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

DEPARTMENT OF SOCIOLOGY

UNIVERSITY OF GHANA

CYBERCRIME IN GHANA: A STUDY OF OFFENDERS, VICTIMS AND THE LAW

BY

DANIEL ENNIN

10279395

THIS THESIS IS SUBMITTED TO THE UNIVERSITY OF GHANA, LEGON IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE AWARD OF MPHIL SOCIOLOGY DEGREE

JULY, 2015

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

DECLARATION

I hereby declare that this thesis is my own work and that to the best of my knowledge, it has not been previously published by another person for the award of any degree at any university, and all the materials used from other sources are duly acknowledged.

…… ……

DANIEL ENNIN **DATE**

(STUDENT)

…… ……

PROFESSOR CHRIS ABOTCHIE **DATE**

(SUPERVISOR)

…… ……

DR. DAN-BRIGHT S. DZORGBO **DATE**

(CO-SUPERVISOR)

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

DEDICATION

This thesis is dedicated to my late brother, Deputy Superintendent of Police (DSP)/ Mr. Bismark Addae for making me who I am today. *May your soul rest in peace.*

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

ACKNOWLEDGEMENT

Thanks to the Lord of hosts for making all things possible and with whom this thesis has seen the light of the day.

I am most grateful to Professor Chris Abotchie and Dr. Dan-Bright S. Dzorbgo whose commitment, constructive criticisms, and suggestions have fine-tuned the outcome of the research.

My next appreciation goes to the personnel of the Ghana Police Service for the insightful information shared with me.

I further wish to extend my deepest gratitude to the "Circuit Court 8" Judge of the Cocoa Affairs Court Directorate in Accra, Miss Patricia Quansah for educating me on Act 772, despite her busy schedules.

I want to render my profound gratitude also to my immediate officer, Superintendent of Police (Supol)/ Mr. J. B. Pokoo-Aikins for his words of encouragement when things were tough. Not forgetting my bosom friend, Sgt. Alhasan Faisal Baba for holding the fort when I am not around. Special thanks to my darling wife, Bernice, for her prayers and support in times of despair.

Last, but not least, to all those who assisted in diverse ways towards the completion of this work, but whose names I could not mention, God richly bless you all.

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

ABSTRACT

The Information and Communication Technology (ICT) has become essential to the operations of government, corporate institutions and individuals, but the benefits accruing from the growing access is being undermined by miscreants who are exploiting its capabilities to the detriment of others. This has tainted Ghana's reputation in the global environment. The main thrust of this study was therefore to explore the dynamics of cybercrime activities from the perspectives of offenders, victims and the law. The objectives that guide the research are; 1) to understand the socioeconomic characteristics of offenders and the victims, 2) identify the motivation that predispose the offenders to cybercrime, 3) establish the various forms of cybercriminal activities in Ghana, 4) to find out the opportunities explored by the fraudsters in their operations, 5) explore the experiences of the cybercrime victims, and 6) to examine the responses and challenges of law enforcement agencies to fight cybercrime.

The research was situated within the Accra metropolis. The study was largely qualitative but the research design enabled the researcher to combine both quantitative and qualitative strategies to collate data from the field. Snowball and purposive sampling methods were used to reach out 26 respondents. They included 11 internet scammers, 6 victims, 8 key informants from the Criminal Investigation Department of the Ghana Police Service and a Circuit Court judge. All the participants took part in the qualitative study. With regards to the questionnaire, 17 out of the 26 respondents participated and they were made up of victims and the offenders.

The findings of the study revealed that cybercrime perpetrators were mostly young men between 17 to 30 years with an average age of 23. The majority of the scammers were from economically deprived homes. With regards to the victims, they are adults who are highly educated and well-to-do in the society. A number of the victims heeded to the scammers request without due diligence. The results of the study further show that a poor legal regime encouraged the youth to indulge in cybercrime. Besides, the Act 772 that supposed to regulate the criminal behaviors in the electronic space is also inadequate to fight the menace in terms of criminalization, evidence and trial of offences. Moreover, the Ghana Police Service lacks the technical know-how and the state-of–the-art equipment to monitor internet fraud. The characteristics of cybercriminals, victims and law enforcement agencies have a reinforcing effect on one another, leading to a vicious cycle of

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

cybercrime. Inability of the police to solve cybercrimes has eroded victims' confidence in the criminal justice system, and this has increased criminals' confidence to continue their operations. This outcome was consistent with the Routine Activity theory which presupposes that crime can occur when there is no adequate police patrols, effective laws which motivated the offender to commit the crime.

The major recommendations that have been outlined to fight the menace are: 1) formulation of appropriate laws to curb cybercrime; 2) government should organize capacity building for law enforcers to enable them abreast with internet fraud issues; 3) government should further establish appropriate facilities to fight the menace; 4) public education should be intensified about the modus operandi of internet scammers; 5) youth focused programmes should be initiated to address youth-unemployment. Finally, further study areas were suggested.

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

TABLE OF CONTENTS

Content **Page**

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

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

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

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

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

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

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

LIST OF TABLES

INTEGRI PROCEDAMUS

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

LIST OF DIAGRAMS

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

LIST OF FIGURES

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

LIST OF ABBREVIATIONS AND ACRONYMS

ANSFNET	:	America National Science Foundation Network
ARPANET	:	Advanced Research Projects Agency Network
C/Supol	:	Chief Superintendent of Police
CCU	:	Commercial Crime Unit
CEOP	:	Child Exploitation and Online Protection
CERT	:	Computer Emergency Response Team
CID	:	Criminal Investigation Department
DVS	:	Documentation and Visa Fraud Section
FBI	:	Federal Bureau of Investigation
IC3	:	Internet Crime Compliant Centre
ICT	:	Information and Communication Technology
INTERPOL	:	International Criminal Police Organization
IP	:	Internet Protocol
ITU	:	International Communication Union
IU	:	Intelligent Unit
JANET	:	Joint Academic Network
LPU	:	Legal and Prosecution Unit
NGOs	:	Non-Governmental Organizations
NW3C	:	The National White Collar Crime Centre
PMMC	:	Precious Mineral Market Company
RCCF	:	Resource Centre for Cyber Forensics
SITU	:	The Statistics and Information Technology Unit
SOCA	:	Serious and Organize Crime Agency
UNOCD	:	United Nations Office on Drugs and Crime
VPN	:	Virtual Private Network

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

CHAPTER ONE

OVERVIEW OF THE STUDY

1.0 Introduction

In the last quarter of the twentieth century, a technological revolution centered on information has transformed the way we think, produce, consume, trade, communicate, and even how we make love (Castells, 2000). The availability of information technology around the world are linking up valuable people and activities while switching off from a conventional networks of power and wealth. To a large extent, cyberspace is the manifestation of postmodern society whereby novel technologies have created new social environment and a new reality. We are now living in an era of simulations, where humans are constantly "substituting signs of the real for the real" (Baudrillard, 1995). The line between reality and unreality is blurred, and in the postmodern world, it is difficult to tell the real from those things that simulate the real (Ritzer, 1996). Bauman (2000) also coined the term "Liquid Modernity" to describe the fragmented nature of contemporary life, and society's inability to provide the stable environment to serve as a frame of reference. Liquid life is where nothing is fixed; everything changes very quickly when we are still learning how to cope with the situation, meanwhile the reality has changed. Individual achievement cannot solidify into lasting possession because conditions of actions designed to respond to them age quickly and become obsolete. Extrapolating past events to solve current or predicting future trends become more risky and often misleading because the strategies might not support the technological advancement.

