University of Ghana http://ugspace.ug.edu.gh
UNIVERSITY OF GHANA, LEGON

DEPARTMENT OF SOCIOLOGY

CYBER CRIME AND THE YOUTH IN GHANA: A STUDY OF THE SAKAWA CONUNDRUM IN ACCRA AND AGONA SWEDRU COMMUNITIES

BY

BELINDA SMITH
(ID. NO. 10155154)

A THESIS SUBMITTED TO THE DEPARTMENT OF SOCIOLOGY, UNIVERSITY OF GHANA, LEGON IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF A MASTER OF PHILOSOPHY DEGREE IN SOCIOLOGY

SEPTEMBER, 2011

University of Ghana http://ugspace.ug.edu.gh

DECLARATION

I, Belinda Smith, hereby declare that, except for references to other people's works which have been duly acknowledged, this research work is a result of my independent research carried out at the Department of Sociology, University of Ghana, Legon, under the joint supervision of Dr. Dan-Bright Dzorgbo and Professor Chris Abotchie. I also declare that as far as I know, this thesis has neither in part or in whole been published nor presented to any other Institution for an academic award.

Belinda Smith

(Student)

14th Sept 2011

Date

Supervisory Team:

14-09-11

Dr. Dan-Bright Dzorgbo (Principal Supervisor)

Date

14th Sept 2011

Professor Chris Abotchie (Second Supervisor)

Date

University of Ghana http://ugspace.ug.edu.gh

DEDICATION

To my wonderful family. You never stopped believing that I could do this. Thank you so much.

University of Ghana http://ugspace.ug.edu.gh

ACKNOWLEDGEMENTS

To Dr. Dan-Bright Dzorgbo and Professor Chris Abotchie, whose perceptive supervision led to the completion of this thesis, I thank you immensely. As my supervisors you guided my research with constructive criticisms, useful suggestions and comments. I appreciate the calls and reminders you continually gave me. I really consider myself fortunate to have been under your supervision. I am also indebted to the officers of the Ghana Police Service, despite your very busy schedules, always gave me time and access to very useful information. I learned so much from the stories you shared with me. To Mr. Charles Nelson, I thank you for all your important information and respect your fight against cyber crime. To my family, thank you for your support. To everyone else who contributed to bring this research to fruition, I humbly thank you.

University of Ghana http://ugspace.ug.edu.gh

ABSTRACT

In the past few years, cyber crimes and youth involvement in cyber crimes have engaged the attention of law enforcement agencies, the media and the general public due to the high prevalence of the crimes. Previous research in Africa has focused mainly on the Nigerian '419' scams and why youths generally indulge in criminal activities. The focus of this research was to examine, from a sociological angle, and from the perspective of selected theories, the motivations and reasons which encourage and influence the high predisposition for youth in cyber crimes or "Sakawa" as it is known in Ghana. The specific objectives were to explore the socio economic demographic backgrounds of youths involved in *Sakawa*, identify the different cyber fraud types that youths in Ghana engage in, examine the reasons and motivations of those engaged in cyber fraud, explore the practices and gains associated with cyber crimes and finally examine the responses and challenges of law enforcement agencies to curb cyber fraud. The methodology employed was qualitative, using snowball sampling method to select 10 cyber crime perpetrators, aged between 18 and 24 years, for an in-depth interview. Two key informants from the Ghana Police Service and Serious Fraud Office were also interviewed. The study areas were Accra, the capital of Ghana, and Agona Swedru, the district capital of Agona in Ghana. The data collected from the field was analysed and the research findings showed that respondents were from economically deprived backgrounds, youth perpetrators engaged in different types of cyber crimes, most respondents gave motivations ranging from a poor legal framework, profitability of the crime, family support and encouragement, low deterrence factor to few job opportunities. The research findings were consistent with the Differential Association and Strain theories and indicated that youth felt a disconnect between their economic goals and legitimate means of achieving them; and further that criminal behaviour is learned, and learned from association with close peers, also perpetrators used some neutralization techniques to assuage guilt. The ability to switch identities and the anonymity presented by the internet encouraged cyber delinquent activities. On the basis of these findings, the following major recommendations were made: there must be enactment of specific legal framework against cyber-crimes, to raise public awareness about the common modus operandi of perpetrators, formulation of proactive economic policies that could engender employment opportunities for the youth and the harmonization of laws against cyber crime at the domestic and regional levels. The research also makes recommendations for future areas of research.

University of Ghana http://ugspace.ug.edu.gh

TABLE OF CONTENTS

University of Ghana http://ugspace.ug.edu.gh

CHAPTER THREE

THOERETICAL FRAMEWORK AND LITERATURE REVIEW

University of Ghana http://ugspace.ug.edu.gh

CHAPTER FOUR

DATA ANALYSIS AND REPRESENTATION OF FINDINGS

University of Ghana http://ugspace.ug.edu.gh

CHAPTER FIVE

SUMMARY, RECOMMENDATIONS AND CONCLUSIONS

University of Ghana http://ugspace.ug.edu.gh

University of Ghana http://ugspace.ug.edu.gh

CHAPTER ONE

OVERVIEW OF THE STUDY

1.1 Introduction

The emergence of the computer and subsequently the internet is viewed as a significant symbol of modernity, and, indeed, as an engine for economic growth. Beginning from the industrial revolution of the 19th century to the last three or so decades, technology has increasingly become part and parcel of modern day living. Most human industries from Aviation to the Zoo have become progressively more dependent on one form or another of technology to function from day to day either at the frontline of activities or behind the scenes of business affairs.

The computer as an information and communication technology (ICT) has so many versatile uses. It is used for work processing, calculation, statistic researches etc. Its impact has been incredible for individuals, organisations, schools amongst others who employed the computer for social to business ventures. There is hardly any organisation without computers to facilitate their day to day activities. These days, computers are globally networked and therefore have improved and transformed how people interact and communicate with each other. They are quick and instantaneous and hence, have undermined traditional modes of communication like the postal mail, telegraphs, etc. The world has come to embrace such social network sites as Facebook, people blog on line on issues bordering on the mundane to critical political issues, Wikipedia offers information on general topics and even the recent release of previously sensitive and

University of Ghana http://ugspace.ug.edu.gh

confidential diplomatic documents on-line by the website Wikileaks is threatening relationships between governments.

However as much as computers and the internet have facilitated communication, it has also brought new ways of criminal activities. Crimes usually evolve with the time and therefore like all other human inventions, the computer has not only been a tool for progress but also has seen its application in deviance and crime. McCaghy (1980: 257) asserts that criminals have always adjusted their strategies to suit the technologies and opportunities of the time. The emergence of the computer and other high technology equipments like mobile phones, I-pads, etc have paved avenues for the genesis of novel types of crime. The 21st century has seen physical movement being replaced by electronic travel due to global networks and people can commit crimes without physically moving from their locations. This makes computer crimes characteristically different from traditional crimes. It should be noted that technology is truly a double edged sword that has transformed the classical and traditional forms of criminal behaviour.

The brand of crime committed with a computer or the internet is often referred to as computer crime, cyber crime or internet based crime. The widespread reach of the internet might have facilitated the transmission of information at a relatively cheaper cost but it also enabled the internet to inadvertly expose the entire world to a " highly 'criminogenic' environment" (Chua et al., 2007:706).

University of Ghana http://ugspace.ug.edu.gh

Attempting to tackle this new breed of crime is challenging traditional Law enforcement methods and it is against this backdrop that the United States of America set up the Internet Crime Complaint Centre (IC3) as a partnership between the National White collar crime centre and the Federal Bureau of Investigation (FBI) to combat cyber crime. This security organisation is to serve as a means of gathering information on internet related crime activities. The IC3 is also charged with collating global statistics on these crimes, publishing Annual Reports based on crime trends, alerting and educating consumers on new crime developments and tips on how to avoid falling victims (IC3 Report, 2007). The activities of cyber criminals cut across geographical borders even though it occurs in cyber space. As such, victims are also found across international borders. Consequently, no individual, organisation or state is immune to the likelihood or impact of cyber crime.

In terms of geographical and institutional impact, Cyber criminals and victims cross international borders and jurisdictions, and by itself, it is irrefutable that no individual, organization, state or continent is resistant to the possibility of cyber crime. As computerization and globalization continue to draw the world closer, Africa is also experiencing constant growth in internet user base coupled with poor security awareness (Olowu, 2009:6).

African countries in engaging in the Digital Revolution have also been drawn into cyber criminal activities. Nigeria is infamously known for cyber fraud which is commonly referred to as '419' or Nigerian letter scams. Nigeria for instance, has featured prominently on the Internet Crime Complaint Centre (IC3) report since 2001 at second position on the list of perpetrator Countries

University of Ghana http://ugspace.ug.edu.gh

after the United States which has remained at first position. Nigeria has however stayed at third position since 2007 to 2009 (IC3 Annual Reports 2007-2009). Other African countries that have featured in the IC3 perpetrator country list are South Africa, Cameroon and Ghana as seen in table (see appendix 1). Ghana is gradually gaining notoriety as a hub for cyber crime activities locally referred to as 'Sakawa'. As a result of this, Ghana joined the IC3 perpetrator country list in 2007 at tenth position but leaped two places to seventh position in the 2008 IC3 annual report. In 2009, Ghana moved further up to sixth place. This shows a steady yearly increase which partially provides justification for research into the phenomenon. This is a relatively new crime trend that is growing progressively within the borders of Ghana.

The drive to embark on this study stemmed from an emerging aspect to the conventional form of cyber crime. In the recent past, Ghanaians, most notably the youth are believed to be blending their reprehensible cyber scams with fetish or ritual performances. This is evident in some recent press stories with such captions as- **"Students Urged to desist from Occultism"** (Ghanaian *Times* 6th May, 2009) **and "Two Students fined for Cyber Fraud"** (*The Mirror* 18th July, 2009:27)**.** The general perception is that the spiritual fortification is required to ensure success and that ritual performances tend to conceal the perpetrator from the eyes of law enforcement agencies.

University of Ghana http://ugspace.ug.edu.gh

1.2 Statement of Problem

Many governments, policy makers and criminologists are warning that Africa is becoming a major source of cyber-crimes. Nigeria for instance is ranked as the leading nation in the region as the source of malicious internet activities and this is spreading across the West African sub-region. As a result of this, Nigeria has gained worldwide notoriety for the Advanced Fee Fraud or '419' scams. This has negatively impacted on its image on the global platform causing foreign investors to be wary of conducting businesses in that country.

Similarly in Ghana, Cyber crime or *sakawa* as it is locally referred to has in recent times, received significant and growing attention from the general populace and State anti-crime agencies. This is evident in frequency of its mention in the media, parliament, and pronouncements by government officials and non-governmental agencies. As a social problem, it damages the image of the country and the perception the international community have of Ghanaian citizens. Cyber crime also impacts negatively on investment opportunities. The Business Eye news journal (2009) reports that according to a press release from the United States Embassy in Accra, "Ghana ranks second after Nigeria on the list of African countries that US e-retailers rejected trade orders from last year". This poses a threat to local business people, business growth and also adversely affects Ghana's ability to participate in exports and e-commerce. It has been reported that Ghana is already suffering the consequences of cyber crime activities as it is presently blacklisted from carrying out electronic commerce transactions (ghanabusinessnews.com, 2009).

University of Ghana http://ugspace.ug.edu.gh

In addition, a number of media publications indicate that the demographic group which is perceived to be most heavily involved – the youth- creates even more cause for worry and concern as the youth not only symbolize the future of any nation but also its most vibrant and important human capital. Some of the media headlines read as follows:

"Sakawa scare- Educationist fear doom for Thousands of School Children, (*Daily Graphic* 13th May, 2009:1) - **"Politicians to Blame- For growing scourge of 'Sakawa',** (*Daily Graphic* 26th May, 2009:16), - **"Sakawa, The veiled monster",** (*Daily Graphic* 30th May, 2009:9) - **"sakawa menace: who is to blame?",** (*Christian Messenger* vol 23, nos 2.May 29th- June 10th, 2009:1)

This demographic group embodies future leaders, policymakers, parents, and indeed the human and social capital of the nation and their alleged involvement in *Sakawa* and other 'get rich quick' schemes does not indicate a happy, stable future society for the nation. The youth have also been reported in the papers to have dropped out of school or skipped school attendance due to cyber delinquent activities and thus negatively affecting the future intellectual capacity of the nation. Furthermore, they are reported to endanger their own lives and the lives of innocent citizens with related ritual and occult activities which are shrouded in secrecy.

Given these, the research seeks to study the emerging cyber crime or *sakawa* in Ghana to determine the nature and extent of this growing social problem in the society.

University of Ghana http://ugspace.ug.edu.gh

1.3 Objectives of Study

The main objective of the study is to explore from a sociological perspective, cyber fraud or *Sakawa* as it is locally referred to in Ghana mainly from the perspective of those directly involved in it.

More specifically, the study

1. Explores the socio-economic and demographic backgrounds of youths involved in *Sakawa;*
2. Identifies the different cyber frauds that the youths in Ghana engage in;
3. Examines the reasons and motivations of those engaged in the cyber fraud
4. Explores the practices and gains associated with the cyber crimes; and
5. Examines the responses and challenges of law enforcement agencies to curb cyber fraud.

1.4 Significance of study

This study is significant for a wide range of individuals, institutions, Governments and Non-governmental organizations (NGO) as well as law enforcement agencies. The study seeks not only to explore reasons motivating youth participation in crime but also to unearth the forms and dimensions of the *Sakawa* conundrum. It is believed this will subsequently aid in averting the menace. This is because it is easier dealing with the phenomenon when the basic motivations behind involvement are understood. Again, the internet offers its users anonymity and invisibility behind which perpetrators are able to commit crime without fear of quick apprehension. *Sakawa*,

University of Ghana http://ugspace.ug.edu.gh

even as a new social phenomenon is shrouded in myths and secrecy. It is therefore vital to go behind the 'veil' so to speak and uncover those and what goes on behind it.

The study will also serve as a critical investigation as this particular dimension of cyber crime affects a particularly vulnerable demographic group, the youth. Additionally, as there is yet to be a comprehensive youth policy in the country, the information gathered in this research should contribute towards ensuring the appropriate mechanisms for addressing youth related social problems.

It is hoped that this research would further help stakeholders in formulating policies and the various anti-crime agencies in understanding as well as curbing the problem. Moreover, the findings of the research, it is hoped, would in a small way contribute to knowledge on cyber crime and deviance in Ghana.

1.5 Definition of Key Concepts

Cyber crime- Walsh and Ellis (2007) define cyber crime simply as the use of computer technology to criminally victimize unwary individuals or groups. Gordon & Ford (2006) defines cyber crime as any crime that is facilitated or committed using a computer, network or hardware device. This therefore implies that the computer has made it possible for even the weak and fearful who would never dream of using a gun to rob, steal, assault and harass others, to do so

University of Ghana http://ugspace.ug.edu.gh

now from the comfort of their home and with relatively little or no risk of detection. As a result, the internet gives a global reach to users, allowing time and space to be crossed without one necessarily physically moving. This means that unlike traditional crimes, proximity between victim and perpetrator is not necessary for cyber crimes to be committed. For the purposes of this study, the researcher conceptualises cyber crime as all crimes committed using the computer, internet network, related software and includes fraud, cyber pornography, hacking, identity theft, theft and use of credit card.

Sakawa – All Cyber crimes in Ghana are locally referred to as *sakawa.* The word itself according to a key informant from the SFO, is believed to be of Hausa origin which literally translates to "burrowing into the center". The term has gained currency in the Ghanaian parlance and is frequently used by the press, Government officials and the population in general. As Nigeria has '419', Ghana can be said to have '*sakawa*'. The term is generally used to describe fraudulent activities, but specifically those cyber crime fraud activities primarily perpetuated by the youth with some purported 'pseudo occult' undertones. For the purposes of this research, it is conceptualised to encompass all fraud activities committed with the internet or cyber space as a conduit.

Youth: The proposed Ghana Youth Policy 2010 defines a youth as all young persons aged between fifteen and thirty five years of age. This research also adopts this definition because the research is based on Ghana, hence the relevance of this categorization.

University of Ghana http://ugspace.ug.edu.gh

1.6 Organization of the Study

The study is organized along the following lines:

Chapter 1 presents a general overview of study in terms of the statement of the problem, objectives and significance of the study.

Chapter 2 covers the research design employed in carrying out the study and those problems encountered.

Chapter 3 addresses the theoretical underpinnings of the study. This chapter also looks at relevant literature about cyber crime globally and in Africa as well as legal responses to it. Also literature on youth and crime are examined within and beyond the Ghanaian context.

Chapter 4 contains the research data analysis and findings of the interviews conducted.

Chapter 5 provides a summary and conclusion of the research. It also suggests appropriate recommendations to stakeholders regarding cyber crime and directions for future research.

University of Ghana http://ugspace.ug.edu.gh

CHAPTER TWO

RESEARCH DESIGN AND METHODOLOGY

2.1 Introduction

There are three commonly identified purposes for conducting social researches. One of them is to offer description. An example is a census which describes population demographics. The second purpose is to explain things, and researches conducted in this mode usually look at causal relationships and explain for example why crime rates are higher in one city than another. The third reason is exploratory (Babbie, 2008; Neuman, 2007). Exploratory researches are carried out to dispel some misconceptions on a phenomenon and help focus future research. This research is exploratory in that it seeks to examine the terrain of cyber crime by looking at the actors involved in it in Ghana, who, at the moment, are a hidden population. It is therefore important to choose a suitable research method to shed light on this social problem which is largely characterized by public speculation and media sensationalism. Against this background, this chapter introduces the research design and methodology employed in the study. It also discusses the paradigmatic orientation of the research, the study areas, the sampling techniques employed, data collection tools and the problems encountered during the course of conducting the research.

2.2 Paradigmatic Orientation of the Study

There are two broad methodological paradigms which dominate sociological research and these are the quantitative and qualitative paradigms. The quantitative research tradition can be traced back to the works of the French sociologist, Emile Durkheim such as *'Rules of Sociological*

University of Ghana http://ugspace.ug.edu.gh

Method (1895) and *'Suicide'* (1897). For Durkheim and Comte, the founder of sociology, Sociology should adopt the research model established by natural scientists. This means that, human behaviour could be scientifically measured and studied in much the same way as natural science phenomenon (cf. Mcintyre, 2005). Against this backdrop, quantitative methods tend to be concerned about measurement issues and statistics. Employing a deductive approach, quantitative methodologists start out with concepts and hypotheses then generate empirical measures that precisely and accurately capture them in a manner that they can be expressed in numbers (Neuman, 2007: 109).

