man in question to facilitate the release of the said trapped fund. If the victim falls for this story he or she will be introduced to some bogus officials ranging from lawyers and sometimes government officials who will help in moving the said fund. As the transaction progresses, the fraudster occasionally demands certain fees from the victim to cover documentation, legal and occasionally bribe to facilitate the release of the money. The victims usually send several thousands of dollars and sometimes are lured to Nigeria to meet bogus government or bank officials at the end of the day they will not receive their anticipated fortune (Ige, 2008). Current studies reveal that, despite various information, campaigns on this issue, advance fee frauds are still growing with regards to both the number of victims and total losses Identity Fraud Survey Report (2008).

4.2. Over-Payment Scam

This scheme entails a lot of procedure. The first step taken here by the Yahoo boys is to locate an online merchandise, conference or hotel in Europe or America. Then he pretends to be a potential buyer, and subsequently he makes an over-payment for the goods either through cashier cheque or stolen credit card and then request that the over-payment be sent to his business associate in Nigeria Ghana or Malaysia. Under this scheme, the fraudster is not interested in the merchandise his main interest is the refund which is normally wired to him through wire transfer long before the credit card company detects that the card is stolen.

4.3. Online Dating and Romance Fraud

Here the fraudster joins several dating sites and creates fabulous profiles which they use to attract lovers. The main objective here is to extract money from the victim (Bureau of Consular Affairs, 2013). In the beginning, males dominated this format, even though they often employ the services of female associates that talk to victims on the phone or via webcam for authenticity. However, in recent times, with the advent of iPod and smart phones young girls known as Runs girls appear to have taken over this crime space.
Under this scheme, the perpetrator starts by initiating a romantic bond with the victim. This can flourish for weeks or even months through phone calls, chatting and exchange of pictures. This is done to build trust and increase vulnerability. Throughout this gestation period, the perpetrator usually does not ask for money or any favour. Once the perpetrator is convinced that the victim has fallen in love, s/he strikes. The most familiar scenario in this format is that the perpetrator frequently sends his or her victim (Lover) an email describing a horrible circumstance like robbery or road accident in which he is involved in. What follows is a series of requests for money from the perpetrator or his agents. The victim sends money out of pity, or concern for these ones they are hypothetically in love with. After a while, most victims become aware that they are dealing with con artist but not before they have lost huge amount of money to them.

5. CONCLUSION AND RECOMMENDATIONS

Although, information and communication technology (ICT) diffusion in Nigeria has given rise to enhanced productivity, social transformation and improved livelihood, it has also led to the emergence of a new social problem among youths.

Cybercrime among youths is a conspicuous symptom of institutional anomie. A situation in which pecuniary success is valued over hard work and honesty. This state emerged largely because of structural inequalities, blocked opportunities, Nigeria quota system policy and government neglect of youths which increases their vulnerability and proclivity to engage in cybercrime.

To check this nuisance ravaging our nation, the authors make the following recommendations

There is need for government to address the rising rate of youth unemployment in Nigeria by creating jobs and granting loans to youths who wants to start their own business. Again, retrogressive, one-sided policy such as Quota system which gives undue advantage to northerners should also be expunged from the constitution.

Furthermore, there is need for enactment of appropriate community and legislative sanction against corruption in the society. If corrupt persons are punished both at community level and national level, it will deter young people from participating in cybercrime. Above all, there is also need for value reorientation in the family, religious institutions and schools bearing in mind that the job of crime prevention is everybody’s business.

REFERENCES