Statistics available at the Ministry of Communications indicate that there are six mobile phone companies in Ghana. Namely; MTN, Vodafone, Tigo, Airtel, Glo and Expresso.

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

Besides, there are 29 million mobile phones subscribers and 13 million internet users in the country *(Daily Graphic, 14/11/2014, page 32*[1]*).*

Daily Graphic, further reported that globally, there are about 4.5 billion mobile phone users, while more than two billion users of smart devices, and 2.9 billion Internet users who send more than seven billion e-mails a day. Additionally, there are about 3.5 billion Google searches, 2.1 billion Facebook interactions, as well as 500 million twits a day. The United Nations Office on Drug and Crime (UNODC) 2013, further projected that by the year 2017, mobile broadband subscriptions will approach 70 percent of the world's total population and in 2020, the number of networked devices (the "internet of things") will outnumber people by six to one, transforming current conceptions of the internet. Today, electronic society has become perhaps some of the most critical issues for almost all governments across the globe because the survival of their economies now revolves on the dynamics of information and communication technology.

However, it is crucial to bear in mind that despite this phenomenal growth, access to the Internet remains highly uneven both between countries, regions, and within individual nations. The technical capacity enabling internet access (PCs, software, reliable telecommunications grids) is unfairly distributed. For example, more than 70 percent of households in Europe have internet access, while the comparable figure for Africa is less than 6 percent (ITU, 2012). Similarly, while Europe boasts 200 broadband internet connections for every 1,000 people, in Africa there is only one such connection per 1,000 (ITU, 2009:5). Unequal access also follows existing lines of social exclusion within individual countries where factors such as unemployment, income and education are

[1] A speech delivered by the Deputy Minister of Communications on 13th November, 2014.

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

reflected in the patterns of internet use (Bartlett & Miller 2011). These inequalities are criminologically important, as they tell us something about the likely social characteristics of both cybercriminals and their potential victims.

The computer technology has become a ubiquitous component in modern life. It allows us to perform task that our fore-fathers could not do. The president of United States, Barrack Obama posited;

> *More than any other invention of our time, the Internet has unlock possibilities we could just barely imagine a generation ago, (http://www.whitehouse.gov/net-neutrality)*

Individuals regularly utilize their laptops, desktops, tablet computers, smart phones to engage in all facets of life, from communications to finance (Smith, 2011). Social networking sites like Facebook, WhatsApp, Viber, Tango and Twitter allow us to stay in touch with our friends and family to share and exchange ideas around the world, while streaming media services entertain individuals 24 hours a day on demand. On-line retail generates billions of dollars in income every year, and most consumers now utilize electronic banking services to manage their accounts and pay bills (Anderson, 2010). In fact, government and industry now depend on the internet and computers to maintain sensitive records and provide real-time information to consumers and citizens about any issue that may be of interest.

The establishment of cyberspace has also collapsed the constraints of space and time that limit interaction in the real world. Borrowing from the sociological accounts of globalization as 'time-space' compression (Harvey, 1990), theorist of the internet suggest that cyberspace makes possible instantaneous encounters between spatially distant actors and these create possibilities for ever-new forms of association and exchange. In the same

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

vein, Castells (2000) elaborated how the collapsing of time and space affects the global business. For instance, in his concept of 'timeless time' he argued that the internet has unified the global capital market. The same capital is shuttled back and forth between economies in a matter of hours, minutes as a results of powerful computer financial analysis software. Therefore, Jones (1993) espoused that individuals sitting at the global nodes of telecommunications network are generating billions of dollars every day in the stock market. The qualitative change in the human experience has affected the industrial paradigm of increasing subcontracting and offshore production business in the global environment, (Aronowitz & Di Fizio, 1994). It is characterized by the technological and organizational ability to separate the production process in different locations while reintegrating its unity through telecommunication linkages, and micro-electronics based precision and flexibility in order to cut down cost and maximized profit.

However, in as much as computers and the internet have facilitated communication, society is witnessing a new form of criminal behavior called cybercrime. While there is no commonly agreed definition of the concept, it generally refers to any criminal act dealing with computers and internet. It is regarded "international" or "transitional" crime since there are no cyber-borders between countries (Thomas & Loader, 2000). Duggal (2015), a cyber law expert defined the cybercrime as "any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further traditional crimes". Cybercrime can be classified into three broad categories: a) crime against individuals (that is the person or his/her property); b) crime against organization (such as companies, corporations, or government establishment); and, c) crime against society at large.

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

In Ghana, the term "sakawa" has been used to describe cybercrime and it has become one of the criminal acts committed mostly by the youth and at times schoolchildren who leave the classroom for internet cafés in order to be involved in the act (The Ghanaian Times, 04/06/2012 :8). This affects academic progress as those involved fail to attend school for a considerable period of time. The perpetrators engage their partners (victims) in a persuasive dialogue over a period of time, falsify documents, and create a situation that convince victims to either transfer money or make available their credit card details to them (The Ghanaian Times, 04/06/2012:8).

1.1 Problem Statement

The role of ICT in an emerging economy like Ghana has been widely recognized at various levels. The recognition is reflected in actions such as the development and deployment of national ICT infrastructures, institutional and regulatory framework for managing the sector. In addition, the promotion by the use of ICT in all sectors of the economy, implementing e-governance in government institutions, the construction of National Data Centre, and the Laptop per child policy indicate that Ghanaians have embraced the knowledge-based society.

The impact of these developments on the economic and social transformation of Ghana seems to have been positive. The contribution of ICT to the Gross Domestic Product increased from 2.3 percent in 2009 to 10.5 percent in 2011 and the industry created 3,500 additional jobs in 2011 compared to 3,050 in 2010 (National Development Planning Commission, 2011).

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

Notwithstanding the success Ghana has chalked in ICT, it is a common knowledge that the spread of cybercrime is on the ascendency. The news that Ghana ranks seventh in cyber fraud, out of ten countries identified in the world and second in Africa is alarming, (Daily Graphic, 15/04/13, Page 7). Cyber fraud ranges from hacking of official websites to abduction and soliciting by young Ghanaian girls for sexual gains abroad. What is more distressing about the growing incidence of cybercrime was the fact that a lot of young people are among the perpetrators of these criminal activities, (Daily Graphic, 30/01/13, page 32). They spend hours browsing and sometimes stay awake all night to carry out their nefarious activities. The menace has occasioned financial losses to many individuals and organization most of which are usually unreported. The internet connectivity, for instance, makes it easier for criminals to operate beyond national boundaries.