On the other hand, the qualitative paradigms approach measures differently. Rather than using numeric measurements, qualitative data are usually presented in words and are largely descriptive. This sociological tradition can be traced to the works of German sociologist Max Weber. Like Durkheim, Weber also regarded sociology as a science. He however, maintained that unlike phenomena studied in the natural sciences, human beings have important qualities like thinking and feeling and as such, these need to be captured by accounting for the social meanings and reasons attached to behaviours (Mcintyre, 2005:127). This approach to attempting to comprehend social meanings of behaviour and actions is known as *Verstehen* which is the German word for understanding. For Weber, the concept of verstehen is that interpretative understanding of a social action and it involves the researcher looking not only at the individual actor and but also understanding the "larger culture in which actors exist and which constrains their thoughts and actions" (cf. Ritzer, 1996: 115). From this perspective, Hakim (1987: 26) argues that even though qualitative research is " about people as the central unit of account, it is

University of Ghana http://ugspace.ug.edu.gh

not about particular individuals per se; reports focus rather on various patterns, or clusters, of attitudes and related behaviour that emerge from the interviews". The qualitative approach best suits the aim of understanding the motives and subjective meanings of an elusive sample population like cyber fraudsters. Additionally, the qualitative approach is suitable for exploratory studies such as this one where the area of research may be so new, vague or centered around crimes (Cooper & Schindler, 2003). The perpetrators of cyber fraud or "*sakawa*" are a hidden population and not evenly distributed within the general population, therefore it would have been difficult to generate numeric statistical data to draw inferences from. As remarked by Glickman (2005: 464), "interviewing scammers resembles infiltrating the Mafia, not part of the training of social scientists". Any attempt to elicit the views of people whose activities are seen not only as immoral but criminal is an arduous task.

2.2 The Study Areas

As respondents were not confined to any particular area, the selected sample areas were Accra in Greater Accra Region and Agona Swedru in the Central Region. These areas were selected because they were frequently mentioned in media reports as having a high prevalence rate of cyber crime commission. Also, based on preliminary information gathered from the Police Services, these areas were likely to be where most perpetrators would be found. These two study areas further allowed researcher to explore the different social experiences of youths located within a highly urbanized area like Accra and semi urban area like Agona Swedru.

University of Ghana http://ugspace.ug.edu.gh

2.2.1 Accra

One area for the study was the Accra Metropole in the Greater Accra Region. The Metropolis hosts the capital city of Ghana, covers an area of 200 square kilometers and is made up of eleven sub-metros namely Ablekuma Central, Ablekuma North, Ablekuma South, Ashiedu Keteke, Ayawaso Central, Ayawaso East, Ayawaso West Wuogon, La, Okaikoi North, Okaikoi South and Osu Klottey.

Accra is Ghana's capital city and it has a population of over 2,905,726 million people (the 2000 National Population Census). Accra has been Ghana's capital since 1877 and as of today is one of the most populated and fastest growing Metropolis' in Africa with an annual growth rate of 3.36% (ghanadistrict.com, 2010).

The original occupants or inhabitants of Accra are the Gas. Some of the indigenous Ga communities in Accra include Osu, La, James Town, Chorkor, Teshie, New Town, etc. However, due to its cosmopolitan nature, people with all ethnic backgrounds have come to settle in Accra. Areas such as Cantonment, Labone, Legon, Lapaz, Dansoman, Madina, Adenta, Nima, etc. are occupied by people from all ethnic backgrounds. As the capital city, Accra is characterized by urban life and fast pace of living.

University of Ghana http://ugspace.ug.edu.gh

Accra's population is very youthful with 56 % of the population under the age of 24 years and has an unemployment rate of 12.2%. The age group of 15- 24 year olds make up 22.6 % of the population (Ghanadistricts.com). The unemployment rate vis a vis the percentage of youth population has serious social and economic implications for the nation.

2.2.2. Agona Swedru

The second study area is Agona Swedru which is the capital of the Agona District and located in the Central Region of Ghana. The Agona District can be found in the eastern portion of the Central Region. It has a total land area of 540-sq. km. and a population of 160,000. The municipality is divided into eleven zones. It lies within latitudes 5 30' and 5 50N and longitudes 0 3.5' and 0 55W. It is the most densely populated town within the Agona District and accounts for about 28.75% of the total population. The total population for Agona District stands at 158,678 (source: 2000 population census: Republic of Ghana). People are attracted to Agona Swedru mainly because of the existence of public and private sector business activities.

The Agona District has a large pool of unemployed youth and has been experiencing a decline in the main economic backbone of the district which is cocoa cultivation. This has contributed to a high incidence of poverty (ghanadistricts.com.2010). Agona Swedru was chosen as a study Area because it was frequently mentioned in the press as a centre for cyber crime activities and it gained a reputation among many Ghanaians and Internet chat room participants as a refuge for

University of Ghana http://ugspace.ug.edu.gh

immorality and promiscuity. This reputation dates back to 1998 when, out of the 77 women showcased in Ghanaian newspapers as portraying nude pictures of themselves, 54 came from the town (Tettey, 2006:17).

2.4 Sampling Techniques

As the population under investigation was a hidden one, there was no means of obtaining a sampling frame. The researcher therefore had to employ two non probability sampling techniques due to the peculiar nature of this research. These were purposive and snowball sampling for selection of respondents. Snowball sampling technique meant that the researcher relied largely on the social network approaching as described by Kumekpor (2002) in terms of identifying "an individual member of a particular social network and using the snowball effect to trace the other members' friends, families, media personnel and colleagues in order to identify possible respondents.

The use of purposive sampling technique was also employed. Taking into cognizance the nature of the research, it was important to seek out the required knowledge necessary for the data collection process. Additionally, the unwillingness of many potential youth respondents to participate and the limited time within which to find suitable replacements found purposive sampling to be very appropriate. According to Kumekpor (2002) the main objective of samplings technique is to select a portion of a universe that the results may, or could be, extended to the whole population. However it is not always the case in research that certain characteristics or

University of Ghana http://ugspace.ug.edu.gh

phenomena are distributed randomly or uniformly in a universe. In such cases, a representative sample may not at all include a unit typical of the characteristics in question, or it may include so few units that the analysis may not be statistically significant. In such cases as noted by Kumekpor (2002: 137-138), it is more appropriate to identify units of the universe, which satisfy the characteristics of the phenomenon under investigation. Given this, the researcher purposively selected respondents that had the knowledge specifically suited to meeting research objectives.

The total population size for study was twelve. The initial targeted perpetrator population was twenty youths but this number was reduced to ten that had become reliable and consistent over the period of data collection. Five of the respondents were selected from Accra and five from Agona Swedru. As the study was dealing with two issues- a hidden population and a crime, the small sample size chosen reflected this. It must, however, be emphasized that the small sample size did not presume to be truly representative. But then as Becker (1998) stressed that samples are not always drawn only to estimate the distribution of certain traits in the population but also to gain an in- depth understanding of a social phenomenon or development which was also the concern of this study. Given the fact that the youth perpetrators operated undercover and therefore were not easily known and the fact that the study is exploratory, the ten youth respondents consisted of a good sample size to work with.

Additionally, two informants were sought to gain the perspectives of law enforcement agencies to *sakawa*. One key informant was purposively selected from the Documentation and Visa unit of the CID, which is the unit primarily engaged in dealing with cyber related offences. Another

University of Ghana http://ugspace.ug.edu.gh
key informant was selected from the Serious Fraud Office (SFO). The selected two key informants were selected primarily based on their background working knowledge of the phenomenon.

The ten youth respondents were identified based on the following sampling criteria:

(1) Respondents were aged between 17 and 35 years

(2) They resided within selected sampling areas that is Accra and Agona Swedru

(3) They were known or identified by a third party as engaging in one form or another of cyber crime.

(4) They willingly confirmed that they did engage in *sakawa*

The rationale for these criteria was to include those who had the best knowledge on cyber criminal activities, exclude those who resided outside of sampling areas and obtain a sample of youth who "best fit" research objectives.

The sampling criteria for selecting the two key security agent informants was solely that they worked in units or departments that handled cyber crime issues and arrests. The relevant departments therefore were the Documentation and Visa Fraud Unit of the Police Service. The key informant was an officer of that unit. While at the Serious Fraud Office, the key informant was the Head of Special Services. The purpose of seeking the views of these key informants was to elicit information on the legal responses of these organizations on cyber-fraud.

The study allowed for perspectives from both cyber crime perpetrators and those assigned with tackling the problem. The intent of this approach was to avoid presenting a one-sided argument.

University of Ghana http://ugspace.ug.edu.gh

2.5 Data Collection Instruments

Data for the study was collected using a variety of ethnographic methods. These were unobtrusive observation, in-depth interviews, and informal discussions. As a data collection tool, the observation method allowed the researcher access into the daily lives of subjects.

The researcher also employed the in-depth interview method with the use of semi-structured and open-ended questions. The choice of this data collection tool was in order to guide interview towards fulfilling research objectives without restricting respondents to yes/no responses. This was motivated by the need to engage with youth involved in cyber crime and understand their life experiences, meanings, stimulus and driving factors. Also in-depth interview as a data collection tool enabled the researcher to gain detailed descriptions of lived experiences of persons involved and better situate the research outcomes within the context of relevant theories. As Cooper & Schindler (2003) assert, in-depth interviews encourage respondents to share as much information as possible in an unconstrained environment. The researcher used a maximum number of prompts and guiding questions. The questions for youth respondents were themed around background of respondents, types of cyber crime and descriptions, crime motivation, inter alia. The questions for the security agency informants were themed around the legal responses to crime, their awareness of cyber crime etc. This allowed respondents to open up and fully discuss the topic. This further enabled a first person perspective from respondents' worldview.

University of Ghana http://ugspace.ug.edu.gh

2.6 Problems Encountered in the Field

A major limitation of the study was the fact that the success of the research depended a lot on the willingness of located respondents to cooperate with the researcher and provide detailed responses. Certain difficulties were faced during the course of carrying out field work. These ranged from most of the respondents refusing to be audio taped, in fact, one respondent felt strongly that he could be identified by his voice whilst another felt that he could be easily implicated to confessing to crime commission. This meant that the researcher had to take lots of research notes and this hampered the smooth flow of the interview process. Another difficulty was that some identified respondents refused to cooperate to be interviewed once they realized that the researcher was female. This, they felt would affect their 'luck'. This was particularly obvious in Agona Swedru that is a semi urban area and strangers are initially viewed with suspicion before trust is gained.

One other difficulty was that for every arrest of a friend or colleague of cyber crime, the smaller the respondent sizes got, so from starting out with a size of twenty to losing ten of those respondents after extensive research work had begun and researcher had to seek out new respondents. Inarguably, a lack of cooperation would have significantly and adversely affected the study and compromised the results of the research. Finding willing respondents was challenging as well as difficult and the researcher was well aware of this problem and devised ways to best overcome them without compromising research objectives and findings. For starters, pseudonyms were given to respondents to hide their real identities. Also, interviews were usually done away from the location where respondents resided so to avoid suspicion from

University of Ghana http://ugspace.ug.edu.gh

others. In addition, the privacy of respondents was constantly emphasized and the purely academic basis of research was guaranteed as a means of encouraging participation in the research.

Another problem was the lack of a reliable cybercrime statistics from the security agencies which would have provided an appropriate support to media reports of a growing trend. In their defence, however, the security agencies explained that they were not yet separating cyber crime activities from other traditional fraudulent activities.

University of Ghana http://ugspace.ug.edu.gh

CHAPTER THREE

THEORETICAL FRAMEWORK AND LITERATURE REVIEW

3.1 Introduction

The chapter reviews relevant theories and literature that have bearing on the research topic. The review evaluates some classical theories that offer sociological explanations for crime commission as well as contemporary crime theories like the Space Transition Theory primarily tailored to explain deviant behaviour in cyber space. There is also an appraisal of some criticisms levelled against the classical theorists.

Also, the literature review covers briefly the early beginnings of the internet. The internet or cyber space has often been referred to collectively as a social technology (Lamb & Johnson, 2006) due to how it allows people of all creeds, race, age to communicate with each other. As a social technology, it represents those computer mediated communication (CMC) devices that enable people to connect for either personal or professional reasons. Cyber crime is a phenomenon, which requires a computer in order to occur. It is a global occurrence particularly in these days of the "Global Village" concept. It is therefore important that the study recognizes what constitutes cyber crime and the variant forms of cyber crime as other studies have recognized. As this research focuses on youth participation in cyber crime, the review also considers the predisposing factors that engender youth involvement in cyber crime. The peculiar nature of *sakawa* believed to combine occults with Information, Communication and Technology

University of Ghana http://ugspace.ug.edu.gh

(ICT) as perpetrated in Ghana would also be briefly examined. Finally the literature review examines the response of law enforcement agencies in tackling phenomenon across jurisdictions.

The review is important because it provides the framework and background for this research investigation into what constitutes cyber crime or as is locally known in Ghana '*sakawa*', the reasons why those involved choose to do so, how they go about acquiring cyber delinquent behaviour, and finally the challenges faced by law enforcement agencies in tackling the problem.

3.2 Theoretical Framework

Sociologists have long recognized that there exists no society without crimes. Durkheim is always remembered for the view that a crime is normal of society just like birth and death (cf. Adler et al.2001:77). As a discipline, sociology has interest in unearthing causal relationships between actors and phenomenon. This has seen various social scientists attempting to explain what causes some people to commit crimes while others do not.

It is difficult for a single explanation to account for all crimes. Various researchers have propounded theories based on biological, psychological, physiological and sociological explanations for crime commission. However for the purposes of this study- cyber crime and youth involvement, there will be a synthesis of four theories to help explain the causes of cyber crime. These are: Strain Theory, Differential Association Theory, Neutralization Theory and the Space Transition Theory.

University of Ghana http://ugspace.ug.edu.gh

3.2.1 Classical Theories of Crime

Classical theories of crime emphasize the social and environmental forces that influence people to commit criminal acts. Social process theories seek to describe the process of criminal and delinquent socialisation, that is, how anti-social attitudes and behaviours are learned (Walsh and Ellis, 2007).

3.2.2 Strain Theory

One of the most famous explanations for deviant behaviour is Strain theory. The notion of Strain theory was propounded by Robert Merton and rooted in Emile Durkheims' concept of *anomie.* In his two famous studies, *The Division of Labour (1893)* and Suicide *(1897),* Durkheim used anomie to represent the absence of rules, norms, values and identities within a society which led to individuals feeling confused, uncertain and isolated. These feelings of disruption could occur when the traditional social framework of family life and work broke down along with the general absence of newer, stable norms and structures of social regulation which were conditions present during periods of rapid modernization as was witnessed by Durkheim during the industrial revolution.

Durkheim further posited that *anomie* could also be the result of social instability when those regulations that restrained individuals' desires and expectations within achievable limits broke down, and led to individuals' pursuit of unattainable goals which in turn led to feelings of disillusionment with themselves and society and further let to a high incidence of suicides (cf. Merton, 1949).

University of Ghana http://ugspace.ug.edu.gh

Robert Merton used Durkheim's *anomie* theory as a foundation to build his Strain theory in 1938. This theory demonstrates how the relationship between culture, social institutions and Anomie affects individual behaviours, causing strain and can eventually lead to deviant conduct. Merton describes culture as that "organized set of normative values governing behaviour which is common to members of a designated society or group". He thus defined social structure as that organized set of social relationships in which members of the society or group are variously integrated.

In describing Anomie, Merton defined it as occurring "when there is an acute disjunction between the cultural norms and goals and the socially structured capacities of members of the group to act in accord with them" (Merton, 1949). Merton was writing with emphasis on the American culture which places a great deal of emphasis on material success and that these materialistic values are shared by members of the society. But access to these material goals is not readily available to all the members of society. Merton suggested that socially structured class differences limited the accessibility of legitimate opportunities to achieving these goals. Individuals in lower class positions were deemed more likely to experience strain which manifests as frustration and further motivates individuals to seek alternative means to achieve these goals including illegitimate means (Merton, 1949). For those who had aspirations but not the means to achieve them, they experienced feelings of psychological strain.

University of Ghana http://ugspace.ug.edu.gh

Table 2: Representation of Merton's Strain Theory Table

Modes of Adaptation	Culture Goals	Institutionalised Means
I. Conformity	+	+
II. Innovation	+	-
III. Ritualism	-	+
IV. Retreatism	-	-
V. Rebellion	+	+
	-	-

Source: Merton, R. K. Social theory and Social Structure (1949: 133)

Key:

(+) Signifies "Acceptance"

(-) Signifies "Rejection"

[+ -] Signifies " rejection of prevailing values and substitution of new values"

The table above is explained further. Robert Merton identified five potential adaptations to strain: *Conformity, Innovation, Ritualism, Retreatism and Rebellion.*

University of Ghana http://ugspace.ug.edu.gh

The conformist "is the most common and widely diffused" of all the adaptive mechanisms (Merton, 1949: 134). Individuals within society that had the legitimate means to meet their socially approved goals were said to be *Conformist*. These individuals conformed to society's desires for meeting their aspirations. Some examples of conformists are medical doctors, academic professors.

The Innovator may accept the socially approved means to success but has limited means of attaining it. He may therefore choose to innovate his own way of attaining society's cultural goals whilst using illegitimate means. Merton meant those that engaged in criminal activity, cheating or other disapproved means of achieving success (Merton 1949: 134). Some examples are drug dealers, armed robbers, prostitutes as well as those engaged in cyber crime. This particular classification of people is significant to the objectives of study. Cyber criminal activities could result from young people feeling that attaining society's goals while using legitimate means may be blocked for them. This results in them innovating by using illegitimate means to acquire what they consider society's symbols of success, for example wealth, cars, houses etc.

The Ritualist is typified as those who in failing to achieve goals, internally give up or abandon any efforts to try and achieve them. They think that if they do not aim high, they will not be disappointed (Merton, 1949:142). Externally though, the individual conforms in a strict manner to the use of legitimate means that are socially proscribed as necessary for goal attainment. Thus, the Ritualist responds to failure and frustrations by either reducing or ignoring the importance of

University of Ghana http://ugspace.ug.edu.gh
said goals. Examples are the overzealous bureaucrat or the frustrated employee who is aware that they are not going anywhere. This category of people are not likely to engage in *Sakawa* and are thus excluded in this study.

The Retreatists are those individuals who find when they meet obstacles in goal attainment, drop out of the struggle for success. They choose to reject conventional goals and means by escaping or withdrawing from mainstream society through drinking excessively or engaging habitually in hard narcotics. Merton indicated that the retreatist were "in the society, but not of it". Some examples are the alcoholics or drug addicts. Merton (1938) believed this adaptation mechanism as the least common. This group is not significant to study.

The Rebels are those individuals who not only reject and withdraw from legitimate goals and societal means but also attempt to replace the conventional ones with theirs. Various radicals and revolutionaries are typical examples of this form of deviant adaptation. This class of people is not important to study.

For Merton, the cause of deviant behaviour lay not in the individual but in the disjunctions between the emphasis placed on cultural goals and the lack of opportunities available to all people to use the legitimate means to reach their goals. He further contended that people may shift from one adaptive mechanism to another as they engage in various spheres of social

University of Ghana http://ugspace.ug.edu.gh
activities. Additionally, these categories of adaptation were in reference to role behaviour in specific types of situation and not to personality (Merton 1949: 133).