This development has impacted negatively on Ghana's image in the global environment. Many companies in the western world have blacklisted credit card transactions coming from the country. To buttress this point, Kwablah (2009) revealed that Ghana was the second most frequently blocked location by U.S e-commerce sites because retailers are skeptical of fake orders from internet scammers. Such negative blows to our credibility cement the difficulty Ghanaians businessmen/businesswomen face in attempts to penetrate the western market with our local products. It's also causing foreign investors to be wary of conducting business in the country and in the end it affects the financial inflows that government could generate to maintain the balance of payment deficit in the fiscal year.

Looking at the pervasive nature of the phenomenon and its socio-economic and political dimensions, concerns have been raised by civil societies, NGOs and opinion leaders

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

urging government to deal decisively with the upsurge of cybercrime in the country. This has increased media reportage and some of the caption reads as follows:

"Government to develop cyber security strategy for the country" (*Daily Graphic 30th January, 2013:32),* **"Government urged to finance cybercrime combat"** (*Daily Graphic 28th January, 2014:32),* **"Government Sets Up Data Processing Commission to protect personal Records"** (*Daily Graphic 14th November, 2014:32*), **"CID equips investigators to fight cybercrime"** (*The Ghanaian Times, 22nd April, 2013:3).*

These media publications stress the point that cybercrime is a relatively new crime that is growing progressively within the borders of Ghana. But before any policy against cybercrime could be effectively implemented, there is a need for further research and understanding of the phenomenon. The study thus, attempted to explore the dynamics of cybercrime activities in the country with particular reference to those who engage in it, their victims and the reaction of the law.

In this regard, the key research questions the study seeks to answer are:

1. What are the socioeconomic backgrounds of offenders and the victims?
2. How do the victims and the offenders come together?
3. What are their gains and the losses (victims & offenders)
4. What motivated the scammers to perpetuate cybercrime?
5. How do the victims get lured into cybercrime activities?
6. How does the law reacting to redress offenders and the victims?

1.2 Study's Aim and Objectives

The aim of the study is to explore the characteristics of the offenders and victims as well as the existing law in order to gain an in-depth knowledge on cybercrime activities in Ghana. The study's objectives are to:

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

1. Understand the socioeconomic characteristics of the offenders and the victims
2. Identify the motivation that predispose the offenders to this crime
3. Establish the various forms of cybercriminal activities in Ghana
4. Find out the opportunities explored by the fraudsters in their operations
5. Explore the live experiences of the cybercrime victims
6. Examine the responses and challenges of law enforcement agencies to fight cybercrime

1.3 Significance of the Study

Technological revolution has created another society for mankind but cyber fraud continues to demoralize its credentials. Those engaged in the act adopted various strategies to deceit innocent people. The study hoped to provide the readers an understanding of what cybercrime is and raises awareness about the various trends of cybercrime situation in Ghana.

Significantly, the results of this study would serve as a reference material for government, security agencies and other stakeholders in the policy formulation, and mapping out strategies to address the problem. Given that there is little research on internet scams, the study adds to the body of knowledge on cybercrimes in which further studies could be carried by other researchers to broaden the scope.

1.4 The Scope and Limitations

The research primarily focuses on the use of internet in perpetuating crimes in Ghana and its implication for the country's image in the global environment. Unfortunately, the research is a mix method with considerable amount of in-depth qualitative techniques, so

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

the study could not be expanded to cover large respondents across the regions of Ghana. This challenge was compounded by time and resource constraints. For that reason, the study was limited to the Accra Metropolis. The city is frequently mentioned in the news media report of having high rate of cybercrime occurrence.

1.5 Definition of Key Concepts

To enable an effective interpretation and understanding of the findings of this study, the following key terms/phrases have been operationally defined in the context of the study.

Cyberspace- the realm of computerized interactions and exchanges

Cybercrime- For the purposes of the study, cybercrime means using the ICT as a medium to defraud people which is popularly referred to as "Sakawa" in Ghana.

Offender- A person who has committed fraud using the internet or cyberspace as a conduit for the purposes of seeking financial reward.

Victim- An individual who has been defrauded financially through the internet

Substantive law- an existing law that deals with cybercrime

Procedural law- the process of trying an accused cybercriminal in court

1.6 Organization of the Study

The study is organized into five chapters. Chapter One constitutes the general overview of the study; covering the background of the study, problem statement, questions guiding the study, aim and objectives, significance of the study, scope and limitations, and definition of key concepts.

Chapter Two covers the review of related literature, and the conceptual framework used in explaining the subject matter.

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

Chapter Three addresses the research methods which include: research design, study area, sampling techniques, sample size, sources of data collection, research instruments, data analysis, ethical considerations, and the problems encountered on the field.

Chapter Four focuses on data presentation and discussion of findings from the interviews conducted and the questionnaire administered.

Chapter Five provides a summary, conclusions, and policy implications to the cybercrime issues in the country.

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

CHAPTER TWO

LITERATURE REVIEW AND CONCEPTUAL FRAMEWORK

2.0 Introduction

This chapter reviewed information relating to cybercrime from various sources; including textbooks, accredited on-line journals, magazines, dissertations, newspapers, organizational reports and other relevant documents. According to Neuman (2003), literature review is based on the assumption that knowledge accumulates and that people learn from and build upon what others have done. Bryman (2008), also explained that reviewing the related studies gives an overview of what has been said, who the key writers are, what are the prevailing themes, question being asked and the methods appropriate for the study. It may provide a critical assessment of the issue in a particular field, stating where the weakness and gaps are, contrasting the views of a particular author, raising question, and providing a summary that evaluate and shows the relationship between different materials.

In view of these, the following subheadings were considered: brief history of cybercrime and internet, definitions of cybercrime, facets of cybercrime, the global trend, Africa standpoint on the issue, and some selected countries were highlighted on their efforts towards cybercrime. Cybercrime in Ghana and the legislative approach, a review of some contemporary and classical theories to understand the dynamics about the phenomenon.

2.1 Cybercrime in Perspective

According to Aidoo et al (2012), cases of computer crimes globally, date back to the early 1960s when the first case of computer crime was reported. Since then, there have been countless reports of computer crimes being committed on a daily basis (Kabay, 2008).

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

These early attackers often used unauthorized access of telecommunications systems to subvert long-distance phone system which modified or destroyed data for financial gain, revenge, amusement or theft of services. Additionally, programmes in the 1980s began with a malicious software, including self-replicating programs which interfere with personal computers. The illegitimate application of e-mails also grew rapidly from the mid-1990s onward, generating torrents of unsolicited commercial and fraudulent activities (Rollins & Wyler, 2013). The evolvement of software applications have created complex problem for information security in the contemporary world.

2.1.1 A Brief History of Internet

The origins of the Internet can be traced to the development of a network, the Advanced Research Projects Agency Network (ARPANET), sponsored by the US military in the 1960s (Yar, 2013). The aim was to establish a means by which the secure and resilient communication and coordination of military activities could be made possible. In the political and strategic context of the 'Cold War', with the ever present threat of nuclear confrontations, such a network was seen as a way to ensure that critical communications could be sustained, even if particular points within the computer infrastructure were damaged in an attacked. The ARPANET's technology would allow communications to be broken up into packets that could then be sent through a different range of routers to their destination, where they could be reassembled into their original form (Snyder, 2001). Even if some of the intermediate points within the network failed, they could simply be bypassed in favor of an alternate route by ensuring that messages reached their intended recipients. The creation of the network entailed the development not only of the appropriate computer hardware, but also of 'protocols,' the codes and rules that would allow different computers to 'understand' each other. This development got under way in

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

the late 1960s, and by 1969, ARPANET was up and running, initially linking together a handful of university research communities with government agencies.

From the early 1970s, further innovations appeared, such as electronic mail applications, which expanded the possibilities for communication. Other networks paralleling the ARPANET, were established such as the UK's JANET (Joint Academic Network) and the American National Science Foundation Network (NSFNET), Abbate (1999). By using common communication protocols, these networks could be connected together, forming an inter-net, "a network of networks" (Castells, 2000). A major impetus for the emergence of the Internet was given when, in 1990, the US authorities released the ARPANET to civilian control, under the auspices of the National Science Foundation. The same year, 1990, saw the development of a web browser (basically an information-sharing application) by researchers at the CERN physics laboratory in Switzerland (Ling, 2004). Dubbed the 'world wide web' (www), this software was subsequently elaborated by other programmers, allowing more sophisticated forms of information exchange such as the sharing of images as well as text.

The first commercial browser, Netscape, was launched in 1994, with Microsoft launching its own Internet Explorer the following year. These browsers made Internet access possible for personal computers (PCs). In the mid-1990s, numerous commercial service providers entered the market, offering connection to the Internet for anyone with computer and access to a conventional telephone line (Ling & Haddon, 2001). These connection services, while popular, were slow and offered a very limited capacity for transmitting data. They have since been supplanted by much faster 'broadband' connections as well as services offering data connections to mobile devices such as phones. Since the

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

commercialization of the Internet in the mid-1990s, its growth has been incredibly rapid. Between 1994 and 1999 the number of countries connected to the internet increased from 83 to 197 (Furnell, 2002:7).

2.1.2 Definitions of Cybercrime

The basic problem for the analysis of cybercrime is the lack of a consistent and statutory definition for the activities that constitute cybercrime (Yar, 2005). According to Smith et al. (2004), defining cybercrime raises conceptual complexities and varied information. In addition to the difficulty of definition, it is also called by variety of terms such as computer crime, computer-related crime, digital crime, information technology crime, internet crime and virtual crime. Cybercrime could reasonably include a wide range of criminal activities and it would appear that scholars, writers and law enforcement agencies are more comfortable with describing various elements constituting cybercrime than defining it (Olayemi, 2014).

At the 10th United Nations Congress on the Prevention of Crime and Treatment of Offenders in 2005, a workshop devoted to the issues of crime related to computer networks divided cybercrime into two categories,

- Cybercrime in a narrow sense is any illegal behavior directed by means of electronic operations that targets the security of computers systems and the data processed by them.
- Cybercrime in a broader sense, is any illegal behavior committed by means of, or in relation to, a computer system, or network, including an illegal possession or distributing information by means of a computer network

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

The United States Department of Justice[2] (2009), in an attempt to define cybercrime summaries the definition in three-stage classification:

First, crimes in which the computer or computer network is the target of the criminal activity. For example, hacking, malware and Dos attack.

Second, an offence where the computer is a tool used to commit the crime. For example child pornography, stalking, criminal copyright violations and fraud.

Third, crimes in which the use of the computer is an incidental aspect of the execution of the crime but may help generate evidence of the crime. For example, addresses found on the computer of a murder suspect as well as phone records of conversations between an offender and a victim before a homicide. In such cases the computer is not significantly implicated in the commission of the offence, but is more of a repository for evidence.

The Council of Europe's Convention (CoE) on cybercrime was created in 2001 to address the jurisdictional issues posed by the evolution of the internet (Weber, 2003). Its solution was to harmonize cybercrime laws and assure the existing procedural mechanisms to assist in the successful prosecution of cybercriminals across member States.

The Convention classified cyber offenses into four categories:

a) Offenses against the confidentiality, integrity, and availability of computer data and system such as illegal access, illegal interception, data or system interference, and illegal devices. "Confidentiality[3]" refers to the protection of information from disclosure to unauthorized parties, while "integrity[4]" refers to the protection of information content. "Availability[5]" means the information should be available to

[2] U.S Department of Justice, National Institute of Justice, *Prosecuting Computer Crimes* (Office of Legal Education 2009). Available at http://www.ncjrs.gov/profiles1/nij/219941.pdf.
[3] This explanation was provided by CoE Report to the Convention on Cybercrime No. 275. Available on: www.oas.org/juridico/english/cyb_pry_explanatory.pdf
[4] Ibid. no. 281
[5] Ibid. no. 290

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

authorize parties when requested. This is mentioned in Article 2 to 6 of the Convention;

b) Computer related offenses which include computer related forgery and fraud are captured in Articles 7 and 8;

c) Content-related offenses: the Article 9 tries to strengthen and modernize the existing law provisions against sexual exploitation of children in an electronic transmission, that is an illicit acts related to child pornography.

d) Offences related to the infringement of copy rights captured in Article 10 of the Convention.

Suman et al (2014:334) defined cybercrime as "unlawful acts wherein the computer is either a tool or a target or both". It means that on one hand, a computer may be the object of the crime when there is theft of computer hardware, or software. Also a computer may be the subject of a crime when it is used as an instrument to commit conventional crimes such as fraud, theft, extortion, or new types of criminal activity such as denial of services attacks and malware, identity theft, child pornography, copyright infringement and mail fraud. Snail (2009:2), further explains that;

> cybercrime 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, sniffing and the production and dissemination of viruses, and crimes that have been in existence for centuries but now committed within the cyber environment such as fraud, possession and distribution of pornographic materials.

Van der Merwe (2008:61) also gives cybercrime a contemporary outlook. According to him, computer crimes "represents a novelty type of criminal activity which started appearing during the nineties as the use of the internet became common place worldwide".

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

Drawing from the foregoing definitions, it is significant to note that there is no consistent and statutory definition for cybercrime, and it is simply committed with the aid of a computer connected to the internet. This creates a 'save heavens' for the perpetrators because the speed, convenience and anonymity that modern technology offers provide diverse range of criminal activities which make it difficult for the security agencies to track. However, in the context of this study, the Council of Europe (CoE) Conventional definition of cybercrime is adopted to explain the internet fraud in terms of confidentiality, integrity and availability of online information. Though it is useful to discussion the CoE Convention on cybercrime in a more detail, this chapter is limited to discuss Article 2 to 10 of the convention. Thus, appendix (ix) presents detail discussion of the articles.