In today's Ghana, there is no limit set on what people can acquire in terms of material goods. In Chris Abotchie's contribution to Sociology of Urban Communities, he argues that to the *Innovators,* while the urban culture emphasizes material success, the reality is that the social structure within society places limitations on the approved means (2008:139). He further stresses that due to the intense competition that exist within urban communities, Merton's innovation becomes the most common form of adaptation. Most of the crimes associated with Innovators in Ghana are economic in nature such as stealing and robbery etc. This notion is corroborated by Ken Attafuah's (2008) work on combating armed robbers in Ghana. The robbers he studied admitted that they resorted to armed robbery because of what they felt were blocked means to acquiring society's goals.

In spite of the fact that Merton's Strain Theory has been hailed as one of the most credible attempts at explaining crime rates in societies, there are those who have levelled some criticisms against the Strain Theory. His theory has been accused of failing to explain why it is not everyone that experiences the effects of anomie that become deviants and criminals (Haralambos and Holborn, 2004:334). Merton's work is also criticized for assuming that there is a value consensus among everyone in the American society which implies that everyone seeks the American Dream and by extension individuals tend to only deviate due to structural Strain.

University of Ghana http://ugspace.ug.edu.gh
Merton's theory cannot possibly account for all crimes, there are other sociologists who have also put forth theories to account for crime and delinquency within society.

3.2.3 Differential Association Theory

Another famous theory for explaining criminal behaviour is Edwin Sutherland's Differential Association which was developed in 1939. A renowned criminologist, Sutherland sought to arrive at a theory that would not only explain individual criminality but also identify those conditions that must be present for crimes to occur. Sutherland outlined nine propositions that engender individuals to acquiring necessary attitudes and techniques that are favorable to delinquent behaviour (Sutherland and Cressey, 1978:80- 83).

These nine propositions are as follows:

1. Criminal behaviour is learned. This means that criminal behaviour is not biologically inherited or in born in individuals but rather learned from others.

2. Criminal behaviour is learned in interaction with other persons in a process of communication. Here, a person does not become a criminal just by living within a criminal environment but learns crime by participating with others in verbal and non verbal communication.

3. The principal part of learning criminal behaviour occurs within intimate personal groups. This means that individuals are highly influenced most by families and friends in learning deviant behaviour.

4. When criminal behaviour is learned, the learning includes

University of Ghana http://ugspace.ug.edu.gh

(a) The techniques of committing crime

(b) The specific direction of motives, drives, rationalizations and attitudes.

As well as learning criminal activity, young delinquents learn how to rationalize and defend their actions particularly as they sharpen their skills and gain experiences.

5. The specific direction of motives and drives is learned from definitions of the legal code as favourable or unfavourable. It is not everyone in society that agrees that laws are to be obeyed; there are those who see them as unimportant.

6. A person becomes delinquent because of an excess of definitions favourable to violations of law over definitions that are unfavourable to violations of law. This is the key principle of Differential Association. Learning criminal behaviour is not simply a matter of keeping bad company but rather it involves a process of identifying and copying other individuals that we respect and value their opinions. When a person becomes a criminal, they do so because of contact with criminal patterns and also because they are isolated from anti criminal patterns.

7. Differential Association may vary in frequency, duration, priority and intensity. This means that the extent to which associations and definitions will result in criminality is related to the frequency of contacts, deviations and their meaning to the individual.

8. The process of learning criminal behaviour by association with criminal and anti criminal patterns involves all the mechanisms that are involved in any other learning. To learn criminal behaviour patterns is similar to learning conventional behaviour patterns and is not simply a matter of observation and imitation.

University of Ghana http://ugspace.ug.edu.gh

9. While criminal behaviour is an expression of general needs and values, it is not explained by them since non criminal behaviour is an expression of same needs and values. Those that engage in criminal behaviour like theft, do so to get what they desire while others engage in non criminal behaviour like work to get money to also buy what they desire.

Sutherland and Cressey (1978) add that high crime rate is due to differential social organization. In areas where delinquency rates are high, interactions with others may likely lead a good boy to learn and acquire anti social skills from delinquents within the neighbourhood

Abotchie (2008: 143) supports this by adding that daily interactions between urban residents particularly those who reside within slum neighbourhoods in irking out their daily needs, "gives rise to crimes". He continues that as a result of the problems of over urbanization implies that most people are unemployed and are therefore prone to criminal activities to be able to survive.

Differential Association has been criticized by some scholars who say it is defective as it fails to consider the issue of persons committing crimes purely out of their free will. Edwin Sutherland was also criticized for failing to account for people who commit crimes due to such personality traits like aggressiveness.

Despite these criticisms, Differential Association Theory has been vital in explaining how delinquents acquire their criminal behaviours. It is still a highly valued sociological theory still relevant now.

University of Ghana http://ugspace.ug.edu.gh

3.2.4 Neutralization Theory

In light of the topic of cyber crime, another relevant theory to be used is the Techniques of Neutralization theory. In 1957, Gresham Sykes and David Matza propounded their theory on the use of certain cognitive techniques to counter those feelings of guilt associated with delinquent behaviour. Prior to the development of this theory, it was a commonly held conviction that juveniles adhered to a code of values and beliefs that differed from those shared by the general population. Sykes and Matza disagreed with this view, stressing that juveniles usually adhered to the same beliefs and norms as the larger population.

However, it was only when a juvenile engaged in certain delinquent acts that the individual moves from a state of lawfulness to a state of lawlessness (Sykes & Matza, 1957:666). In reaching the above mentioned end, Sykes and Matza identified five techniques used to justify delinquent behaviour. They are as follows:

1. ***The denial of responsibility***: Individuals who applied this technique of neutralization refused to accept responsibility for their actions. This denial was believed to go beyond an initial belief that the individual's behaviour was as a result of accident, and went as far as the belief that factors beyond their control were responsible for their behaviour. These factors could range from blaming behaviour on family structure or slum neighbourhood in which one resides or bad companions. The delinquent effectively sees himself as "helplessly propelled" into deviant situations (Sykes & Matza, 1957:667). It could be the way people usually blame the devil for their own actions.

2. ***The denial of injury:*** this second technique of neutralization stems from the individual believing that there was no injury or harm caused to the person who was affected by the

University of Ghana http://ugspace.ug.edu.gh

delinquent behaviour. Moreover, if there was any harm, then the harm was minimized by the fact that the victim could afford the damage and was therefore not that harmful in the true sense.

3. ***The Denial of the Victim***: the third technique of neutralization builds upon the second technique aforementioned. Individuals who applied this technique, accepted that there was a victim to a crime, but concede that the harm to the victim was justified. As far as the criminals are concerned, the harm is really not a harm but retaliation or revenge. Sykes & Matza contend that " by a subtle alchemy, the delinquent moves himself into the position of an avenger and the victim is transformed into a wrong doer" (1957: 668).

4. ***The condemnation of the condemners technique*** involves the delinquent justifying their behaviour on the basis that those who condemn their criminal acts are " hypocrites, deviants in disguise or compelled by personal spite" (Sykes & Matza, 1957: 668). The delinquents also feel that if given the chance, their condemners would have engaged in the same act.. Usually, the condemners are usually those regarded as assigned the role of enforcing the norms of society like the police, teachers and parents. They may refer to the police as corrupt, stupid and brutal. By attacking higher authorities, the delinquent inadvertently represses the wrongfulness of his own behaviour.

5. ***The Appeal to higher loyalties*** technique was applied when the delinquent recognized that perhaps an act was inappropriate but justified the behaviour on the grounds that their immediate social group needed their behaviour at the time. This technique increases the offender's moral integrity by claiming altruistic motives for criminal act. For example, the offender feels he committed crime to help out friend or family.

University of Ghana http://ugspace.ug.edu.gh

Sykes & Matza (1957: 669) argued that these techniques of neutralization were not only responsible in reducing the effectiveness of social control mechanisms but also lay behind a large share of delinquent behaviour. It was pertinent to apply this theory to this research to evaluate whether sakawa practitioners experienced any feelings of guilt and how they countered such feelings as espoused by Sykes & Matza.

3.2.5 Space Transition Theory

Considering the relative novelty of the internet and cybercrime, it was practical to include a theory that is specific to deviant behaviour in cyber space. In 2007, Karuppannan Jaishankar (International Journal of Cyber Criminology, 2007:7) propounded the Space Transition Theory to offer an explanation as to the changes that occur to the conforming and non conforming behaviour of individuals when they move from the physical space to cyber space and vice versa. The theory argues that individuals behave differently when they move between these spaces. He postulates that:

1. Those 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 cyber space provide the offenders the choice to commit cyber crime.

3. Criminal behaviour of offenders in cyberspace is likely to be imported to physical space and vice versa

University of Ghana http://ugspace.ug.edu.gh

4. Intermittent ventures of offenders into cyberspace and the dynamic spatio- temporal nature of cyberspace provide the chance to escape and get away with crimes.

5. (a) Strangers are likely to unite together in cyberspace to commit crime in the physical space.

(b) Associates of physical space are likely to unite to commit crimes in cyberspace.

6. Persons from closed society are more likely to commit crimes in cyberspace than persons from open society.

7. The conflict between norms and values of physical space and norms and values of cyber space may lead to cybercrimes.

Jaishanker cautions that there is a need for testing of theory to see if it explains various cyber criminal activity.

3. 2. 6 Theoretical Synthesis

The concept of theoretical Synthesis is a model adapted from Adediran's (2008) work on the causes of '419' activities in Nigeria. He used a hybrid of the Multi linear Theory and the application of Robert Merton's latent and manifest function of the internet.

This theoretical synthesis requires the integration of the four different criminology theories earlier explained. Cyber crime is a relatively new phenomenon that requires some explanation. This necessitates the use of different theories to complement each other's shortcomings. Hence, the study adopts a fusion of the theories above. The Strain theory gives an exposition as to how certain individuals react to frustrations they feel in trying to reach their socially approved goals.

University of Ghana http://ugspace.ug.edu.gh

Differential Association theory on the other hand offers an account as to how individuals imbibe their delinquent skills and while the Neutralization theory sheds light on how cyber crime perpetrators counter any feelings of guilt associated with crime commission. Considering the unique nature of social interactions in cyber space, Space Transition theory also provides an explanation of cyber delinquent behaviour in cyber space.

These theories would be applied to the study of cyber crime in Ghana but before we do this, a brief history of the internet is relevant.

3.3. A Brief History of the Internet

The Internet revolutionized the communications world like nothing before. The invention of the telegraph, telephone, radio, and computer set the stage for this unprecedented integration of capabilities. The Internet is now seen as a mechanism for information dissemination, a medium for collaboration and interaction between individuals and their computers without regard for geographic location.

The first recorded notes premiering the idea of the global information system now recognized as the Internet was written in 1962 by J.C.R. Licklider of the Massachusetts Institute of Technology (Leiner et al., 2003). His idea, termed the "InterGalactic Computer Network", entailed an internationally connected set of computers that encouraged ease of access to information. While working at the Defense Advanced Research Projects Agency (DARPA), Licklider's co-worker Lawrence Roberts (1967) published his idea for "ARPANET" which stands for Advanced

University of Ghana http://ugspace.ug.edu.gh

Research Projects Agency Net. ARPANET quickly evolved into what is now known as the Internet. With this amplified popularity for technology, the Internet experienced the perfect environment to thrive, and soon began to do so .This in turn heightened interest among private Internet users (Leiner et al, 2003, Anderson, 2005). With this amplified popularity for technology, the Internet experienced the perfect climate to thrive, and soon began to do so.

William Gibson (1984) predicted in his novel "Neuromancer" that society's increasing fascination and dependence on computer technology would create a completely electronic world he termed "cyberspace." Cyberspace would be composed of millions of different outlets of information that were easily accessible at the click of a button. Gibson also accurately predicted that his new concept would contain dangerous channels leading to sources of vulgarity, criminal activity, and a dangerous hidden world of exploitation. In reality, Gibson's predictions have come true as the range of crimes committed online, otherwise known as cyber crimes, is quite Substantial and covers amongst others from fraud, theft to sexual solicitations.

3.4 Defining Cyber Crime

It might not be easy to find the word 'cyber-crime' in contemporary lexicon, but it is a very popular term describing the criminal activities related to cyberspace or the cyber-world. While scholarly consensus on a single definition of the terminology is yet to be achieved, it would appear that writers and law drafters are more comfortable with describing various elements constituting cyber-crime than in defining it.

University of Ghana http://ugspace.ug.edu.gh

According to the Council of Europe (COE) Cyber Crime Treaty (2001), cyber crime involves 'action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data', here, the definition of cyber crime refers to offences ranging from criminal activity against data to content and copyright infringement.

A thorough reading of the definitions put forward validates the argument that most authors only resort to simply describing the role of computers and the internet in the commission of crime (Collier, 2004: 322-328; Bazelon et al, 2006: 261-264). This explains why Olowu, 2009:3 identifies Casey (2004: 8) as proffering a dubious definition of cyber-crime by referring to it as 'any crime that involves computers and networks, including crimes that do not rely heavily on computers'. Olowu (2009) however, fails to provide a definition of his own. The other spectrum of the coin sees others who seek to classify cyber-crime into computer-related and content-based species (Walden, 2003, p.295; Lewis, 2004, pp.1355-1356) or between 'true cyber-crime'– dishonest or malicious acts that would not exist outside online environment and 'e-enabled crime' – criminal acts already known to the world but now promoted through the internet (Gordon & Ford, 2006, Burden et al. 2003: 222). Yet, there have been debates about whether unlawful activities involving computers and the internet should be classified as crimes or civil wrongs (Barton and Nissanka, 2003, p.401).

Gordon & Ford (2006:13) opine that although the term "cyber crime" is in common usage, there still exists a problem of the term having a precise definition. They emphasize that defining cyber

University of Ghana http://ugspace.ug.edu.gh

crime and differentiating types of cyber crime is very important because definitions not only provide researchers with a universal language which is vital for meaningful discussions to occur but additionally aid to determine the scope of the problem under review and also allow for clear communication,(2006:17). This especially true for Law enforcement agencies since cyber crimes usually occur across several jurisdictions and across national borders that it is very important that a universal understanding of a definition of cyber crime should aid in combating the problem. Gordon and Ford(2006) proffer the following definition of cyber crime: "any crime that is facilitated or committed using a computer, network, or hardware device".

Correspondingly, Snail (2009:2) explains that cyber crime also known as computer crime can be defined as any criminal activity that involves a computer and can be divided into two categories- crimes that can only be committed using a computer which were hitherto not possible before the dawn of the computer such as hacking, cracking, sniffing and the production and dissemination of viruses and crimes which have been in existence for centuries but are now committed within the cyber environment such as internet fraud, possession and distribution of child pornography to name a few. Van der Merwe (2008:61) gives cyber crime a contemporary outlook. According to him, computer crimes represent a novel type of criminal activity which started appearing during the early nineties as the use of the internet became more common place worldwide.

From all of the definitions given, one can see that cyber crimes are simply crimes committed with the aid of a computer that is connected to a network. This facilitates the perpetrator to go

University of Ghana http://ugspace.ug.edu.gh

beyond his immediate location and reach what the researcher calls a ' world wide audience' anonymously.

3.5. FACETS OF CYBERCRIME

Similar to traditional crimes, cyber crime has many different facets and occurs in a wide variety of scenarios and environments.

Wall (2001:3-7) chooses to subdivide cybercrime using four established legal categories:

1. Cyber-*trespass* – crossing boundaries into other people's property and/or causing damage, e.g. hacking, defacement, viruses.
2. Cyber-*deceptions* and *thefts* – stealing (money, property), e.g. credit card fraud, intellectual property violations (a.k.a. 'piracy').
3. Cyber-*pornography* – activities that breach laws on obscenity and decency.
4. Cyber-*violence* – doing psychological harm to, or inciting physical harm against Other people thereby breaching laws pertaining to the protection of the person, e.g. hate speech, stalking.

This classification helps in relating cybercrime to existing conceptions of proscribed and harmful acts but it does little in the way of isolating what might be qualitatively different or new about such offences and their commission when considered from a perspective that looks beyond a limited legalistic framework.

University of Ghana http://ugspace.ug.edu.gh

Some reports lists types of cybercrimes based on most top complaints made by victims (Hansen, 2003, IC3 Report 2009). These are Internet Auction Fraud, Credit Card Fraud, Travel and Vacation Scams, Bogus Business Opportunities, Identity Theft, Hacking, Phishing and Pharming, Nigerian letter scam or 419 scams. Other studies choose to add Cyber Terrorism (Fabry 2001: 186), cyber stalking, Child predation, (Gordon & Ford 2006:18). Some of these cyber crimes are expatiated in detail below.

INTERNET AUCTION FRAUD

According to the IC3 Annual Report 2009, Auction Fraud involves the misrepresentation of a product advertised for sale through an internet auction site such as E-bay or Craigslist. Hansen (2003:20) contends that this is where the buyer having already made payment, receives an item that is less valuable than promised or worse, receives nothing at all.

CREDIT CARD FRAUD

This involves the unauthorized use of a credit/debit card, or card number, to fraudulently obtain money or property. Credit/debit card numbers can be stolen from unsecured websites, or can be obtained in an identity theft scheme. In Ghana, Tettey (2008) discusses internet fraud encompassing the sale of credit card information illegally collected from people around the world.

University of Ghana http://ugspace.ug.edu.gh

INTERNET PORNOGRAPHY AND CYBER SEDUCTION

Many people use the internet in search of social relationships. This is not bad thing in itself but there are those who have a predilection for pornography particularly, child pornography. Internet users today, enjoy entering chat rooms and meeting people from other walks of life and locations like previous generations enjoyed doing with pen pals (Slater & Kwami, 2007). The problem herein is that there are those who enjoy manipulating lonely insecure adults and children into revealing personal details of their lives. As well as luring them to upload compromising pictures of themselves which are posted online for everyone to have access. The anonymity of the internet avails itself well to pedophiles and scam artists to exploit others in cyber space (Walsh & Ellis, 2007:387).

PHISHING AND PHARMING

Olowu (2009:4) notes that due to the explosive growth of online fraud, 'phishing', and to a lesser extent 'pharming' have become part of nearly every Internet user's vocabulary in most recent time. Phishing and pharming are two popular forms of fraud that aim to dupe victims into believing they are at a trusted Web site such as their banks, when in fact they have been enticed to a bogus Web site that intends to steal their identity and drain their financial resources (Brenner, 2004, p.6; Chawki, and Abdel-Wahab, 2006).

University of Ghana http://ugspace.ug.edu.gh

CYBER-TERRORISM

Fabry (2001) espouses that acts of cyber-terrorism can range from the use of personal information for extortion, to hacking into a network, to physical and/or electronic destruction of a networked information system. Perhaps the simplest description is that ideological concerns rather than economic or political considerations motivate these attacks. Terrorism can be an extremely effective tool for shaping that response. The growing dependence of modern societies on computer-controlled information infrastructures has opened up new areas for unconventional warfare. Hansen (2003:21) cites the example of cyber-warfare that broke out between American and Middle Eastern hackers after September 11th 2001 terrorist attacks that occurred in the States of America.

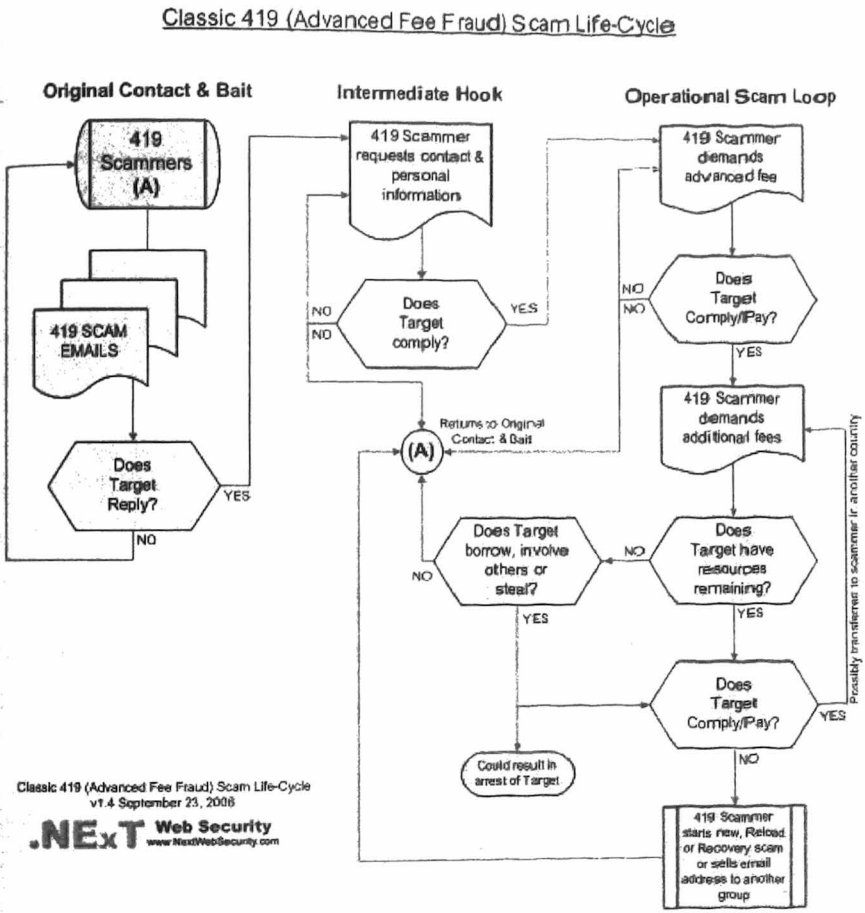
ADVANCED FEE FRAUD (AFF) or '419'

There have been quite a significant number of studies done on the Advanced Fee Fraud (AFF) or 419 as it is popularly referred to (Chawki 2009; Adogame 2009; Holt & Graves 2007; Smith2001). The 419 scam gained its name after the penal code outlawing the crime in Nigeria which code was enacted in the early 1990s (Tettey, 2006).

Tettey further adds that 419 scams predate email use but technology has expanded its 'geographic scope'. Adogame (2009) underscores that the internet and email technology have

University of Ghana http://ugspace.ug.edu.gh

changed the "face, pace and fate of AFF". The flow chart below represents the life cycle of a 419 scam as represented by NExT web security.



(Fig i)

source: www.NExTWebSecurity.com

University of Ghana http://ugspace.ug.edu.gh

This flow chart reflects the sophisticated multi stage levels that are employed to ensure perpetrators are successful in scams from the moment the bait is accepted by "target". The scam starts out as "bait" which is usually done through sending out "internet solicitations"- (see Tettey, 2006: 249). These solicitations could range from mutually beneficial schemes, bogus lottery scams, transfer of illegally acquired assets (Tettey, 2006) to charitable request. Glickman (2005) estimates that a single person can send out from one thousand to over a hundred thousand scam emails in a day. He explains that "if twenty thousand messages are sent out daily and one percent responds, that is two hundred people to work with". Brady (2003:13) asserts that scammers need just a one percent success rate to make proceeds.

From the flow chart, there are actions for whether the target responds or not. If the target does not respond, the 419 scammers start the process again with a new scheme. If the target responds then an "intermediate hook" would have occurred whereby the scammer would request as much personal information from target. As with the baiting stage, there is action process for compliance or non compliance. If there is a non compliance to the request, then the baiting process restarts. But if target complies, then the scam operation moves on to the "operational scam loop" where there is a demand for the advanced fee payment.

The amount requested will depend on the nature and sophistication of scam. Similar to the previous stages, there are actions as to if target would yield or not to their demand. Once target consents to making payments, subsequent demands are made and there is even the possibility of transferring target to another scammer somewhere else to continue scam or begin a totally new

University of Ghana http://ugspace.ug.edu.gh

one. Some of these targets are hooked on for lengthy periods and spend thousands of dollars unable to concede to the fact that they have been scammed. Glickman (2005:468) cites a US commerce official as saying that "once people get hooked, my experience is they become more and more resistant to accepting that it's a scam, because they become vested in the deal". As a result, they choose to live in denial not wanting to believe that the whole deal is a scam.

3.6 Predisposing Factors

One of the core objectives of this study is to interrogate the factors that propel the youth to indulge in "*sakawa*". It is extremely vital therefore to look at the factors that predispose the youth to committing cyber crimes as this would inform the strategies to combat the menace. These factors would be identified as social, political, economic.

3.6.1 Social Factors

3.6.1 (a) Youth and Propensity to Crime Commission

Many studies indicate that crimes are mostly committed by the youths (Baron, 2006; Agnew, 1985; Cloward & Ohlin, 1960). Kimmel & Aronson (2009) are of the view that "When we say crime, we might also say young". Irving Spergel cited in Walsh et al (2007), writing on reasons why youths commit crime and join gangs is of the view that they do this for reasons such as status, security, money, power, experiment and new experience. Entorf & Spengler (1998) postulate that when considering youth especially young males, firstly, one may be inclined to

University of Ghana http://ugspace.ug.edu.gh

think that in general they do not accept social norms as older people do. This could be attributed to "age-specific rebellion or lack of hindsight" (Eide, 1994). Also young people could be said to be in a "better" social and physical position to commit crimes as they are inclined to take risks and are more "adrenaline driven".

Further, the threat of loss in reputation and social status is higher for adults with well-established social networks than for young people (Eide, 1994). He further adds that when compared to other demographic groups of the population, young people usually are physically superior to other groups of the population which in effect gives them the comparative advantage of perpetrating crimes that require strength or speed. The youth also tend to spend much more time in their circle of friends and crowds which may create social interactions when initially law-abiding members of a clique begin to imitate the behaviour of the group's delinquent peers (Ploeger, 1997).

In attempting to profile offender characteristics, McCaghey (1980:258) notes that due to the relative novelty of cyber crime, generalizations about offenders are based more on speculation than on evidence. He further cites the study of Parker (1974) who says perpetrators are usually young and aged between 18 to 30 years, reckless, self confident and desperate. Some media reports indicate that some perpetrators in Ghana have been known to be as young as 13 years of age. Additionally, just simply being young elevates the tendency of associating with bad company which could have harmful social interactions. Further, being young and unemployed increases the likelihood of committing crimes (Entorf & Spengler, 1998).

University of Ghana http://ugspace.ug.edu.gh

The Ghana country Report by the United Nations Development Programme (UNDP) for year 2007 states that the nation has a rapidly increasing population growth rate at an average of 2.7 percent per annum over the past two decades. This high growth puts incredible pressure on the labour force and this has been identified as a main reason for the high incidence of youth unemployment in the Ghana. The Ghana Statistical Service Report (2005) puts the unemployment rate at 10.4 percent for males.

In what can be considered an application of Merton's ideas, Ken Attafuah, a Ghanaian criminologist indicates that prior to crime participation, most armed robbers had encountered barriers to their "upward social mobility". He further lists the following as constituting society's measures of success- attaining good grades, advancing in school, acquiring a trade or vocation, winning respect, finding a job, making good money and acquiring material things (2008: 49-71). Most of the robbers interviewed by Attafuah (2008) indicated that they lacked easy access to high quality education, training, employment and inheritance which for them represented the conventional goals of society and hence they had to resort to crime. Attafuah(2008) draws upon Merton's Strain Theory to offer some explanations as to why people engage in crime. He indicates that the armed robbers in dealing with social strains due to blocked opportunities choose to innovate as a mode of adapting. Additionally, Attafuah(2008) states that advances in high technology gadgets have not only further expanded opportunities for criminality but also ensured greater efficiencies in crime executions.

In their study on how tertiary students perceived cybercrime in Edo State, Nigeria, Olusi et al. (2009) contend that the youth of a nation represent its wealth and when this demographic group

University of Ghana http://ugspace.ug.edu.gh

do not find pride in labour but would rather seek rapid means of making illicit money, it poses a threat to the well being of such a society. The study discovers that most students did not view cybercrime as being wrong and showed interest in getting involved if they got the opportunity. Their study also indicates that mostly male students got involved and usually sent out spam mails. Olusi et al. (2009) further add that the success gained by the those the students knew, they were encouraged to want to try cyber crime as well.. They note also that cyber cafes that operated in Edo State, Nigeria, did not put in any measures to curb cyber criminal activities as they were profit driven.

3.6.1(b) Economic and Political Failures

The Political Economy of any nation has severe implications for its populace. A stable and sound political and economic environment reflects in the social conditions. The citizens are provided with all the basic amenities and infrastructure to enhance their quality of life and this in turn affects the civil obligations of the populace towards paying taxes, carrying out their civil duties etc. On the other hand a deficient political and economic environment can result in rapid social disorganization.

Against this background, Adogame (2005:556) shows the fruition of '419' scams in Nigeria as the nation went from "oil boom to oil doom". As Nigeria went through various economic deregulations, austerity measures, structural adjustment programs, misappropriation of money, corrupt elites from both the military and civilians sectors etc., enterprising individuals sought ways to cushion their economic hardships, albeit, through illegal means. This, according to

University of Ghana http://ugspace.ug.edu.gh

Adogame, they did by devising many fraudulent schemes with the aim of raising funds and through the assistance of expatriate partners in the western countries. With the country undergoing economic and socio-political transformations, the situation gave impetus to the scammers to persuade unsuspecting individuals to move funds located in Nigeria to offshore accounts in order to prevent them from being seized, squandered or devalued. Further, legitimacy was given to scam acts by claiming that "the initiative was an unofficial and indirect strategy to recover from the West much of the country's wealth and resources stolen during colonialism" – Adogame 2005.

Glickman (2005:475) concurs with Adogame when he adds that ordinary Nigerians may silently feel some sense of pride in taking westerners "to the cleaners". Perpetrators of 419 schemes make unsolicited contacts with people living in foreign countries with promises of mutually beneficial business deals which are non- existent. Needless to say, the business partner living abroad is scammed out of money.

Glickman (2005) rationalizes that while it may seem strange to enter into business transactions running into millions of dollars with someone that is shrouded in secrecy, the notion is based upon racial stereotypes which sees Africans as "childlike, intellectually unsophisticated, innocent in business dealings and probably corrupt", (2005:464). This type of mindset is likely to be what fuels crime as people continue to be scammed despite warnings and education on cyber crime activities.

University of Ghana http://ugspace.ug.edu.gh

Glickman (2005) argues further that at the social science level, 419 schemes are a manifestation of cultural and social problems. Furthermore, the Nigerian 419 scams demonstrate a "political and cultural success syndrome" which is largely characterized by "wealth, corruption, political patronage and even elements of witchcraft that make for big man leadership".

Adogame (2009) who opines that a cross section of the youth in African countries where Advanced Fee Fraud syndrome is practised, are disillusioned with their Governments and leaders in the face of constant economic, political and social crises. Their disappointment with the so called elites has given them "legitimacy to further their vices". Out of surmounting frustrations, the advanced fee fraud services offer perpetrators a feasible conduit towards upward social mobility. For these fraudsters, if the 'climb on the social ladder' is not attainable through legitimate means then they are only emulating their corrupt leaders who have risen to the top by the use of dubious means.

Adeniran (2008) acknowledges that every society has norms that define acceptable behaviour, and agents of socialization socially transmit such norms. But what happens when there is a incongruity between what is taught and what is observed? Can the youth really be expected to steer clear of fraud when they can see that fraudulent individuals have great affluence and society does not despise them for their questionable wealth? Ninalowo (2004) opines that in societies such as Nigeria with gross structural inequalities, weak sanctioning system and wide gap between the "haves" and the "have-nots", there is a tendency for the deprived to reject rules and embrace illegal means of achieving culturally prescribed goals.

University of Ghana http://ugspace.ug.edu.gh

Therefore, the involvement of youth in cybercrime cannot be separated from the value that many societies place on Wealth accumulation.

3.6.1 (c) 'The Triple Engine A'

In the view of Cooper (1997), there are three major features of the Internet which combine to accelerate and intensify online fraud. These are Access, Affordability and Anonymity. They are jointly referred to as the "Triple A Engine" (Adeniran, 2008:6).

Access to internet use is encouraged as most of the cyber cafes are profit driven the higher the number of users the higher the rate of profit hence little effort is shown to drive criminals away from cafes (Olusi, 2009). The Internet is reputed as the world's largest computer network with an estimate of 1.1 billion users (Global Reach 2003). Today, virtually anyone can access the Internet with a phone line, a computer, and a modem. As such, Internet technology has created a new form of criminality i.e. 'cybercrime'. It is now possible to gain access to a computer without leaving home and to engage and related electronic frauds without leaving a trace.

Adogame supports this notion by adding that the internet gives sufficient opportunities for nameless and faceless fraudsters to flourish. The internet affords perpetrators the ideal medium to communicate with large numbers of people under a cloak of anonymity which means that discovery is made more difficult and leads to an increase in the number of people being defrauded.

University of Ghana http://ugspace.ug.edu.gh

Other studies support this notion by adding that from a criminological perspective, the internet is viewed as a powerful tool for the unscrupulous to perpetrate offences while maintaining anonymity through disguise and a formidable challenge to those seeking to track down offenders. (Yar 2005:6 ; Snyder 2001: 252; Joseph 2003: 116-18).

3.7 Response of Law Enforcement Agencies

Cyber space is still by and large "terra incognita" (Chawki, 2009:16) . This implies that there lies plenty of room for criminal activity. In trying to combat cyber crime, Glickman (2005), notes that fraudsters remain difficult to apprehend. Scam operations are quickly shut down and tracing the origin of emails as a result of a combination of advanced technology and global internet links are proving very difficult. Glickman adds that by the time a server has been found, "the scammers have scrammed". Additionally the under reporting of the crime as a result of victims humiliation and fear of being arrested also presents a problem to the detection and apprehension of criminals.

Tettey (2008:244) contends that due to the "ubiquity, fluidity and speed " through which these scams are perpetrated, a holistic global collaborative solutions is required to address the problem. The transnational nature of the internet predicates that there would be "jurisdictional complexities" which security agencies have to deal with.

University of Ghana http://ugspace.ug.edu.gh

In tackling the 419 syndrome in Nigeria, the BBC (accessed 25th oct., 2009) reported that the Economic and Financial Crimes Commission otherwise known as the EFCC had shut down 800 fraudster emailers and made arrests of 18 high profile "cyber crime syndicates". In conjunction with computer giant Microsoft, the EFCC is collaborating in order to use "smart technology "rather than raids on internet cafes. Cybercrimes continue to remain a challenge to Nigeria security agencies despite efforts to counter it.

Cyber crime activities in Africa are negatively impacting on Africa. In Olowu 's (2009:14) opinion, despite progress made to tackle the problem, most of the laws addressing the phenomenon are in his opinion rather obsolete.

3.8 The Modernity of Witchcraft

Stories of the occult and hunt for wealth has always abounded in African societies. An increasing anthropological literature has explored the ways in which emerging inequalities in Sub- Saharan Africa have played out in dialogues concerning the occult (Comaroff & Comaroff 1999; Geschiere 1997; White 1997). Most of these literature is based on an understanding of what Geschiere (1997) referred to as "the modernity of witchcraft". This is the combination of modernity in Africa and the response of witchcraft traditions to modern social dynamics.

University of Ghana http://ugspace.ug.edu.gh

Smith (2001) points out that Nigerian stories of rituals and occult relating to wealth attainment reflect the pressure and uncertainty of class and kinship struggles. Also as a result of rapid social change in Nigeria, there exist an increasing conflict between individual needs and widely shared values of social obligation. Smith (2001) further cites that noting the pressures of Nigeria's economic insecurity, individual ambitions remain in constant contradiction to obligations to kin and the wider community. In Cameroon, the situation is somewhat similar. Jua (2003: 22) comments on how Cameroonian youths believe they can enlarge their "fields of possible" by means of various improvised practices, including occultism. He notes that the youths are compelled into going to extraordinary lengths in their quest to increase their social capital. Correspondingly, Comaroff & Comaroff (1999) indicate how inequality essentially gives rise to "occult economics". Also, Meyer (1995) writes that Ghanaian stories of satanic riches are part of a popular culture which one may refer to as a 'culture of poverty'. It could therefore be deduced that those people who choose to indulge in rituals and the occult, do so due to economic hardships.

In the past in Ghana, there was belief in 'sika duro'(blood money) and Nzema beyie (witchcraft). What is of interest now is that it is speculated that these occult processes are now being combined with modern 21st century technology for the commission of cyber fraud or "sakawa". Assimeng (2010:167) hints that the issue of the occult is better "believed than discussed" as the phenomenon is quite an intricate one. The visual, audio and print media are rife with stories of young people indulging in the occult in order to gain wealth. Assimeng (2010) explains that there are those Ghanaians who are willing to seek "short cuts" to acquire

University of Ghana http://ugspace.ug.edu.gh

what society qualifies as social qualifications and therefore do not wait for the social structure to bestow upon them "appropriate rank and esteem" as it was done in the past. Despite purported dangers involved with relevant rituals, there is continued indulgence. Some alleged rituals include sleeping in coffins, not bathing, not eating most desired food, etc. Actual proof of indulgence is difficult to ascertain but it is becoming part of the social reality. In line with the symbolic interactionists, Thomas & Thomas (1928: 351) who postulate that based on the interpretations individuals give to situation, man's creative capacity allows him to believe that " if men define situations are real, they are real in their consequences (cf. Ritzer, 1996). Those who choose to indulge in rituals and the occults believe that the results they obtain are as a consequence of their actions. Even though it may be difficult to prove empirically, the actors believe in this, based on meanings that have been assigned to conducting rituals.

University of Ghana http://ugspace.ug.edu.gh

CHAPTER FOUR

DATA ANALYSIS AND PRESENTATION OF FINDINGS

4.1. Introduction

The major intent of this research was to investigate the experiences and opinions of youth involved in cyber crime in Ghana. The objectives which informed the research included attempts to find out the backgrounds of those involved, the motivations for their involvement as well how they utilize their social capital to acquire and hone their skills. Another key objective was to examine the strategies adopted by the government security agencies in combating the menace. Consequently, the study sought to engage the respondents through in-depth interviews towards eliciting from perpetrators, possible motivations for involvement in cyber crime. The study also sought to use the Differential Association and Strain theories as the basis for examining youth propensity to cyber crimes. In this chapter, the study presents and analyses data collected from the respondents.