2.1.3 Facets of cybercrime

The 2013 Internet Crime Compliant Centre (IC3) Annual Report published in 2014 highlighted the various types of cybercrimes mostly complained of by the victims. These are Internet auction fraud, credit card fraud, bogus business opportunities, identity theft, hacking, phishing and pharming, and Nigerian 419 scam. Some of these crimes are expatiated in the sections that follow:

a) Credit Card Schemes

Credit card fraud is one of the biggest challenge to business establishments in the 21st century. It occurred when the person uses another individual's credit card for personal reason while the owner of the card is not aware that the card is being used, Schmalleger and Pittaro (2009). The authors further explained that credit card fraud are committed through an act of deception, illegal used of people's account for personal gain, and misrepresentation of account information to obtain goods or service. According to the

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

Eurobarometer[6] survey conducted in 2013 which covered more than 27000 people in all member States revealed that 76% agreed the risk of becoming credit card/banking online fraud victim has increased over the years. This destructive impact hampers the digital economy and many people may not take full advantage of all the possibilities internet brings to individuals in the postmodern world.

b) Identity Theft

Identity theft begins when someone takes your personally identifiable information such as your name, social security number, date of birth, and residential or office address without your knowledge for personal financial gain (Schmalleger & Pittaro, 2009). There are different types of schemes in which identity criminals' use. These ranged from technical and social engineering strategies. The social engineering occurs when someone is either in person, over the telephone or computer, uses means to deceive someone else to divulge sensitive information. Usually, the social engineer knows some information about the person and that pushes the victim to believe that the person is genuine. In the same vein, criminals who are ICT incline can also scam the internet and re-rout people's electronic mail accounts without their consent.

c) General Merchandise and Auctions Fraud

According to IC3 Annual Report of 2013, auction fraud involves the misrepresentation of a product advertised for sale through the internet. In an attempt to make the deal appear legitimate, the criminal often instructs victim to send full or partial payment to a third-party agent via wire transfer and to fax their payment receipt to the seller as proof of

[6] European Commission Press Release (2013). Online threats: survey shows impact of cybercrime. Available at Europa.eu/rapid/press-release_IP-13-1130_en.htm

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

payment. Once payment is made, the criminal pockets the money and the victim receives an item that is less valuable than he/she promised or worse, receives nothing at all.

d) Cyber Pornography and Obscenity

These are activities that breach the laws on obscenity and decency. Sexually, explicit images and video are accessible online and constitute a multibillion dollar industry (Edelman, 2009). Though these materials may not be illegal, the internet has also fostered the growth of a wide range of communities supportive of deviant sexual behaviors (DiMarco, 2003). Online spaces enable individuals to find others who share their interests, creating supportive communities where individuals can be part of the group and later validate their practices. For example, the customers of prostitutes regularly use technology to communicate with others who share their interests and solicit illicit sexual services in the real world (Holt & Blevin, 2007). The internet has also become a popular venue for sexual predators and other sex related offences, (Olayemi, 2014).

e) Phishing and Pharming

The explosive growth of online fraud has made 'phishing', and to a lesser extent 'pharming' part of nearly every Internet user's vocabulary in most recent time (Olowu, 2009). Phishing and pharming are two popular forms of fraud that aim at luring victims to believe that they are at a trusted web site such as their bank, when in fact they have been enticed to a bogus web site with the intent to steal their identity and drain their financial resources (Adeniran, 2008). Every day millions of e-mails are sent around the globe, millions of web pages are accessed to gather information, and millions of people use online sites to transact business. We strive to trust the systems that are in place to deliver our e-mail messages and to route us to the proper web server. Unfortunately, a growing

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

cyber-thieves are using this same system to manipulate us and steal our private information; they take advantage of people's being trusting the system.

f) Advance Fee Fraud

This scam is purported to originate from Nigeria, which requires victim to pay a series of fees to process transaction that supposedly enables the victim claim large sum of money. These fees would usually cover duty, stamp and form charges (Cukier et al, 2007). Warner (2011: 742) further explained that the "419 schemes", known in pre-internet incarnation as "advanced-fee fraud began after the collapse of World oil prices during the 1990s which left the Nigeria oil-dependent economy shriveled. The increasingly educated and yet unemployed youth began to garner infamy for its culture of deception by posting pen pals to deceive people to make a living. Adogame (2009) accentuates that the internet and email technology have changed the "face, pace and fate of advanced fees fraud. Cybercrime has created an image nightmare for Nigerian. When one comes across the phrase 'advance fee fraud', the assumption that comes to one's mind is that all scam emails originate from Nigeria. Accordingly, Chawki (2009) explained that Nigerian ISPs and the entire Internet networks were black-listed by some multinational companies. To that effect, the country experienced annual global loss of $1.5 billion in the year 2007.

g) Hacking

Defined broadly, hackers are individuals with a profound interest in computers and technology who utilize their knowledge to access computer systems for malicious or unethical purposes (Holt, 2007). Though hackers engage in and develop cyber security tools, individuals view hacking in its malicious context because of the economic and personal harm (Furnell, 2002). In fact, malicious hacking is often tied to the creation and

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

distribution of pirated software's that can automate attack against computer system (Chu et al., 2010). These programs can disrupt e-mail operations, and at times damaged private files in the computer.

h) Cyber-Terrorism

Olayemi (2014) espouses that the acts of cyber-terrorism is causing psychological harm to, or inciting physical harm against others, thereby breaking the laws pertaining to the protection of the person such as hate speech and the distribution of injurious materials online. Perhaps the simplest description is that ideological concerns rather than economic or political considerations motivate the attack which intends to cause grave harm. For instance, on December 22, 2014, the US security officials accused North Korea security agencies of exposing tens of thousands of sensitive documents from Sony Company Website. In response, the U.S imposed economic sanctions against several North Korean government agencies in retaliation for the country's role of hacking into "Sony Pictures" and threating U.S moviegoers (www.myjoyonline.com). Again, on 30th June, 2015 hackers broke into the U.S government computers and they compromised the personal data of 4 million federal employees. The U.S investigation had named China as chief suspect. In response, China had denied any involvement, and called U.S claim as irresponsible (www.citifmonline.com).

i) Botnet

A defining feature of today's cybercrime landscape is the extensive use of computer tool across a wide range of cyber-offences. Botnets consists of network of interconnected, remote-controlled computers, generally infected with malicious software (UNODC, 2013:32). The legitimate owner of such system may often be unaware of the fact of

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

infection. These enable cyber criminals to send spam email or take part in a distributed denial of service attack (DDos). Such infected computers are often called “robot” or “bot” computers. When several computers are affected with a category of malware, they can be simultaneously controlled from a single command servers system (CSS) to perpetuate crime.

2.1.4 Legal Classification of Cybercrime

The fluid nature of cybercrime has led to a great body of research on the various offenses that fall under this term. One of the well-referenced and constructed framework to understand cybercrimes from the legal perspective is Wall’s (2001) four established categories:

1. *Cyber-Trespass*- this involves crossing boundaries into other people’s property and causing damage, that is hacking, defacement and its related offences.
2. *Cyber-deceptions and theft*- This type of cybercrime involves stealing, (money, and property). That is generating credit card fraud, intellectual property violence, piracy etc.
3. *Cyber –Pornography*- These are activities that breach the laws on obscenity and decency
4. *Cyber-Violence*- This involves causing psychological harm to, or inciting physical harm against others, thereby breaking the laws pertaining to the protection of the person such as hate speech.