University of Ghana http://ugspace.ug.edu.gh

Table ii: **Profile of Respondents**

Respondents	Age	Marital status	Religion	Highest level of Education	Resident in	Sex	Business / employment status
Christopher	24	Single	Christian	University Graduate	Agona Swedru	Male	Former teacher
Victor	21	Single	Christian	SHS graduate	Agona swedru	Male	unemployed
John	21	Single	Christian	SHS dropout	Agona swedru	Male	unemployed
Sule	19	Single	Muslim	JHS dropout	Agona swedru	Male	Boutique owner
Roy	23	Single	Christian	SHS graduate	Adjirigano	Male	Boutique owner
Samuel	19	Single	Christian	JHS dropout	Newtown	Male	unemployed
Daniel	24	Single	Christian	University Graduate	Tesano	Male	Barbering salon/ Boutique
Jibrin	18	Single	Muslim	JHSGraduate	Dzorwulu	Male	unemployed
Rafik	20	Single	Christian	SHS Dropout	Agona swedru	Male	Unemployed
Vivian	23	Single	Christian	Beauty school diploma	Tesano	Female	Freelance beauty therapist

Source: Fieldwork, January- May, 2010

University of Ghana http://ugspace.ug.edu.gh

4.2. The Socio- Demographic Economic Background of Perpetrators

In consonance with the basic tenets of Sociology, the researcher was of the strong conviction that the upbringing and residence of an adolescent have critical implication for adult behaviour. Series of questions and follow up questions were asked in order to interrogate the area of residence, level of education, religious affiliation, just to mention a few. The 10 respondents have been fictitiously named as Christopher (24 years), Victor (21), John, (21) Sule (19), Raffik (20), Roy (23), Samuel (19), Daniel (24), Jibrin (18) and Vivian (23). Nine of the respondents were Ghanaians, and one (Roy) was of Liberian citizenry with an estranged Nigerian father but had been resident in Ghana for eleven years.

4.2.1. Age and Sex of Respondents

Even though the study did not employ a survey design, the age and sex distribution of respondents are worth commenting. Out of the ten respondents, there was only one female respondent whose involvement was even partial and intermittent. However, this does not permit the researcher to conclude that the female sex is immune to *sakawa*. It could just be that, they were less likely to admit their involvement and hence, talk to researcher. It will therefore, require further research to establish the involvement or other wise of females.

The age distribution of respondents clearly points to the fact that *sakawa* is predominantly a youth phenomenon. The age of respondents ranged from 18 to 24 years old with an average age

University of Ghana http://ugspace.ug.edu.gh

of 21 years old. In fact, the average age at engagement in *sakawa* could be lower since respondents might have been involved in it for some years "now" prior to this study.

The ages of respondents and by extension, that of *sakawa* practitioners, creates a matter of grave concern. The youth represent the human capital of any country and indulgence in cyber delinquent acts has negative repercussions for their future. The age demography of the youth respondents is consistent with the literature that young people have a higher tendency to commit crimes due to "age- specific rebellion or lack of hindsight" as noted by Eide, 1994. Also the likelihood of committing crimes increases with being young, unemployed, reckless, self confident and desperate (Entorf & Spengel, 1998; Parker, 1974).

4.2.2 Educational Levels of Respondents

The research found a very subtle correlation between classroom education and the practice of *sakawa*. The educational attainments of the respondents ranged from Junior High School up to University. The informants consisted of two university graduates, two senior high school graduates, two senior high school drop outs, one junior high school graduate and one junior high school dropouts and finally one diploma holder.

What is noteworthy about the educational attainments of informants is the conspicuous absence of people who have never been to school. Characteristically, all informants had received some

University of Ghana http://ugspace.ug.edu.gh
form Information Communication Technology (ICT) education because it enabled them to utilize computers and the relevant software.

It was also evident that all the respondents expressed that in attaining their education, they were constantly faced with financial constrains. As a result of this forty percent of informants had to dropout (n = 4).

4.2.3 Occupation of Respondents

Most criminologists have found a strong and inverse correlation between gainful employment and the tendency to resort to wholly deceptive techniques to cheat and defraud. In addition to the lack of employment, there is a wealth of literature that indicates that certain types of occupations are far more susceptible to specific categories of crime (Abotchie, 2008).

It emerged from this research that *sakawa* is predominant among people who have gained some level of education and are willing to work but are unable to find any paid employment. Most notably, the informants were ambitious young people who wanted to improve their lot. Six of the respondents were not in any form of business or trade. Three of the respondents owned boutiques that sold women and men clothing with a barbering salon attached to one of the boutiques. Of all the respondents, only Christopher had ever been employed as a teacher but had quit due to what he considered very low wages in view of his graduate certificate. As he noted:

University of Ghana http://ugspace.ug.edu.gh

" I really enjoyed teaching from my national service to when I was fully employed but I just couldn't make ends meet. I had really struggled to send myself to the university believing that I would get a good job when I graduated. As that did not happen, I had to teach in a JSS school in Swedru but the pay was poor and irregular. My friends were making money by just chatting and used to tease me on being "too known". I decided to quit and join them. I now spend three times my monthly pay a day".

It was not surprising to the researcher that people who had been empowered with knowledge in ICT were embracing *sakawa* as an avenue for amassing wealth. In a country and era where "success" in terms of wealth becomes more important than the means to obtaining it. The sentiments of Jibrin, an 18 year old respondent are worth re-echoing to substantiate this claim;

> What is the essence of a University degree if you cannot find any decent job to do? Now, man has to seek first the economic kingdom and all other things shall be added. There is no alternative to making money. When you get it, people respect you and the girls like people with money. And since I have rolled my sleeves ready to work but cannot find any, what is wrong getting some little money from some "obronis"?

Obronis in this context and in Ghana is a Twi word for any person who is white. After scrutinising the opinions of informants, the researcher is confident enough to state that absence of jobs coupled with general poor economic conditions facilitate youth involvement in fraudulent activities. This assertion is in consonance with the findings of Adediran (2008) who studied the phenomenon of cyber fraud in Nigeria. At 0.005 significance level, Adediran established that unfavourable economic conditions encouraged the youth to attempt illicit activities such as cyber

University of Ghana http://ugspace.ug.edu.gh

fraud. This is supported by Durkheim's Anomie theory, where he contends that during conditions of social instability when those regulations that restrain individuals' desires and expectations within achievable limits breakdown, individuals are likely to find ways to overcome or look for their own substitutes for norms and values.

The major finding of this study is that the youth, especially students at the tertiary levels unemployed have embraced the Information Communication and Technology inventions such as mobile telephones, electronic mailing, "chat" systems and Internet messaging to gain access to upward social mobility. On the other spectrum, the youth have however utilized these services as veritable grounds for carrying out fraudulent activities.

4.2.4 Family Background of Participants

The aspect sought to critically investigate the economic milieu and normative patterns surrounding the upbringing of the participants and how childhood experiences might have impacted on current behaviour. This attempt is backed by and premised on, the social deregulation theory espoused by some sociologists.

Durkheim's famous anomie theory, modernised by Robert Merton and adopted by several others traces the antecedents of criminal behaviour to general levels of lawlessness and improper

University of Ghana http://ugspace.ug.edu.gh
socialization. Below is a catalogue of the family backgrounds of *Sakawa* participants and how these may have predisposed them to delinquent behaviour.

The parentage of each of the perpetrators often has an element of obscurity and deprivation. Three of the respondents reported some childhood separation from immediate families to enable extended family members either paternal or maternal to care for them as their parents were unable to due to serious financial constraints. 50 % of the respondents (n= 5), reported being raised solely by a mother with minimal remittances from their fathers while 30 % (n= 3) reported that they had never set eyes on their fathers. The remaining 20% (n= 2) indicated that their fathers did contribute to their welfare and education. All the respondents intimated that they came from large families with more than five siblings including step siblings. This meant that money was always tight.

Most importantly, perpetrators invariably visit internet cafes outside their own areas of residence. The research revealed that certain suburbs and internet cafes in Accra and Swedru were identified and utilised as "joints" where perpetrators known as "penpal boys" visited.

Regarding parents' educational backgrounds, the research revealed that parents and guardians of *sakawa* boys had very moderate levels of formal classroom education. Among the informants, only one respondent (Roy) had one parent who was a university graduate and was in fact a lecturer in a South Eastern University of Nigeria. It should however be mentioned that the

University of Ghana http://ugspace.ug.edu.gh
respondent and his father have been estranged for some years now. The other 90% of the respondents had semi illiterate parents with the highest qualification as primary school.

The economic activities of parents help us to understand why perpetrators could not look into the future with optimism. It was obvious that there was very little, if not nothing, that parents could bequeath to off-springs. The predominant economic activities of parents included trading in petty items like second hand clothing, food vending by the road sides, seamstress and commercial /taxi driving and farming. One respondent, Roy reported that his aunty and guardian is not engaged in any payable employment. According to him, she occasionally received monthly remittances from his mother who had relocated to the United States of America.

All respondents intimated that their childhood was characterized by deprivations and felt that life was very tough as there was a lack of money most times, never paid school fees on time, never had running water in their homes, could never eat exactly what they wanted just what was available. Three of the four school drop outs indicated that they had to drop out as there was always constraints to buying books, uniforms, shoes. The fourth dropout intimated he just got bored with school and never saw its essence.

Different career aspirations were indicated by respondents. 30 % (n= 3) had hoped to be footballers, 10 % (n= 1) had wanted to be a science teacher, another 10 % (n=1) respondent indicated that he just wanted to be rich, 20 % of the respondents indicated that they wanted to be

University of Ghana http://ugspace.ug.edu.gh

hip-life artistes, 20 % indicated that they would want to go into politics or law. The only female, Vivian, hoped she would be able to be the proprietor of her own beauty salon. None of the respondents had fulfilled any of their aspirations. Those that had wanted to be footballers indicated that they were yet to play in any local league games. The researcher could infer that all the career aspirations indicated were tied more to attaining wealth than to their passion for the career. Sule an aspiring footballer in Agona Swedru noted that:

> "Anytime you see the Ghanaian international football stars, they have the most beautiful girlfriends like actresses, their cars are always very expensive like Sule Muntari's Dodge Challenger, they build very big houses in Ghana. They are very rich, and I so much admire the way they live".

The lack of opportunity of the informants to pursue their dreams and fulfil their aspirations has a serious implication for the involvement in *Sakawa*. This assertion is in tandem with the conclusion arrived at by Ninalowo (2004) after studying "yahooism" in Nigeria. His thesis was summarized that society places premium on wealth accumulation and not the means to attaining it. Hence structural inequalities will cause conflicts "between the "haves" and the "have-nots". This situation increases the tendency for the deprived to reject rules and to embrace illegal means of achieving culturally prescribed goals. *Sakawa* activities cannot be delineated from the value that society gives those with status symbols like money, power etc.

University of Ghana http://ugspace.ug.edu.gh

4.3. Modi Operandi of Sakawa (Methods of Working)

After an extensive interaction with the perpetrators of *sakawa*, it was obvious that though there is no uniformity of modus operandi, there are observable similarities of strategy. In other words, perpetrators adopt varied means to entice, coerce and hypnotize their clients into relinquishing their property and wealth. In view of the poverty and lack of employment opportunities in Ghana, people are adopting new ways to open up their "fields of possible" (Jua, 2003). Among the strategies adopted by cyber criminals are those seen as avenues for getting richer quicker. All respondents indicated that they indulged in "*sakawa*" which included Gold scams, credit card fraud, romantic scams and online ticketing. The modi operandi employed in each of these areas will now looked at in detail below.

4.3.1 Establishing Initial Contact with Client

The whole transaction and interaction begins with the sending of a number of persuasive e-mail messages to numerous recipients around the world. Even though Advance Fee Fraud and impersonation did not begin with the internet, the electronic mail (email) enables criminals to reach to a greater number of potential victims at a very low cost and without being traced. The choice of the internet is based on strategic and economic grounds as noted by one of the informants;

> "The internet gives me the opportunity to "talk" to many people at once by chatting to all of them at the same time in different windows of course. We even have software programs that give you up to one thousand different questions to ask your "client", by the time they are finished responding to these questions you would know everything about

University of Ghana http://ugspace.ug.edu.gh

them." - (Samuel). When probed further as to what type of questions, he mentioned the following

Are you short tempered?

Can you dance? Do you like dancing?

Can you keep a secret?

Do you believe in life after death?

Do you believe in marriage? Why?

Do you believe in monogamy?

Do you consider yourself a neat or messy person?

Do you consider yourself lazy?

Do you drink?

Do you have a role model?

Do you have any siblings? If yes, are they older/younger to you? Are they male or female?

Do you have many friends? Are you in touch with friends from school/college? How close are you?

Do you like cooking?

Do you like eating out at restaurants?

Do you like going window shopping?

Do you like partying? Attending parties? Throwing parties?

Do you like pets?

Do you like to go dancing?

University of Ghana http://ugspace.ug.edu.gh

Do you like to travel? Which has been your best vacation so far? What made it so special?

Do you love children?

Do you own or use a desktop computer or a laptop?

These are just a few of the a thousand questions the scammers have access to trying to know all about the client. They never run out of things to chat with their unsuspecting client. These questions are primarily aimed at leading the other party ('the client/ victim') into thinking they are establishing a relationship with someone who really wants to know them.

The first stage of extorting of money and property begins with the sending out of unsolicited mails and/or faxes. An essential feature of such a mail is that the subject or title is very captivating and enticing enough for to induce the unfortunate recipient to read them. The researcher requested each of the informants to try and recollect some of the titles they frequently used. The titles were varied but the recurring one is "Urgent: Read and Reply as soon as possible". Another popular heading is one that asks recipients to redeem a lottery prize such as "Congratulation: Redeem your Fortune." Mysteriously, it is common for scammers not to provide a subject at all. As explained by Roy

> "Sometimes, it makes a lot of sense not to put a title at all. This creates anxiousness (sic) and the chance that he will open the mail. But it even makes more sense to write a title that easily draws attention to itself such as "greetings, blessed one in Christ". Whatever way you choose to write the title, we make sure that the title will make the recipient feel special and emotionally linked to the sender so as to increase a good response ."

University of Ghana http://ugspace.ug.edu.gh

The content of such a message may appeal to the recipient to assist in the transfer of frozen or hidden funds out of a West African country. Due to several known and unknown reasons some people believe these scams. A massive amount of *sakawa* messages are sent out every day by *sakawa* perpetrators. While the majority of recipients ignore their contents, there is always the probability of a small percentage of gullible individuals responding and they often end up having their money stolen or credit card details pilfered at the hands of fraudsters.

The initial task of *sakawa* boy is to lure the victim into releasing personal information which will then be surreptitiously used to drain the victim's accounts and engage in identity theft. This implies that the initial email must be highly persuasive and credible to both local and foreign recipients. The observation of the researcher was that victims were often lured because limited or no funds are requested at the initial stages and that the victim's expectations of making huge returns are exaggerated.

With reference to the content of such e-mails, a deliberate effort is always made to assure the recipient that the scammer is a sound and trustworthy associate with a genuine profitable business venture. A *sakawa* message , for instance may begin with the sending out of an official looking e-mail purporting to be from the relative of a former senior government official. Such a relative, invariable dead, would be said to have accrued large sums of money prior to his death which is currently being held in a bank account within the country from which the email is being sent. In such a scenario, Daniel, one of the informants narrated alternative ways of swindling a client;

University of Ghana http://ugspace.ug.edu.gh

"The first move is to express confidence in the clients ability to offer the assistance needed. We will then ask for the help of the recipient to remove the money by channelling it through his or her bank account with the assurance that his collaboration will earn him about 30 percent of the total sum. If the client consents to the terms of the venture, he is requested to provide personal information such as address, employer, social security number, bank account information, etc. The vital information could then be used in a manner that I cannot possibly describe to you...My Nigerian friend taught me this method but I hardly use it because it requires a lot of people helping you and can take a long time to bear fruit".

This means that there is some growing collaboration between the *sakawa* boys of Ghana and Nigerian '419' scammers to improve on cyber criminal activities.

4.3.2 Engagement and Process of Defrauding Clients

The point must be emphasised that messages sent by clients are usually bogus intended to defraud and yet some people tend to go along with these fraudsters. Most of the messages request assistance to transfer a fixed amount of money into the recipient's bank account. Should an individual receive and respond to one of these messages, the sender has several options available to defraud the victim. Irrespective of the technique that is used, the fundamental principle is to slowly drain the funds of the victim over time. At this juncture, it will be useful to state verbatim the confession of Raffik, one of the informants

"It is advisable that at the initial stages, you ask for a small donation to begin the processing of documents that will ensure the successful transfer of the money of a deceased wealthy relative out of Ghana. Further payments must be made because of

University of Ghana http://ugspace.ug.edu.gh

"problems" in obtaining the account. The processing of the documents becomes unending until the fool is no longer willing to pay by which time I will be glad to cut ties with him or her."

Multiple fraud schemes have been reported by the various informants in this research. Rafik reported of posing as a lawyer seeking assistance to obtain funds from a deceased client. Christopher also reported of impersonating as a government official who had over-drafted a business contract and that he needed the assistance of the recipient to get the over- drafted amount out of the country. In the case of Victor, he confided in the researcher of posing as the child of a deceased wealthy diplomat who had left behind a significant amount of money. Victor appealed to the recipient to come to his aid otherwise he loses his fortune to other living relative. In the case of John, he claimed to be suffering from a terminal illness, in which case his death was imminent. John therefore needed a trustworthy person to bequeath his wealth to so that it is forwarded to religious charities around the world. All the male respondents admitted to changing to female roles to suit the scam at hand at one point or another. The researcher concluded that the internet allowed sakawa perpetrators to be able to "gender switch" as theorized by Adediran(2008) or to status switch as recognized by researcher.

4.3.3 Gold Scam

Ghana is renowned as a land of gold and Ghana's youth are utilizing this prominence to defraud foreigners. Most of the respondents in this research confessed of indulging in gold scams on a number of occasions. Here, the victims are consciously sought for instead of the usual strategy of sending emails to randomly selected email addresses. As narrated by Victor-

University of Ghana http://ugspace.ug.edu.gh

"A prospective gold buyer can be identified online with the help of any business website such as "mate1.com". This makes it possible to easily trace and obtain a list of email addresses of business men. After that, through manual or with the help of an email software (atomic email sender), emails are sent out inviting buyers to buy gold from you. Sometimes, samples of high quality gold dust are sent to clients that insists on getting samples via any courier service. Once client receives the samples and expresses interest in doing business, details of price and company registration procedure with corresponding costs every step of the way must be undertaken. Obviously, the cost of all this is on the client. These include costs of license and shipping of sample to respective countries".

With respect to the gold scam, several dimensions and versions were reported by informants. Smelting of gold dust into bars for instance is a known and utilized money making avenue. This is usually done with false Precious Minerals & Marketing Corporations (PMMC) or the Geological Survey Department letter heads and old edited transaction documents. After the initial deposit payment, a story is fabricated to explain major hindrances why the deal is not going through. This unforeseen difficulty will therefore, require further inflow of cash from client. Stories could range from customs interception due to unavailability of a particular document or clearance certificate. Usually there is a lot of reluctance and hesitation at this point, but due to the financial commitment that has been made, the clients are compelled to pay. The back and forth transactions prolongs for a long time until the client becomes frustrated by which time a huge financial amount would have been paid to the *sakawa* boy.

University of Ghana http://ugspace.ug.edu.gh

Another dimension to the gold fraud is the issue of money "recoupment". The researcher labels this category of fraud as very malicious in the sense that duped clients are sought out and "reduped" without remorse. Here, scammers contact clients and produce a list of victims that have lost huge sums of money through internet scam. Their victims are contacted and lured into believing money lost can be retrieved but only after a required fee has been paid. They mostly impersonate the Ghana Police Force (over the internet) and try to recoup money lost. The cooperating client undaunted in retrieving his lost fortune is convinced to make the requested payments. However, far from regaining lost money which never surfaces he or she only subjects himself or herself to further pain and loss.

4.3.4 Online Dating

This was declared as most common, easiest and the least sophisticated scam to pull off. *Sakawa* perpetrators are always willing and able to cast their net anywhere, no matter how far or deep. People who patronize dating websites abroad are usually more susceptible to this type of scam. Foreigners who seem to be desperate about establishing amorous relationships are also taken advantage of. Popularly called referred to in Ghana by cyber criminals as 'come and marry', online dating begins with the registration of a site through an internet protocol(i.p.) configuration and credit card payment. This payment is done through the acquisition of 'liberty' a software which can be locally purchased and paying a hacker online with the liberty. The liberty is a form of currency to hackers internationally. The hacker generates a credit card which the scammer uses in registering at the dating sites.

University of Ghana http://ugspace.ug.edu.gh

Sites where clients are sought for are blocked to West African countries and as such, accessing these sites requires the use of different internet protocol addresses that represent European and American countries. Mobile phone communications are achieved through the use of software called **"magic jack"** that switches the caller identification off as a caller from another country. The scammer then advertises his or her profile on the site as a man/woman seeking a partner. Interested dating partners reply with email addresses and sometimes live chat sessions in the website. The client is then engaged in weeks of love chat sessions luring him/ her to the point of sponsoring visa acquisition and passport acquisition bills. These bills range from two to six thousand dollars on the average. Airline tickets to designated countries are also covered by these clients. The victims' inadvertly serve as recipients in receiving items shopped with generated credit cards and also act as transit avenues.

4.3.5 Internet Shopping

Internet shopping involves the use of credit cards to shop online. This is the most basic and most rudimentary form of internet fraud. It requires available sites, credit cards and recipients. The recipients are the risk takers and in instances of fraud detection is subject to arrest. This is the only limitation to internet shopping originally called *sakawa* and now very rare. Since Ghana was blacklisted from being able to conduct electronic transactions, committing this internet fraud has been difficult for scammers.

The common factor in all these forms of internet fraud is the **liberty** or a credit card with authentic credit card details. The '**liberty**' is a software program that allows one to gain valid

University of Ghana http://ugspace.ug.edu.gh

credit card detail that is sold to prospective buyers with varying amounts of money in them. The amount of money in an account corresponds to the amount of liberty purchased. The price of liberty ranges from twenty dollars to a million dollars depending on what you want to buy with it, but it is undoubtedly cheaper to purchase than a credit card. A credible hacker is also required. It is the hackers form of payment that is the 'liberty'. It is with the liberty that the credit card will be generated from.

4.3.6 Ticketing Scam

This type of cyber fraud also requires the use of a credit card. This is also acquired through theft or hackers online again through the payment of 'liberty'. The credit card is used to make airline bookings and pay for tickets. A regular collector is sent to collect the ticket and the ticket is sold to a prospective buyer half the price or in most organized events, the full price. Here, it is necessary to have readily available clients because the ticket can be blacklisted once the error is detected.

4.4 Reasons and motivations

The respondents provided several reasons and motivations for engaging in cyber fraud. The main reasons gathered included poor level of deterrence provided by the legal regime and law enforcement agents, the ease of entry into the 'world' of cyber crime, the profitability of the crime and the opportunity it gives the respondents to support their nuclear and extended families

University of Ghana http://ugspace.ug.edu.gh

and the lack of job opportunities for the youth amongst others. These motivations are explored further below.

a. The Legal Response

The research findings support this assertion that due to an inadequate legal framework, most respondents were encouraged to indulge in cyber crime. All of the respondents mentioned the poor legal regime as a major motivation for engaging in the crime because it was easy to get away with their criminal acts. Additionally, the cyber café owners do not put up any mechanisms to detect any delinquent activities on the internet. One respondent however mentioned that to his knowledge, only one cyber café in Accra could be said to put up strong warnings against cyber delinquent activities and that was *Busy Internet Café*. The respondents did not exhibit any fears towards being detected and apprehended as the Internet provided the ideal environment to get away with crime. This ties in with the literature which discusses how the anonymity of the internet provides the perfect breeding ground for cyber criminal activities (Adogame, 2009; Yar 2005:6; Snyder 2001: 252; Joseph 2003: 116-18).

b. Ease of entry

All respondents stated the 'low entry threshold" as a main attraction to becoming a cyber fraudster. According to the respondents, minimal capital was required. In most cases, high availability of internet cafes and the only equipment required was a webcam. Minimal computer skills were necessary to commit cyber frauds and so it was easy to acquire the necessary skills.

University of Ghana http://ugspace.ug.edu.gh

and the lack of job opportunities for the youth amongst others. These motivations are explored further below.

a. The Legal Response

The research findings support this assertion that due to an inadequate legal framework, most respondents were encouraged to indulge in cyber crime. All of the respondents mentioned the poor legal regime as a major motivation for engaging in the crime because it was easy to get away with their criminal acts. Additionally, the cyber café owners do not put up any mechanisms to detect any delinquent activities on the internet. One respondent however mentioned that to his knowledge, only one cyber café in Accra could be said to put up strong warnings against cyber delinquent activities and that was *Busy Internet Café.* The respondents did not exhibit any fears towards being detected and apprehended as the Internet provided the ideal environment to get away with crime. This ties in with the literature which discusses how the anonymity of the internet provides the perfect breeding ground for cyber criminal activities (Adogame, 2009; Yar 2005:6; Snyder 2001: 252; Joseph 2003: 116-18).

b. Ease of entry

All respondents stated the 'low entry threshold" as a main attraction to becoming a cyber fraudster. According to the respondents, minimal capital was required. In most cases, high availability of internet cafes and the only equipment required was a webcam. Minimal computer skills were necessary to commit cyber frauds and so it was easy to acquire the necessary skills.

University of Ghana http://ugspace.ug.edu.gh

The cost of browsing per hour in Accra ranged from 60 pesewas to Gh¢1 while in Agona Swedru, it ranged between 50 pesewas to 60 pesewas. All the respondents were in agreement that it was quite cheap to browse and this made it quite lucrative as the capital was low and the profits could be very high.

c. Profitability

Most of the respondents also stated that the high level of profitability and gains from cyber crimes made it very attractive. Some of the respondents who were otherwise gainfully employed admitted that the high earnings from cyber crime made them choose the criminal path over other professions such as teaching and trading enterprises. For instance, two of the respondents were University graduates and one was a former teacher, while the other owned a barbering salon/boutique. The only female respondent who was a diploma holder and a trained beauty therapist, also stated that cyber crime was more lucrative than other work and she hoped to make enough money to open her beauty shop.

The profitability of the crime was also supported by western union receipts provided by some of the respondents. The amounts on the receipts ranged from GHC7,047 to GHC 9,163.25 (Appendix ii), a clear indication of the 'high earnings' from the crime and the motivation for participants.

University of Ghana http://ugspace.ug.edu.gh

d. Lack of Job Opportunities

Fifty percent of the respondents were "unemployed" i.e. they had no other form of employment. Respondents claimed that the lack of job opportunities in spite of their educational achievement was one of the reasons why they turned to cyber crime. It is important to note that the educational qualifications of the respondents ranged from JSS graduates to University graduates which indicated that cyber crime cut across diverse educational levels.

Respondents also stated that the anonymity which the crime provided, as well as the lack of violence as compared to armed robbery, made the crime easy to engage in the face of lack of formal employment opportunities.

e. Support to Nuclear and Extended Families

About 80% of the respondents were of the view that the ability to support their nuclear and extended families from the proceeds of cyber crime was a major motivation for entering into the 'world' of cyber crime and their continued criminal activities. Most of the respondents had been able to put other family members through school. Several respondents also mentioned the respect and admiration of family members as a motivation. None of the respondents had experienced any family outrage at their criminal activities. Indeed, there seemed to be tacit family support for their criminal activities as family members routinely came to them for help. Of all the respondents, only one stated that family members did not know of her criminal involvement.

University of Ghana http://ugspace.ug.edu.gh

4.5. Becoming A Sakawa Operator

It is clear from the research field work that people do just become *sakawa* operators over night. *sakawa* is a learned behaviour. It requires intensive indoctrination and continuous learning. Asked about how informants got into the sakawa activity, Daniel replied that;

> "I had to leave school that is the university, for a month and understudy a friend of mine. Previously I was going from school to his house and back but tight schedules demanded I see him frequently and longer. So I moved to his place".

When the researcher probed further to know the motivation to engage and hook on to cyber fraud, one response was that

"it is very easy to learn and does not involve any violence to me or the client. You only need to ask your friends. For those who are not computer literate, they give their clients to others who have more experienced and they share the gains." - John

From the interaction with informants, the researcher can state that perpetrators harbour no guilty conscience nor show any remorse for the effects of their acts. On the contrary, they defined the duping of Europeans as a way of revenge. In the words of Christopher,

> "There is little or no difference between what is going on and what was meted out to our forefathers some few centuries ago because the whites also used their knowledge to take our resources like our gold away".

University of Ghana http://ugspace.ug.edu.gh

This tallies with Neutralization theory as indicated in the literature review. The research indicated that some neutralization techniques were applied. These were Denial of injury. The respondents felt they were not using guns to harm or rob people. Another common neutralization technique was Denial of responsibility. Most of the scammers felt that were propelled into *sakawa* due to circumstances beyond their control like poverty, compelled to help family, their family structure. The third common technique was the Denial of victim where *sakawa* operators felt that they were justified in paying back foreigners for slavery and this was some sort of personal reparation.

For the youngsters who indulge in *sakawa*, a lack of money informs most human relationships. Perhaps, to the youth, money brings respect, acknowledgements and power to the person who has it. The society that Ghanaian youth live in today is very wealth conscious. Images of flashy, luxurious cars, homes and lifestyles are regularly presented to them in the media and the strain that these place on individuals lead to criminal activities. As anti- crime agencies continue to find ways of curbing crime and barriers are being put up to hinder activities, the trend to occult protection may continue.

As Attafuah indicated that progress in technological gadgets not only continue to expand criminal opportunities but also provide greater expertise in crime executions These reasons tie in with the modus operandi of *Sakawa* or cyber fraud as it is facilitated by the use of technological tools like the computer, the Internet, mobile phones etc. Unlike the commission of conventional

University of Ghana http://ugspace.ug.edu.gh

crime which is mostly done on person-to-person basis, cyber crime offers the perpetrators anonymity, low detection and invisibility which all aid in perpetration.

By way of conclusion, it was glaringly clear that sakawa in a relatively new form of crime that eludes the watchful eye of the Law Enforcement Agencies. Cyber fraud is predominantly a youth phenomenon. This explains why informants were enticed into the activity by "a body –body" (Christopher), "E be my paddy" (Victor) or "my class mate from JHS who had made it big" (Jibrin), Vivian commented that it was her boyfriend that showed her how to make money from the internet.

To the majority of these youth, going back to school is not only a forgotten dream but a non requirement to a successful life but they indicated that they would rather make sure that their younger siblings and other external relations are catered for.

4.5.1 Resort to Occultism

The *sakawa* conundrum in Ghana is significantly different from traditional cyber fraud in other several countries because of the alleged resort to spiritual powers. On one hand, in the Western countries, the concern of authorities regarding cyber fraud is identity theft, and hacking, credit card fraud. On the other hand, Africa remains a continent that accommodates people who cling to traditional beliefs in the supernatural forces as sources of wealth and power. There is no

University of Ghana http://ugspace.ug.edu.gh
shortage of stories that ordinary traders, politicians and even bureaucrats seek "juju" for different purposes. Under these circumstances, the law enforcement agents seem to have been rendered powerless since it is almost impossible to identify people who have "secret rooms" where a snake or disappeared relative is vomiting money for its owner.

In short, juju and cyber fraud are believed to be two separable illegal and notorious avenues for extorting money and property from unsuspecting victims. It is therefore not surprising that Ghanaian youth are believed to be blending these two techniques to achieve the same result. The researcher asked series of questions and that sought to verify this mystery. The responses showed that most of the rumours were indeed, reflective of the reality.

Though informants were extremely economical with information regarding spiritual participation, one of them confessed to having been "fortified" in some way. New entrants such as Victor, Roy, Rafik, indicated that usually they visited Ghanaian shrines and 'mallams' while the experienced ones such as John and Samuel had visited similar shrines in Benin. They were however very reluctant to discuss the specifics of visits to various shrines.

Informants did not have to talk for long for the researcher to identify the reasons for resorting to supernatural forces. There were two major reasons that emerged as the common denominators in the confession of seven of the informants. The first was to be guaranteed of the gullibility and susceptibility of victims to respond to their messages and subsequently go along with the tricks

University of Ghana http://ugspace.ug.edu.gh

of the scammer. The second reason was to maintain anonymity and therefore nullify all attempts by police to arrest culprit in case a victim reports to the law enforcement agencies. Christopher, Daniel and Victor all said they did not patronize anyone for talisman or prayers but agreed they knew those who did and did not see a problem with it.

Thus, the assurance that someone will necessarily respond positively to a scam, that one is more likely to evade arrest when detected and the visible success of those who indulge in cyber crime provides a fertile ground for people to resort to sakawa.

4.6 Responses and Challenges of Law Enforcement Agencies

This study was an exploratory one to foray into a contemporary twist on old fashioned crimes of fraud and deception. The modern angle to this was the application of technology such as the computer and internet. Frauds are being conducted now across geographical locations and between people who may never have physically met and have only been in contact primarily through the internet.

As a result of trying to understand further the scope of cyber crime, it was therefore one of the objectives of the research to discover what the general response of the mandated Law Enforcement Agencies was to the *sakawa* phenomenon. On preliminary visits to the police and serious fraud offices, it was determined that there was no specific unit mandated to handle cyber crime or sakawa. The researcher was told at the police headquarters that this was in the pipeline.

University of Ghana http://ugspace.ug.edu.gh

Additionally, the researcher realized that it would have been difficult to pin down a number of key informants at the Police Services and the Serious Fraud Offices to interview as a result of their very busy schedules. So researcher had to settle for speaking to an officer each from both crime fighting institutions, hence the small number of informants. But as earlier reiterated, this was just to shed more light on the phenomenon under study to gain the perspective of those tasked with dealing with crime issues in the country. The interview schedule was themed under attempting to understand legal definitions (if any) were given to cyber crime and sakawa, to understand the scope and magnitude of the problem and collate any statistics that had been gathered. Further, the study wanted to determine if the police had knowledge regarding the profile demographics of those involved and crime areas. Also it was the intent of the research to ascertain how the selected security organisations were reacting to the problem.

One of the cardinal aims for this research was to gain an understanding of the responses and actions of the Serious Fraud Office(SFO) towards combating, if not eliminating, cyber crime. The first attempt during the interview session was to find out how Ghanaian law enforcers define cyber crime and how such definition varied from what is defined as *sakawa*. This question was posed to an official at the SFO and his response which could be regarded as the voice of the SFO was that;

> "In my opinion, cybercrime is any form of crime where electronic systems, the internet, computers are used to commit a crime. Some examples are "419" scams from our brothers in Nigeria and hacking."

The key informant of the Ghana police gave the following as a definition for cyber crime;

University of Ghana http://ugspace.ug.edu.gh

" Any crime committed using the computer, internet and mobile phone to fraudulently steal from another person".

Further contradictions were observed when the official was required to define sakawa. His answer as to what constitutes Sakawa was that;

> Sakawa involves the use of the internet to cause an unsuspecting person or entity outside your jurisdiction to part with valuable assets like money, phones, video cameras etc.

It was obvious from the interviews that there are still ambiguities about the phenomenon as the informants provided vague and sometimes contradictory views. The first step to tackling a major canker such as sakawa is to enact a specific law that defines the crime and prescribes the appropriate sanctions to be meted out to culprits.

Both officers however indicated that as of now, Ghana lacked a cyber crime law and that there was a Bill on cyber crime being put before parliament waiting to be passed. This Bill was a collaborative effort between the Ghana Police and Internet Service Providers Associations with significant input from Europol and Interpol. Because of this lack of regulation, presently in Ghana, admissibility of digital evidence is at the discretion of the trial judge and in most cases, digital evidence is not allowed. Further, as the police key informant notes:

> "As of this moment we do not separate cyber crimes or cyber frauds from regular frauds. All such crimes are handled by this unit and are grouped as one".

The key informants also expressed challenges involved in identifying the fraudsters. The law enforcers were usually contemptuous about the expectations on them to trace and apprehend

University of Ghana http://ugspace.ug.edu.gh

"hidden and complex crimes" such as *sakawa*. This stems from the fact that communication between

> "The boys and their victims are out of the view of everyone including the police. In addition, the conversations or rather negotiations between the perpetrators and the potential victims are shrouded in secrecy. It becomes virtually impossible to detect such crimes with our limited logistics. We can only rely on the few victims who report to us but this is very rare because the victims will rather report to security agencies in their home countries and from our information, the victims are usually advised not pursue the case in Ghana. So under the current constraints, we are doing our best"- police key informant.

This ties in with the literature where Glickman (2005) indicates that fraudsters are difficult to apprehend as scam operations are difficult to trace to origin due to the complexity of the Internet. It is therefore, not surprising that the police have often confessed of "swooping on internet cafes and arresting all users at what they term as "odd hours". Most of such people often turn out to be honest and innocent patrons.

Yet the agencies are optimistic that the menace could be minimized through public awareness campaigns on the threat of *sakawa* schemes.

The efforts of the Internet Service Providers were identified as being critical in the attempt to combat cyber crime. It is acknowledged that a concerted and collaborative effort across the

University of Ghana http://ugspace.ug.edu.gh

territories of African countries is needed to solve the problem. The effective sharing of information among sovereign countries will help us to make a head way in nipping the canker in the bud. The conclusion of the SFO informant is worth quoting verbatim;

> "it would require a holistic approach which would include all stakeholders, from youth organizations, churches, mosques, police, cybercafés, schools, banks neighbouring countries. This would involve public education. Also it is important to ensure that when caught, offenders are not allowed to benefit from their crimes. Their money, cars, houses should be confiscated."