The first two categories comprise ‘crimes against property’, the third covers ‘crimes against morality’, and the fourth relates to ‘crimes against individuals or the state; those activities that breach the laws protecting the integrity of the nation and its infrastructure.

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

For example, terrorism, espionage and disclosure of official secrets. Such classification allows legal expert to prescribe an appropriate sanctions to the internet fraudsters.

2.2 Cybercrime- The Global Trend

Information and Communication Technologies (ICT) have become important tools in today's knowledge-based information society and economy. As a result, governments and commercial organizations increasingly rely on Internet-worked information systems to carry out services that are critical to administrative and business successes (Daily Graphic, 15/04/13, Page 7).

The UNODC (2013) Annual Report projected that, it will become hard to ignore a computer crime and perhaps any crime, which does not involve electronic evidence in the near future. To buttress the internet crime, the International Telecommunications Union (ITU, 2014) concluded that;

> The global annual loss due to cybercrime was estimated between 375 and 575 billion United State dollars. The price variation is due to the difference methodology member states adopted to calculate the losses. The report further suggested that Germany is the most affected country by cybercrime with an estimated loss equivalent to 1.6% of the DGP, followed by U.S 0.64% of the GDP, Brazil 0.32% of the GDP and Kenya, 0.10 per cent (ITU 2014:15).

The wider reach of the internet has facilitated the transmission of information at a relatively cheaper rate and inadvertently expose the entire world to a 'highly criminogenic' environment (Chu et al, 2007). It means that crimes in cyber space brings together offenders and victims situated in different countries and continent, so it has become an international problem.

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

To tackle the trend of this emerging crime, the United State of America in the year 2000 set up an Internet Crime Complaint Centre (IC3) which is a partnership between the National White Collar Crime Centre (NW3C) and the Federal Bureau of Investigation (FBI) to combat the menace. This security organization is to serve as a conduit for gathering and disseminating information on internet related criminal offences.

In every year, the IC3 generates global statistics on cybercrime through the information received from the individuals who have been duped on the internet. Intelligence analysis are deduced from the report for the yearly comparison of cases and also to educate victims about the dynamics of internet fraud worldwide. The Figure 1 depicts yearly compilation of complaints captured in IC3 (2013) report.

Figure 1. IC3 Complaints by Year

Figure 1 expounds the distribution of cybercrime cases from 2000 to 2013. In 2009, the IC3 received the highest reported cases totaling 336, 655 across the globe. In 2013, the IC3 received 262,813 consumer complaints with adjusted dollar loss of $781,841,611,

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

which was 48.8 percent increase in reported losses of $581,441,110 between 2011 and 2012 (IC3 2013 Annual Report, page 3). The report further indicated that the US and UK have higher percentages (0.09%) of cybercrime victims respectively, while Nigeria leading the global chart of internet scammers with an average percentage of 0.97. Hence, the data try to portray that irrespective of geographical location and economic viability of a country, cybercrime activities can still take place.

2.3 A Snapshot of Cases captured in IC3 2013 Annual Report

Cybercriminals have been victimizing people by offering rewards, cash, business deals and baiting advertisement. The IC3 (2013) reported that a genre of these socio-engineering scams emerged internationally, and are believed to originate mostly from the West Africa coast. The perpetrators defamed the reputation of some international enterprises and email accounts of their officials to obtain personal information from internet users. Sometimes they call people from illegal telephone exchanges. In response, some victims' remitted money to these scammers. The following is an overview of basic techniques perpetrators use to make emails look legitimate as captured by IC3 to exemplify the diversity and the scope of the fraud.

2.3.1 Case 1- Criminal's Defamed the Reputation of DHL Courier Services (Report: 25 April, 2013, IC3 Compliant: 11304290514210121)

DHL is a renowned courier services company which takes care of global dispatch, delivery of parcel and express shipments. The organization helps to connect people and improve their lives through commerce and social networks. Scammers use this brand of trapping internet users. The conversation which follows is a malicious email sent by fraudster claiming to be originated from the DHL delivery service.

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

We the management of DHL Courier Service hereby uses this medium to notify you that the parcel is still in our possession. This parcel contained an international Cashier Bank Draft/Cheque worth the sum of $800,000 and it is ready for delivery to your doorstep. Meanwhile, before the delivery or shipment will take place, you are advice to reconfirm to us the following data mention below:
1. Your name 2. Full address 3. Age 4. Sex 5. Telephone. The above requested information will enable us deliver your parcel correctly without any mistake or delivering your parcel to a wrong person. Note: No charges should be made before delivery except the stamp duty fees which is just $75. Delivery would be made to your doorstep as soon as we receive your mail. Best regard, Mr. Mohmo Benson DHL Courier Service Managing Director. Email: mohnobenson@admin.in.th

Scammers pay special attention to the content of the email. After all, if the message looks suspicious, a potential victim would be likely to delete it. For instance, the narrative revealed that the fraudster is holding a position of trust in the DHL Company. The amount involves is also quite attractive which can bait the victim to respond.

2.3.2 Case 2- Scammer Defamed Nokia Corporation of £500,000

(Report: 29 April 2013, IC3 Compliant: 11304290717025121)

Nokia Corporation is one of the world largest producing cell phones. The company adopted 'easy to reach' marketing strategies such as low cost or promotions to increase their customer base (Kumar et al, 2010). However, scammers circulate false messages on the internet to indicate that the receiver had a promotional package being run by Nokia. The excerpt of the technique utilized by the criminals is highlighted from the IC3 report.

Either you or someone you know entered your information on our web Address for the 2013 Nokia Cash Splash promo and we are using this medium to officially notify you that the result of the promo was recently released as shown below:Mohamedd.hzmsa@shell.com £900,000.00 Confidential Unclaimed; bows.sm1091@bluewin.ch 200,000.00 GBP Confidential Unclaimed. We are happy to inform you that you are our second prize winner and you won 500,000 GBP (five hundred thousand Great British Pounds) at this promo. Your ticket number is NOK92677TF. Please take note of your number as it will be needed for verification. To receive your money, winners are expected to reply this email with the following information for verification. 1. Your full name 2. Residential address 3. Mobile number 4. Email address 5. Ticket number. Copy your international passport or driver license. Your payment will be issued to you when we receive your reply with your information as outlined above. Please bear it in mind that you won big in this promo because you are one of our valuable customers. However, if you wish to decline the receipt of your prize money, you are to notify us on time so that the opportunity will be given to another Nokia phone user. Warning: because

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

*of numerous fraudulent schemes going around the internet, confidentiality should be accorded at all times. You are expected to keep the news of your winning and your ticket number to yourself until you have received your prize money. This is to avoid false claims and abuse of the program. Nokia corporate will never ask you to pay any fee before you receive your prize. You can call *44-708-646-5692 if you wish to speak to someone from our office. Please inform us as soon as you receive your money congratulations! Timo Ihamuotila Chief Financial Officer Nokia Corporation-UK*

From the scenario, the fraudster represented himself as the agent of Nokia Company. The next step was to persuade the potential victim to provide identifiable information and also not to divulge such information to the third party. It is likely that people who have not subscribed to any promotional reward may response to the call but as a wise saying 'all that glitters is not gold'.

2.3.3 Case 3- Criminal defamed Africa Development Bank with Illegal money Proposal of $5.5 million (Report: 29 April 2013, IC3 Complaint: 11304241115394441)

The overreaching objective of the Africa Development Bank (AfFB) is to spur sustainable economic development and social progress in its regional member States, thus contributing to poverty reduction. The strategic location of AfDB connects Africa commerce to other parts of the world. As a result, the Bank has an enviable reputation from international and multinational agencies but the sad news is that some miscreants use it as conduit of swindling innocent victims. The IC3 (2013) highlighted this crime technique.

Hello, compliment of the day to you. I am Mr. Gabriel Compaore a banker by profession from Africa Development Bank (AfDB) here in West Africa and am currently holding the post of bill and exchange manager of the Bank. I am sending this brief letter to solicit your partnership to transfer $5.5 million US Dollars into your bank account. Bear in mind that I contacted you because the deceased customer was a foreigner and only another foreigner like you can successfully claim out this money. It is this regard that I decided to contact you with the confidence and hope that I must be safe and protected in your hands since what is involved is such a huge amount of money in million dollars. However, I shall text you the application form as soon as I hear from you. Can you be able and capable

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

to assist me by providing me with your receiving bank account where this fund lodge in your favor? I shall give you 40% of the total sum as soon as this fund hit your account I shall visit you in your country for the sharing. Please this is very confidential. Please forward me the below information; your name: your country: your phone number: your tel/fax; your age: your occupation: a copy of your photo. I am looking forward for your prompt response. I shall text you the application form when I receive a positive response from you. Best regard

Technological revolution has created a new social world and various authors who write on cybercrime have alluded to the fact that there is a correlation between the concept of globalization and cybercrime. Brenner (2010) argues that crimes carried out by cyber criminals often reflect the emotion of persons in society. She further mentioned greed, obsession, and drive for profit are the reasons why many internet crimes are committed. Also the amazing fact about cybercrime is the realization that many victims may be at a distance or a world away from each other.

One can deduced from the cases that have been discussed, that the scope of techniques adopted by criminals varied. Personal information was common denominator perpetrators asking for. The information creates a field day for identity thieves, hackers to study the behavioral profile of the person which is then use for exploitation such as sending spam ware, virus, and botnet to infect computers. The narratives further revealed that cyber offenders lack fluency in the use of English, lexis and the general syntax of the sentences in their email messages.

2.4 Cybercrime in Africa

Cybercrime indeed constitutes a worldwide problem and no State is beyond vulnerability. However, to understand why cyber criminality in Africa differs from other areas in the world, one should understand the state of information security in this region which is

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

affected by factors such as the growth of user base, poor security awareness, lack of training for law enforcement, inadequate regulations and weak cross-border collaboration (Olowu, 2009).

The IC3 2012 annual report ranked Africa as the third highest continent regarding cyber fraud mostly because of inadequate action and control mechanisms to protect computers and networks. Nigeria was ranked as the most internet fraudulent country in Africa. Other top cybercrime destinations in Africa were Egypt, South Africa, Kenya, Ghana, Zambia and Cameroon. The subsection trying to discuss some regulatory and technological measures outlined by Nigeria and South Africa to contain cybercrimes. They are recognized globally as a hub for cybercriminals.

(a) The current legislative efforts on Cybercrime in Nigeria

The country has an unenviable image in cyberspace due to the activities of cyberdeviants generally referred to as "yahoo boy" or "419". Nigeria ranks third among cybercrime committing countries in the world ranking as reported by the IC3 2013 Annual Report. Responding to the global quest to fight cybercrime, the Nigeria government in 2006 passed the Advanced Fee Fraud and Related Offences Act[7] to prescribe, among others, ways to combat cyber fraud. The general provision of the Act prohibits obtaining property by false pretence, fraudulent invitation, laundering of fund obtained through unlawfully activity, conspiracy, abetment and aiding of crime. Section 2 makes it an offence to commit fraud by false representation. Section 3 makes it an offence if a person manage any premises, or knowingly permits the premises to be used for any online fraud,

[7] The Advanced Fee Fraud and Related Offences 2006 was enacted by the National Assembly of the Federal Republic of Nigeria and assented to it on 5th day of June, 2006

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

constitute an offence under this Act. The section further provides that the sentence for the offence is the imprisonment for a term of not more than 15 years and not less than 5 years without the option of a fine.

Section 4 refers to the case where a person who by false pretence, and with the intent to defraud any other person, invites or otherwise induces that person to visit Nigeria for the purpose connected with the commission of an offence under this Act, is liable for imprisonment term not more than 20 years and not less than seven years without the option of a fine.

The Act empowered the Nigeria Economic and Financial Crime Commission (EFCC) to carry out surveillance responsibilities to regulate industry players, cybercafé operators, among others (Adomi, 2007). What has been prescribed as due care measures by EFCC is that cybercafés operators should not accept anonymous internet users. Also cyber industry players should further use their system to keep record of all the transactions engaged by the users including their home address, telephone numbers, and emails address (*ibid*). It appears that the Nigeria effort to deal with the cybercrime are mostly contained in this Act but the multifaceted nature of the crime limits the effectiveness of the law. So Olyemi (2014), observed that there are several related bills on cybercrime before the Nigerian legislature and the National Assembly for various considerations to augment the Advanced Fee and Related Offences Act. Some of these bills are; the Cyber Security and Critical Infrastructure bill, the Electronic Commerce bill, Computer Security Protection bill, and the Evidence Act Amendment bill. Since these bills are yet to be passed into law, the safety of 'cyber citizens' (people in cyberspace) in Nigeria cannot be guaranteed.

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

(b) South Africa

South Africa is one of the advanced countries on the continent. Its advancement is spread across to all aspect of its development especially technological innovations. This has seen South Africa having to deal with a fast increase in cybercrime. The country passed the Electronic Communication and Transactions Act[8] (ECT), and assented to it on 31 July, 2002. The spirit of the Act is captured in the preamble which states;

> provide for the facilitation and regulation of electronic communications and transactions; for the development of a national e-strategy for the Republic; to promote universal access to communication and transactions and the use of electronic transactions; to provide for human resource development; to prevent abuse of information system; to encourage the use of e-government service; and to provide for matters connected therewith" (ECT 2002, Act 25, Preamble)

The legislation seeks to criminalize actions related to the illegal access and unauthorized modification of information as well as the possession and distribution of hardware devices and software programs that facilitate an offender's action of cybercrime. The ECT Act sufficiently deals with jurisdiction, the acceptability of data messages, the admissibility of electronic signature, as well as the regulation of cryptography (ECT, part 1, and 2 of the Act respectively). The South African law enforcers in fighting cybercrime have come out with cyber inspectors whose task are to monitor the internet activities and further ensure that the provisions of the ECT Act are complied with, (Chapter One of the Act, which covers Interpretation, Object and Application). Cybercrime prohibited under the ECT is stated under chapter XII (13) of the Act. These activities are grouped into four categories: those involving unlawful access to data, interception and interference with data, computer related extortion, and forgery.