There is generally a poor legal regime for fighting cyber crimes in Ghana. The Criminal & Other Offences Act does not specifically criminalize cyber crimes. Indeed, the law was passed in 1960 and subsequent amendments have not made provisions for crimes committed with the use of modern technology. Discussions with officers of the Documentations and Visa Fraud Unit of the Ghana Police Service revealed that cyber crime perpetrators are charged under criminal provisions such as Fraud and Defrauding by false pretences. These provisions however require that dates and geographic locations where the crimes were perpetrated must be stated. This is therefore a major challenge for law enforcement agents. And this legal lacuna makes it easy for perpetrators to get away with the criminal acts.

The law enforcement agents also showed a poor knowledge of the legal regime. Officers of the Ghana Police Service during the interviews stated that there was no law specifically

University of Ghana http://ugspace.ug.edu.gh
criminalising cyber crimes. However, the Electronic Transactions Act of 2008 (Act 772) criminalises stealing, unlawful appropriation and other cyber offences. The poor knowledge of the law enforcement agencies in this area clearly contributes to the prevalence of the crime since the Police would be unable to prosecute offenders under the Act.

University of Ghana http://ugspace.ug.edu.gh

CHAPTER FIVE

SUMMARY, RECOMMENDATIONS AND CONCLUSIONS

5.1. Introduction

The final chapter of the study summarizes all that has gone by to and reiterates the major findings from the field. Once the researcher was armed with first hand information from the study area coupled with reports from the existing literature, she was able to draw conclusions and build a conceptual model for *sakawa* occurrence. The research also added useful recommendations. Some of the findings that are worth re-echoing and the appropriate solutions are catalogued in this final chapter.

5.2. Summary

This study has been devoted to the study of cyber crime or what is popularly known as "sakawa" in Ghana.

As stated in the first chapter of this research, the main purpose of the research was to seek a sociological motivation for the high prevalence of youth involvement in sakawa in Ghana. Due to the in-depth nature of the information required from respondents, the methodology of the research was the use of open-ended questions in a relaxed interview format, aimed at getting the respondents to speak freely about their family and educational backgrounds, and their reasons for engaging in cyber crime.

University of Ghana http://ugspace.ug.edu.gh

5.2.1 Socio-economic Background of Respondents

The research clearly revealed that respondents were from economically deprived backgrounds. A large number of respondents were compelled to drop out of school due to the economic difficulties in their families. In line with the Strain theory as discussed in the review of existing literature, all of the respondents used cyber crime as a means of attaining their economic dreams and societal goals due to what they perceived as blocked means to attain same legitimately.

5.2.2 Types of Cyber Crime Activities Engaged In

The research also revealed that youth perpetrators engaged in different types of cyber crimes like gold scams, online dating or "come and marry", internet shopping, charity appeals and ticketing scams. Respondents all seemed to commence their criminal activities with crimes that had the lowest entry barriers such as equipment, and progressed to more sophisticated crimes as their economic status improved. For instance, perpetrators started with internet dating scams and moved on to gold scams and Advanced Fee Fraud.

5.2.3 Reasons and Motivations

With regard to reasons and motivations for engaging in crime, most respondents gave motivations ranging from a poor legal regime which did not deter perpetrators, profitability of the crime, family support and encouragement (albeit tacitly in most cases), to few job opportunities. In addition and consistent with the Space Transition Theory, the anonymity

University of Ghana http://ugspace.ug.edu.gh
provided by the internet, identity flexibility and the lack of associated violence in committing cyber crimes, made participation by youth easy and attractive.

The Learning theory and Neutralization technique also support the research findings. All respondents stated that the criminal activities were learned, mostly from peers and close associates. This response also ties in with Sutherland's Differential Association. All respondents also applied some neutralization technique such as denial of victim, denial of responsibility and denial of injury caused to the victims.

5.2.4 Response of Law Enforcements

The poor response of the law enforcement agencies, and the gaps (supposed and actual) by the criminal law regime also encouraged perpetrators to commit more crimes and be more audacious in their activities. In sum, the law served as poor deterrence to new perpetrators or to discourage existing perpetrators. The research findings also indicated that none of the respondents had a strong fear of being caught or the consequences they were likely to face on being apprehended.

5.3 Research Recommendations

Computers and the internet have now been accepted as the mark of all progressive societies of the twenty-first century. This idea seeks to emphasise the fact that cyber crime transcends geographical boundaries and that it has acquired a "universal jurisdiction". Computer technology

University of Ghana http://ugspace.ug.edu.gh

emerged as one of the remarkable inventions that penetrated every continent and many households. However, this positive information and communication tool has served as a veritable ground for carrying out nefarious and fraudulent activities by the youth all over the world. The menace is to the extent that no nation or even individual is immune to the activities of this indignant subculture.

The researcher therefore recommends that the fight against cyber crime in Africa must be collaborative, concerted and inter-territorial. This is the sure way to trace, track, apprehend and severely punish both domestic and international cyber criminals. There must be a regional normative initiative that would streamline and synergise the efforts of African states in combating the phenomenon of all forms of cyber crimes.

5.3.1 Vulnerability of Africa

An important factor making Africa a source and target of much cyber-criminal activity is the growth of international banking and money-laundering. The unique opportunities of a quickly developed financial infrastructure allowing anyone to transfer monetary fund to any State, anonymously and through tangled routes have caught the attention of cyber-criminals. Electronic transfers are an efficient tool for concealing sources of money intakes and laundering illegally earned money. There are many well-known online money laundering cases involving victims in Africa who were tricked in order to steal their identity or transfer money from their real accounts using phishing and scams (Ojedokun,, 2005, p.14; Oriola, p.238).

University of Ghana http://ugspace.ug.edu.gh

If Africa is to continue to attract foreign investors in order to ensure sustainable economic development, the researcher recommends the promulgation and implementation of concerted laws instead of the ad hoc measures adopted by individual countries. In many of the few countries with specific legal framework against cyber-crimes, the existing laws lack the potential to tackle the transnational aspects of the phenomenon. For instance, the Nigerian draft Bill mentioned earlier limits all powers of search, arrest, prosecution and punishment to the extent of the country's territorial jurisdiction. This must cease and give way to transnational policies.

5.3.2 Internet Facilities are Cheap and Safe

This study confirms the claims of Dampsey (2001) that electronic communication afford tremendous opportunities for criminals to connect with a large population of potential victims cheaply and efficiently. This feature of the internet coupled with the likelihood of victims not reporting the crime to the police serves as incentive for the youth to engage in cyber fraud. Buchanan and Grant (2001), report that regardless of the method used in swindling the victims, there is always low likelihood of the victim reporting their experience to law enforcement agencies. Two reasons were provided to explain why some victims are reticent about cyber crimes. The first reason is that the victim fears that he or she will be prosecuted for their involvement in the illegal act. The second reason is that victims may feel embarrassed for having responded to and acted upon emails sent out by persons they do not know or have never met.

The researcher recommends that there should be public policies that aim at preventing and combating this form of crime. This could be done through raising awareness about the common

University of Ghana http://ugspace.ug.edu.gh

modus operandi of perpetrators as well as encouraging victims to report their experiences even if this may not lead to any arrest of scammer.

5.3.3 Tackling Youth Unemployment

Unemployment and under-employment were seen as critical factors luring the youth into sakawa in both Accra and Swedru. As more and more youth continue to suffer unemployment, this creates a lot of anxiety about their future. Most Ghanaians in urban and rural settings adapt to change and respond to crises or opportunities by changing their means of making a living and by practicing a number of different livelihood options at the same time (UNDP Report 2007). The youth involvement in cyber crime was a response to their unemployment situations and a means of making a living.

Sakawa has been observed as a popular accepted means of economic sustenance among Ghanaian youth, especially the college age ones. The formal sector has few and very competitive employment opportunities for university graduates while available opportunities to youth in the informal sector are hawking, shoe shine, potters, to mention a few. It must be realized that these tend to be socially degrading and physically strenuous while sakawa offers wealth at the stroke of a computer keyboard. The present moral codes of the nation do not necessarily espouse dignity in labour and therefore the youth themselves see no reason why they should have to labour hard when there are very easy economic opportunities offered by the internet.

University of Ghana http://ugspace.ug.edu.gh

The researcher thus strongly advocates for intervening social policies such as social benefits for the youth. It is laudable to see the Government making good its pre electoral promise to resolve the problem of youth unemployment. The National Youth Employment Program (NYEP) is ongoing at the national level to train and or retrain some of unemployed youth. This and other proactive economic policies that could engender employment opportunities for the youth must be encouraged to boost their chances of being employed or self employed.

5.3.4 Online Security Awareness

Poor security awareness means that investments to fight cyber-crimes are minimal, leaving businesses across Africa vulnerable to cyber-crimes or online attacks. The African continent is in dire need of strong ICT security awareness training, targeting native speakers to educate users, employees and law enforcers to understand the risks and prevent attacks.

Users in Africa also utilise international social networks such as *Facebook* and *Myspace* for communications, friendships, blogging and other activities that, if not taken with caution, can lead to identity theft and malicious activities against home users and employees in both private and public sectors as long as there is no policy.

Olowu (2009) espouses that Information security awareness is crucial for combating cyber-crimes. In Africa, there is a significant lack of security awareness among users, whether the general public or organisations and enterprises. Comparing security awareness in Africa to Europe or the US, one would see far less effort being made to raise awareness among users. One

University of Ghana http://ugspace.ug.edu.gh

of the major factors that make information security awareness programmes ineffective in the region is that most ICT security awareness programmes available are in English, making them difficult to implement in a region where the overwhelming majority are French, Arabic, or Portuguese speakers.

5.3.5 Cultural Renaissance

The exaltation of sudden wealth by society without questioning its source must be checked motivates criminal behaviour. Every society has norms that define acceptable behaviour and agents of socialization socially transmit such norms. But what happens when there is a discrepancy between what is taught and what is observed? Can the youth really be expected to eschew fraud when they can see that fraudulent individuals have great affluence and society does not despise them for their questionable wealth?

Ninalowo (2004) opines that in societies such as Nigeria with gross structural inequalities, weak sanctioning system and wide gap between the "haves" and the "have-nots". There is a tendency for the deprived to reject rules and embrace illegal means of achieving culturally prescribed goals. The involvement of youths in Ghana in online fraudulent practices cannot be separated from the value that the society places on wealth accumulation.

The researcher therefore strongly recommends the reorientation to a modern culture that emphasises wealth not the means used to attain it. In other words, the attainment of wealth must

University of Ghana http://ugspace.ug.edu.gh

be seen to be as important as the means to acquiring it. Thus, as we socialize the young ones to value hard work and integrity, this must not be at variance with what they observe among the leaders of society.

To Adeniyi (1999), the youth must be seen as the foundation of for the future growth and sustainable development of any nation. The youth should therefore be utilised as key agents for social change, economic development and technological innovations but not at the expense or morality. We need to advocate for a cultural and social renaissance since it is difficult for any nation to flourish and sustain itself when the youth are not engaged in ways and processes that enhance their capacity. This step will help promote social cohesion and reinforce those norms and ethos that are embedded in the social and moral fabric of society.

5.3.6 Policy and Legislation

It is difficult to fathom the absence of specific laws to respond to sakawa. Lack of regulation invariably equals lack of law enforcement training, tools and techniques used to investigate cyber-crimes. Even though cyber crime or sakawa has pervaded and is damaging Ghana as a nation there is yet to be a specific legal framework against it.

In fact, in the entire Continent of Africa, it is only Egypt, Botswana, Lesotho, Mauritius and South Africa that have attempted to enact specific laws against cyber crime. The South African approach in the Electronic Communications and Transactions Act, 2002, does not hold better as

University of Ghana http://ugspace.ug.edu.gh

the powers of 'cyber inspectors' to search, seize or arrest only envisage cyber-crimes within the South African territory.

It is hereby strongly recommended that policy makers in government, business and law enforcement must react decisively to these emerging challenges. Laws, policies and investigative skills must be developed to apprehend cyber criminals and prevent future nefarious activities on the internet. It is extremely important for Ghana to follow these examples and put together a legal framework that defines and stipulates specific sanctions against sakawa.

5.3.7 Difficulty of Law Enforcement Agencies

The police and other law enforcement agencies have a herculean task when it comes to combating sakawa. Besides the timidity of victims to report, tracing the source of an e-mail in a third world country such as Ghana is a laborious task. The additional cumbersome slow judicial process also detracts victims from pursing cases. Most victims are usually foreigners who may not have the time or afford to relocate to Ghana for a period of time to pursue a case that could take years to prosecute. Hence, without the victim present, it is difficult for law enforcement to pursue the case.

The new media revolution that brought the internet and e-mail technology provides ample opportunity for nameless and faceless fraudsters to thrive. The perpetrators know that they can better communicate under complete anonymity with minimal effort through the use of the

University of Ghana http://ugspace.ug.edu.gh
internet ably backed by spiritual potency. Under these circumstances, most police men do not even bother to initiate investigations into sakawa allegations.

The recommendation that is pushed forward here is the immediate harmonisation of laws against cyber crime at the domestic and regional levels. Although there are a number of approaches around Africa to create a stable online environment, these measures have been few, isolated and uncoordinated. It has been observed that some of these laws conflict beyond individual country borders.

5.4 Recommendation for Future Research

This study has mainly examined the motivations for youth involvement in cyber crime specifically from the perspective of selected sociological theories. There were however significant time restrictions which limited the scope of this research. Notwithstanding, there is room for further research into the area of youth involvement in cyber crime. For instance, it would be important and necessary for future research to examine specific geographic locations and the impact of geography on youth involvement in cyber crime. As respondents in this study were selected from Agona Swedru and Accra, it would be important to study youth in other parts of Ghana in order to establish the general applicability of the results of this study over other parts of the country.

University of Ghana http://ugspace.ug.edu.gh

It would also be worthwhile to investigate the socio-economic impact of sakawa at the meso and macro levels of society. Another area worthy of study would on the impact of cyber crime from the perspective of victims so as to have a more holistic view of the phenomenon.

5.5 Conclusion

The internet has certainly provided unprecedented opportunities for criminals to perpetrate their acts on a wide range of people across geographical jurisdictions. There is convincing evidence that the internet will continue to spread and become essentially ubiquitous in economic and social life. In fact, there is no likelihood that cyber crime will ever be completely eliminated. This serves as enough basis for the researcher to conclude that our societies are going to be increasingly dependent on a fragile and insecure information structure.

According to the World Bank, 'African States are to face great challenges; they have to work by themselves to generate 100 million new job opportunities by 2020 or the region's instability will increase' (World Bank Report 2008, p.15). Statistics reveal that the unemployment rate is very high among youth in Africa, most of whom are university graduates with computer skills and Internet competency. Even where youth do not have access to Internet at home, cyber-cafés are readily available throughout the region at relatively low rates creating high levels of access to the Internet. To discourage cyber crime, African governments would have to focus on job creation and youth engagement strategies that promote pro-social behaviours.

University of Ghana http://ugspace.ug.edu.gh

In addition, there is no easy way to identify the fraudsters due to the use of spoofing and anonymity enhancing software that conceal an individual's location and identity. The internet allows perpetrators the chance to "gender switch" (Adeniran, 2008) and status switch as one can be anyone they want to be online. The best we can do is to persuade and coerce the perpetrators to refrain from its occultism aspect because of its possible linkage to ritual murders and other devastating consequences. Thus, it is imperative that researchers consider the ways that cyber crime changes in tandem with the dynamic nature of the internet. This will improve our understanding of the internet as a conduit for crime in the 21st century.

Finally, a more responsive legal regime, which enables law enforcers to effectively apprehend and prosecute cyber crimes; and thereby efficiently deter perpetrators, is an absolute necessity in curbing cyber crimes.

University of Ghana http://ugspace.ug.edu.gh

References

ABOTCHIE, C., 2008. *Sociology of Urban Communities*. Hans Publications, Accra.

ADEDIRAN, A. 2008. 'The Internet and Emergence of Yahooboys sub-culture in Nigeria', *International Journal of Cyber Criminology*, Vol. 2, no. 2, pp. 368–381.

ADLER, F., LAUFER, S., W., MUELLER, G., 2001. *Criminology* . 4th Ed. Macgraw- Hill, New York.

ADOGAME, A. 2009. 'The 419 code as Business Unusual: youth and the unfolding of the Advanced Fee Fraud online Discourse', *Asian Journal of Social Sciences,* Vol. 37. Pp 551-573.

ATTAFUAH, K. A. 2008. *Fighting Armed Robbery In Ghana*. Justice & Human Rights Institutes, Accra.

ASSIMENG, M. 2010. *Religion And Social Change in West Africa: An introduction to the Sociology of Religion.* 2nd Ed. Woeli Publishing, Accra.

BAZELON, DL, CHOI, YJ AND CONATY, JF, 2006. 'Computer Crimes', 43 *American Criminal Law Review,* pp 258- 264.

BECKER, H. S., 1998. *Tricks of the Trade: How to think about your research while doing it.* University of Chicago, Chicago.

BURDEN, K., PALMER, C. AND LYDE, B., 2003. 'Cyber-Crime: A New Breed of Criminals?' *Computer Law and Security Report*, Vol.19, no. 3.

CASEY, E. 2004. *Digital Evidence and Computer Crime*. Elsevier Press, St. Louis.

University of Ghana http://ugspace.ug.edu.gh

CAVANAGH, A. 2007. *SOCIOLOGY IN THE AGE OF THE INTERNET*. Macgraw Hill, Berkshire.

CHAWKI, M., 2009. 'Nigeria tackles Advance Fee Fraud'. *Journal of Information, Law & Technology*. Vol.1.

CHUA, HUANG C.E., WAREHAM J., ROBEY D., 2007. 'The role of online trading communities in managing Internet auction Fraud'. *MIS Quarterly* Vol. 31, No. 4, pp. 759-781.

COLLIERS, D. 2004, 'Criminal Law and the Internet' in Buys, R, (ed.). *Cyberlaw @ SA.*, (2nd Ed.), Van Schaik Publishers, Pretoria.

COOPER D. R. & SCHINDLER P. S., 2003. *Business Research Methods*. 8th ed. McGraw-Hill, New York.

COMAROFF, J. & COMAROFF, J., 1999. 'Occult Economics and the violence of Abstraction: Notes from the South African Postcolony'. *American Ethnologist* Vol. 26, No. 2, pp. 279- 303.

ENTORF, H. & SPENGLER, H., 1998. 'Socio-economic and demographic factors of crime in Germany: Evidence from panel data of the German States'. http://econstor.eu/bitstream/10419/24268/1/dp1698.pdf. Accessed May 22nd, 2009

EIDE, E., Aasness,J., Skjerpen, T., 1994. *Economics of Crime: Deterrence and the Rational Offender*. Elsevier Science B.V., Amsterdam.

FABRY, J. M. COL., 1999. 'Cybercrime, Cyberterrorism and Network Warfare: The Next generation of concern for users of Networked Information systerms'. *Annual Review of Institute for Information Studies*. Pp.161- 184.

University of Ghana http://ugspace.ug.edu.gh

GOODMAN, M., 2001. ' Making Computer Crime Count'. *Annual Editions. Criminal Justice 03/04*, 27th ed. pp 28- 33. McGraw-Hill, Dushkin.

GLICKMAN, H., 2005. 'The Nigerian '419' Advance Fee cams: Prank or Peril'. *Canadian Journal of African studies.* Vol. 39. Nos. 3. Pp 460- 489.

GORDON, B., 2000. 'Internet Criminal Law' in Buys, R. (ed.) . *Cyberlaw @ SA: The law of the Internet in South Africa.* Van Schaik, Pretoria.

GORDON, S. & FORD, R. 2006. 'On the definition and classification of cybercrime'. *J Comput Virol.* Vol. 2, Pp. 13-20.

HARALAMBOS, M., HOLBORN, M., HEALD, R., 2004. *Sociology: Themes and perspectives.* 6th ed. HarperCollins. London.

HANSEN, B., 2002. 'Cyber crimes: should penalties be tougher?'. *Annual Editions. Criminal Justice* 03/04, 27th ed. pp. 19- 27. McGraw-Hill, Connecticut.

HAKIM, C., 1987. *Research Design: Strategies and Choices in the Design of Social Research.* Allen & Unwin, London.

Internet Crime Complaint Center (IC3) Annual Report, 2001- 2008. http://www.ic3.gov/crimeschemes. Accessed March 27th , 2010.

Jaishanker, K., 2007. ' Establishing a Theory of Cyber crimes'. *International Journal of cyber criminology, Vol. 1, No. 2: pp. 7-9.*

JOSEPH, J., 2003. 'Cyberstalking: An international perspective' In Y. Jewkes (ed.) *Dot.cons: Crime, deviance and identity on the internet.* . Willan Press, Cullompton.

University of Ghana http://ugspace.ug.edu.gh

JUA, N., 2003. 'Differential Responses To Disappearing Transitional Pathways: Redefining Possibility among Cameroonian Youths'. *African Studies Review*, Vol. 46, No. 2: pp. 13-36.

Kimmel, M., & Aronson, A., 2009. *Sociology Now*. Allyn & Bacon, Boston.

KSHETRI, N., 2006. 'The simple economics of cybercrimes, security & privacy magazine'. *IEEE Computer Society*, vol.4, No. 1, pp 33- 39. http://doi.ieeecomputersociety.org/10.1109/MSP.2006.27 Accessed May 22nd, 2009.

KRISTINA, C., MARSHINI ,C., CHRISTOPHER, L. FRANK, R., DANIKA, K., SEYMOUR , E. G., 2008. 'Cybersecurity in Africa: An Assessment'. Georgia Institute of Technology, Atlanta

KUMEKPOR, T., 2002. *Research Methods & Techniques of Social Research*. Sonlife Press & Services, Accra.

LAMB, A. & JOHNSON, L. 2006. 'Want to be my friend? What you need to know about Social Technologies'. *Teacher Librarian,* Vol. 34, No. 1, pp. 55-57.

LEINER, B., CERF, V., CLARK, D., KAHN, R., KLEINROCK, L., LYNCH, D., POSTEL, J., ROBERTS, L. & WOLFF, S., 2003. 'A brief history of the Internet'. *Internet Society*. http://www.isoc.org/internet/history/brief.shtml. Accessed October 24th , 2009.

MCCAGHEY, C. H., 1980. *Crime in American Society*. Macmillan, New York.

MCINTYRE, L. J., 2005. *Need to know: Social science research methods*. Mcgraw -Hill, New York

MERTON, R., 1938. 'Social Structure And Anomie'. *American Sociological Review*, Vol. 3: pp 672- 682.

University of Ghana http://ugspace.ug.edu.gh

MEYER, B., 1995. 'Delivered from the powers of darkness': Confessions of satanic riches in Christian Ghana. *Journal of international African Institute*. Vol. 65, no. 2: Pp 236- 255. Edinburgh University Press. Accessed October 22nd, 2009.

NEUMAN, W. L., 2007. *Basics of Social Research: Qualitative And Quantitative Approaches*. 2nd Ed. Allyn And Bacon. Boston.

NINALOWO, A., 2004. *Essays on the State and Civil Society*. First Academic, Lagos

OLOWU, D., 2009. 'Cyber-Crimes and the Boundaries of Domestic Legal Responses: Case for an Inclusionary Framework for Africa', *Journal of Information, Law & Technology*, vol. 1 http: //go.warwick.ac.uk/jilt/2009 1/olowu Accessed October 10th, 2009.

OLUSI, F. I., AGUELE, L.I., IHUMUAIBVI, P. O., & EDOBOR, R. I., 2009. ' Students Perception of Cyber Crime in Edo State: Implications for Teaching and Learning',. *LWATI: A Journal of Contemporary Research* Vol . 6, No.1. Accessed March 26th , 2010.

RIBADU, N., 2007. 'Cyber-crime and Commercial Fraud: A Nigerian Perspective', presented at the Congress Celebrating the Fortieth Annual Session of the UNCITRAL, Vienna, Austria.

RITZER , G., 1996. *Modern Sociological Theory*. 4th Ed. Macgraw- Hill. New York

SERIOUS FRAUD OFFICE GHANA, 2007 Annual Report.

SERIOUS FRAUD OFFICE GHANA, 2008 In- House training Manuals

University of Ghana http://ugspace.ug.edu.gh

SLATER, D., & KWAMI, J., 2005. 'Embeddedness and Escape: Internet and mobile use as poverty reduction strategies in Ghana'. Working Paper. Information Society Research Group.

SMITH, J.S., 2001. 'Ritual killing, 419, and Fast Wealth: Inequality and the Popular Imagination in southeastern Nigeria'. *American Ethnologist*, Vol. 28, No. 4: pp. 803-826. http://www.jstor.org/stable/3094936 Accessed June 3rd, 2009.

SNAIL, S., 2009. 'Cyber Crime in South Africa – Hacking, cracking, and other unlawful online activities', *Journal of Information, Law & Technology (JILT)*, Vol. 1

SNYDER, F., 2001. 'Sites of Criminality And Sites of Governance'. *Social & Legal Studies Vol. 10*: pp 251–256.

SUTHERLAND. E., 1978. *Criminology*. 10th ed. Lippincott, Philadelphia

SYKES, M. G. & MATZA, D., 1957. 'Techniques of Neutralization: A Theory of Delinquency'. *American Sociological Review*, Vol. 22, No. 6 (Dec., 1957), Pp. 664-670. http://www.jstor.org/stable/2089195 Accessed June 17th, 2010.

TETTEY W. J., 2006. 'Globalization, Cybersexuality among Ghanaian Youth, and Moral Panic'. In Joseph Mensah (ed.) *Neoliberalism and Globalization in Africa: Contestations on the Embattled Continent.* New York: Palgrave Macmillan, pp. 157-176.

TETTEY W. J., 2008. 'Globalization and Internet Fraud in Ghana: Interrogating the Political Economy, Survival, Subaltern agency and their Ramifications'. In Joseph Mensah (ed.) *Neoliberalism and Globalization in Africa: Contestations on the Embattled Continent.* New York: Palgrave Macmillan, pp 241-255

University of Ghana http://ugspace.ug.edu.gh

TIVE, C., 2006. '419 Scam: Exploits of the Nigerian Con Man'. iUniverse, Bloomington.

United Nations,2007. Ghana Country Report.

United Nations Office of Drugs & Crime Report, 2002. Crime and Development in Africa.

MERWE, A., V., & Snail, S., 2008. 'A Brief Excursus on the South African Online Alternative Dispute Resolution'. *Journal of Information, Law & Technology*, vol. 2. http://go.warcick.ac.uk/jilt/2008 2/ merweandsnail Accessed October 10th, 2009.

WALSH, A., & ELLIS, L., 2007. *Criminology: An inter-disciplinary Approach*. Sage Publications. California.

WALL, D., 2001. ' Cybercrimes and the Internet.', in D. Wall (ed.) *Crime and the Internet*. Routledge, London.

YAR, M., 2005. 'The Novelty of 'Cyber Crime''. *European Journal of Criminology*. Vol. 2, No. 4: pp 407–427

http://www.ghanadistricts.com/districts/ Accessed May 20th, 2010.

http://www.ghanabusinessnews.com/2009/02/17/cyber-crime-giving-a-bad-name-to-ghana/

http://bbc.co.uk/2/hi/africa Accessed October 25th, 2009.

Accra Metro Profile 2009, www.ghanadistrict.com Accessed May 24th, 2010.

University of Ghana http://ugspace.ug.edu.gh

NEWSPAPER ARTICLES AND MAGAZINES

Christian Messenger vol. 23, nos. 2, May 29th- June 10th, 2009:1

Daily Graphic 26th May, 2009:16

Daily Graphic 13th May, 2009:1

Ghanaian Times 6th May, 2009

The Business Eye: Nigeria's Investigative Business Journal. 29th June – 5th July, 2009 .Vol. 3, 26th Ed.

The Mirror 18th July, 2009:27

University of Ghana http://ugspace.ug.edu.gh

Appendix i

Ranking	Top ten cyber crime perpetrator Countries. (Beginning with the highest ranked) Statistics are from the 2007- 2009 Annual IC3 reports		
	2007	**2008**	**2009**
No. 1	United states of America	United States of America	United states of America
No. 2	United Kingdom	United Kingdom	United Kingdom
No. 3	Nigeria	Nigeria	Nigeria
No. 4	Canada	Canada	Canada
No. 5	Romania	China	Malaysia
No. 6	Italy	South Africa	**Ghana**
No. 7	Spain	**Ghana**	South Africa
No. 8	South Africa	Spain	Spain
No. 9	Russia	Italy	Cameroon
No. 10	**Ghana**	Romania	Armenia

University of Ghana http://ugspace.ug.edu.gh

Appendix ii. Western Union control sheets

These control sheets represent monies received for two separate gold scam deals.

WESTERN UNION

(1)

MTCN:

Date & time: (EST) 18/08/2010

Agent: Agricultural Develop Bank

GLOBAL ACCESS

Operator ID: 123

Amount received: 9,163.25

Tax: 0.00

TOTAL: 9,163.25 Ghana Cedi

Originating country: UNITED ARAB EMIRATE DUBAI1

Exchange rate: .3830789

Amount sent: 23,920.00 UAE Dirham

Telephone:

DIA KING NO.19

OTA

A

Passport

ber:

ration date: 16052015

DER:

uestion: DUBAI

er: DUBAI

AIN TERMS AND CONDITIONS GOVERNING THE MONEY TRANSFER SERVICE YOU HAVE SELECTED ARE SET ON THE BACK OF THIS M. BY SIGNING THIS FORM, YOU ARE AGREEING TO THOSE TERMS AND CONDITIONS. IN ADDITION TO THE TRANSFER FEE, STERN UNION AND ITS AGENTS ALSO MAKE MONEY FROM THE EXCHANGE OF CURRENCIES. *PLEASE SEE IMPORTANT INFORMATION ARDING CURRENCY EXCHANGE SET FORTH ON THE BACK OF THIS FORM. UNLESS YOU HAVE CHOSEN TO BE PAID A CURRENCY FFERENT FROM THE ONE DESIGNATED BY YOUR SENDER, THE CURRENCY TO BE PAID AND THE EXCHANGE RATE FOR YOUR NSACTION ARE TYPICALLY DETERMINED AT THE TIME THE TRANSACTION WAS SENT.

tomer signature:

Agent Signature:

Customer Signature:

Date:

Agent Signature:

Customer Name (please print):

Date :

WESTERN UNION

To Receive Money

(2)

Ecobank
The Pan African Bank

CEIVER:

MTCN:

dress:

ST LEGON

Telephone:

Date & Time: (EST) 08/17/2010 5:15:00 AM

Agent: Ecobank Ghana Ltd

Operator ID: 723

ORA

Passport

number:

xpiration date: 25012014

Amount received: 7,047.68

Tax: 0.00

TOTAL: 7,047.68 Ghana Cedi

Originating country: UNITED ARAB EMIRATE/SHARJAHED1

Exchange rate: .3830260

Amount sent: 18,400.00 UAE Dirham

ENDER:

al question: DUBAI

swer: DUBAI

ERTAIN TERMS AND CONDITIONS GOVERNING THE MONEY TRANSFER SERVICE YOU HAVE SELECTED ARE SET ON THE BACK OF THIS ORM. BY SIGNING THIS FORM, YOU ARE AGREEING TO THOSE TERMS AND CONDITIONS. IN ADDITION TO THE TRANSFER FEE, ESTERN UNION AND ITS AGENTS ALSO MAKE MONEY FROM THE EXCHANGE OF CURRENCIES. *PLEASE SEE IMPORTANT INFORMATIO EGARDING CURRENCY EXCHANGE SET FORTH ON THE BACK OF THIS FORM. UNLESS YOU HAVE CHOSEN TO BE PAID A CURRENCY FFERENT FROM THE ONE DESIGNATED BY YOUR SENDER, THE CURRENCY TO BE PAID AND THE EXCHANGE RATE FOR YOUR RANSACTION ARE TYPICALLY DETERMINED AT THE TIME THE TRANSACTION WAS SENT.

University of Ghana http://ugspace.ug.edu.gh

INTERVIEW GUIDE (Youth Respondents)

My name is Belinda Smith, a graduate student of the University of Ghana. I am undertaking a research for my thesis as part of the requirements for my MPHIL in Sociology. The research aims to gain deeper insight into the 'sakawa world' primarily for those engaged in it. It may be termed as attempting to separate the facts from fiction. I humbly request you grant me an interview. Your participation is very important towards the success of this research. As the topic under research is quite sensitive, please be rest assured that the interview will be treated confidentially, your identity will be protected and none of the information you will give will be passed on to a third party as the information will be used purely and only for the purpose of this research.

1. Socio Economic Demographic Information

(The questions in this section attempt to elicit information as to the socioeconomic background of respondents and so will give us an insight into 'who' our respondents are)

Age of respondent

Ethnicity

Religion

Highest educational qualification

Occupation

Brief family background

Educational background of parents

Number of siblings

University of Ghana http://ugspace.ug.edu.gh

Here respondent will be probed into disclosing a brief back ground of growing up. Details of location and environment would be needed.

Did you grow up in a monogamous or polygamous setting or nuclear/ extended family setting?

What were your career aspirations growing up?

Have you achieved any of your aspirations?

If yes, which one/s

If no, why?

Do you have any personal perception of a successful person?

Probe further:

- If tied to material wealth such as nos. of cars, string of girlfriends, wives how did they arrive at this perception? Is it from watching members of family, celebrities,
- Do you have any role model? Who? Why is this person your role Model?

2. To identify the different various cyber fraud types and how they are engaged in

(these questions are aimed at uncovering the 'what' regarding sakawa)

- What is sakawa
- What does the word sakawa mean?

Do you know what language it is derived from?

- Are there different types of sakawa?
- If yes, please state the various types you know of
- How did you get involved in the business?
- Do you have any fears regarding the activity?
- How do you differentiate between cyber crime and sakawa?
- If you had to physically interact with your client, would you still indulge in your business?

University of Ghana http://ugspace.ug.edu.gh

- Do you think your family is aware of your indulgence?
- What do they think?
- Do you use the internet for any other activity apart from cyber business?
- How often do you attract/gain potential clients?

3. **Examining reasons and motivations. (These questions target the 'whys' of respondent indulgence)**
   - What motivates you to engage in this cyber business? Probe for whether the following account for*** deterrence, ease of learning, spiritual dimension, the lack of violence***
   - What do your peers think about it?
   - What are your perceptions of the legal consequences?
   - Has that perception any consequences on indulgence?
   - Can you justify reasons for indulgence?
   - Do you think you can still engage your client if you had to do it face to face?
   - Do you engage in any occult activities?

   Probe further on the occult dimension.

4. **Determining challenges**
   - What are your challenges?
   - What have been your Material (probe further: cars, savings, house) and emotive (probe further respect, success, wealth, independence, magnet for the opposite sex) gains.
   - Is this the only way you feel you could have gained it/them?
   - Are you remorseful?
   - How do you think the society perceives sakawa activities
   - What are your challenges?
   - Do you see it as any other job?
   - What are your future plans?

Do you belong to any youth organization/club/association?

How do you think the youth in Ghana are perceived?

University of Ghana http://ugspace.ug.edu.gh

INTERVIEW SCHEDULE (SFO)

My name is Belinda Smith, a graduate student of the University of Ghana. I am undertaking a research for my thesis as part of the requirements for my MPHIL in Sociology. The research aims to gain deeper insight into cyber crime which is popularly referred to as 'sakawa '. I humbly request you grant me an interview. Your participation is very important towards the success of this research. The primary aim for this interview is to gain an understanding of the responses and actions of the Serious Fraud Office towards cyber crime. Any information garnered will be used purely and only for the purpose of this research. I thank you for granting me time to conduct the interview.

1. When was the Serious Fraud Office (SFO) established in Ghana?
2. Why was the SFO established as there was already the Ghana Police Force?
3. What is cyber crime?
4. What is *Sakawa*?
5. Are Cyber crime and *sakawa* the same phenomenon?
6. Does the SFO have a working definition for cybercrime?
7. If a Ghanaian defrauds a foreigner, does the SFO come in to investigate that case?
8. Are there any laws addressing cyber crime in Ghana?
9. What is your opinion on what constitutes *Sakawa*?

University of Ghana http://ugspace.ug.edu.gh

10. Do you have any idea what age group and gender indulges the most in cyber crime?

11. What in your opinion is the motivation for cyber crime or sakawa?

12. What are your views on the "juju" dimension of sakawa?

13. What proactive measures are being employed by security agencies to tackle the problem?

14. Are SFO officers trained to recognize and apprehend those involved in cyber crime activities?

15. Does the SFO work in collaboration with other state law enforcement agencies?

16. What can be done to curb this crime?

University of Ghana http://ugspace.ug.edu.gh

INTERVIEW SCHEDULE (Police)

My name is Belinda Smith, a graduate student of the University of Ghana. I am undertaking a research for my thesis as part of the requirements for my MPHIL in Sociology. The research aims to gain deeper insight into cyber fraud which is popularly referred to as 'sakawa '. I humbly request that you grant me an interview. Your participation is very important towards the success of this research. The primary aim for this interview is to gain an understanding of the responses and actions of the Ghana Police Service towards cyber crimes. Any information garnered will be used purely and only for the purpose of this research. I thank you for granting me time to conduct the interview.

1. What unit of the police service handles cyber crime?
2. Is the Ghana Police Force the only body mandated to deal with this phenomenon?
3. What is cyber crime?
4. What is Sakawa?
5. Are Cyber crime and sakawa the same phenomenon?
6. Does Ghana Police Service have a working definition for sakawa?
7. Are cyber crimes/ sakawa treated differently from traditional crimes?
8. Are there any laws addressing cyber crime in Ghana?
9. What is your opinion on what constitutes sakawa?
10. Do you have any idea what age group and gender indulges the most in cyber crime?
11. What in your opinion is the motivation for cyber crime or sakawa?
12. What are your views on the "juju" dimension of sakawa?

University of Ghana http://ugspace.ug.edu.gh

13. What proactive measures are being employed by security agencies to tackle the problem?

14. Is sakawa confined to any particular locality?

15. Does the Police have current statistics on cyber crime trends?

16. Does Ghana police force work in collaboration with other state law enforcement agencies?

17. What can be done to curb this crime?