The ECT which is the main law in South Africa in fighting against cybercrime has some specific provisions that specifically speaks to the issues of cyber activities prevalent in the

[8] Electronic Communication and Transactions Act 25 of 2002. Accessed on 4th October, 2015 from www. Up.ac.za/media/shared/409/Zp_Files/25-of-2002-electronic-communications-and-transactions-act_31-ma.zp44223.pdf.

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

world today. Section 86(1) of the ECT criminalizes all forms of hacking, while Section 88(1) of the Act also criminalizes any attempt by criminals to gain unauthorized access. The country in its attempt to fight cybercrime on the global scale has formed an alliance with the European Cybercrime Treaty which encourages members' states to make laws to fight the menace. Other laws such as the Electronic Communications Act[9], (Act 36 of 2005) and the State Information Technology Agency Act[10] (Act 88 of 1998) are used in South Africa to curb the cyber menace. In my view, the acts implemented by South Africans do not have the capacity to effectively dealt with the cyber menace. This is because the power of 'cyber inspectors' to search, seize or arrest are within the sovereign will of the State.

2.5 Cybercrime Legislation and Cooperative Alliances in the United States and United Kingdom

Despite the high rate of cybercrime victimization in the United State and United Kingdom according to the IC3 world report of 2013, they have been balancing this out through implementing regulatory and technologically advanced measures to arrest the menace. Having examined the anti-cybercrime legislative framework in Africa, the researcher took the opportunity to review these two countries efforts towards cybercrime combat. This enabled the researcher to do a geographically incline comparison.

(a) United States

Examining how cyberspace has affected conflict over the last decade, the former United States Defense Secretary, Robert Gates observed that "after wars have been fought on

[9] Electronic Communication Act 36 of 2005. Accessed on 4th October, 2015 from www.saflii.org/za/legis/consol_act/eca2005270.pdf
[10] State Information Agency Act 88 of 1998. Accessed on 4th October, 2015 from us-cdn.creamermedia.co.za/assets/articles/attachments/03397_stainftecageact88.pdf

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

lands, the 21st century should expect to fight current wars in the air and cyberspace" (cited in Murphy, 2010). The US, a highly developed technological state, has established legislative and cooperative frameworks to deal with many cybercrime issues. The former include:

The National Information Infrastructure Protection Act[11] of 1996, aimed at protecting individuals against various computer generated offences. Section 1030(a)(1) of the Act provides that "anyone who knowingly accesses a computer without authorization or exceed authorized access and obtains classified information with the intent or reason to believe that such information is to be used to disrupt the United States, or to the advantage of any foreign nation is subject to a fine or imprisonment for not more than ten years (for a first offense)". It means that a person who deliberately breaks into a computer for the purpose of obtaining classified or restricted information is subjected to criminal prosecution.

The Electronic Communications Privacy Act[12] (ECPA) of 1986 was passed by the United States Congress to implement and extend government restrictions regarding the use of wire taps on telephone calls and transmissions of electronic data by way of computer. The ECPA consists of three parts. The first outlaws the unauthorized interception of wire or oral electronic communications. It also establishes a judicial supervised procedure to permit interceptions for law enforcement purposes. The Second part focuses on the privacy of, and the government access to store electronic communications. The third

[11] The National Information Infrastructure Protection Act of 1996; Legislative Analysis by the Computer Crime and Intellectual Property Section of United States Department of Justice. Accessed on 7th December, 2015 from www.irational.org/APD/CCIPS/3010_anal.htm

[12] Electronic Communications Privacy Act of 1986 (ECPA) was enacted by the United States Congress to extend government restrictions on wire traps from telephone calls to include transmission of electronic data. Accessed on 7th December, 2015 from Congressional Research Centre/www.fas.org/spg/crs/misc/R41733.pdf

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

creates a procedure for pen-trap provisions that permit the tracing of electronic communication data by law enforcement representatives.

The Patriot Act[13] was introduced on October 23, 2001 to safeguard Homeland Security after the 9/11 attack. The law gave a new powers to the US Department of Justice, the National Security Agency and other federal agencies on domestic and international surveillance of electronic communications; it also removed legal barriers that had blocked law enforcement, intelligence and defense agencies from sharing information about potential terrorist threat. But the Patriot Act raised concerns among civil liberties groups and other critics surrounding the data privacy rights of US citizens. Concerns were heightened in 2013, when National Security Agency (NSA) contractor Edward Snowden leaked information showing that the agency was using the law to justify the bulk collection of data about millions of individuals' phone calls (Doyle, 2014).

The US further ratified the Council of Europe Convention on cybercrime in August 2006 and entered it into force on 1 January, 2007 which is not only deals with computer related crime, but also provides for mutual assistance to foreign police agencies in gathering and sharing electronic evidence with any kind of crime[14].

According to Cassim (2009), the US government has established many cybercrime agencies working in conjunction to protect the public and the critical infrastructure of the United States. They also provide information to individual's on how to protect oneself and one's family from cybercrime attack. These agencies include:

[13] The US Patriot Act of 2001 was signed into law on October 26, represents the US government's primary legislative response to terrorist attacks of September 11, 2001

[14] Bureau of national Affairs, Inc. (2006). Convention on Cybercrime. Reproduced with the permission from Privacy & Security Law Report, Vol. 5, No. 41 (1450-1454)/ available at www.bna.com

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

i) **Federal Bureau of Investigation (FBI):** the FBI local office in each States receives reports about the following cybercrime: computer intrusion (e.g. hacking), password trafficking, child pornography or exploitation, internet fraud and spam, internet harassment, internet bomb threats, trafficking in explosive or incendiary devices or firearms over the internet and intellectual property crimes.

ii) **The USA Secret Service**: the US Secret Service focuses mainly on large cybercrimes which could affect infrastructural and financial institutions in the United States such as counterfeiting currency and spam[15].

iii) **Internet Crime Complaint Centre (IC3):** the IC3 is a centre for receiving, developing and referring criminal complaints about cybercrime to the related authority at the federal, state and international level. The agency is a partnership between the FBI and the National White Collar Crime Centre (NW3C). The IC3 serves as a central reporting mechanism for complaints involving Internet related crimes.

iv) **Additionally,** The USA has entered into alliances with several governments and organizations through the efforts of US-Computer Emergency Response Team (CERT)[16]. The mission of the CERT is to provide the nation's cyber security stance, coordinate cyber information sharing, and positively manage cyber risk collaborations with other national CERTs.

[15] For more information visit www.secretservice.gov/ectf.shtml)
[16] Computer Crime & Intellectual Property Section (CCIPS) at US Department of Justice. Reporting Computer, Internet Related, or Intellectual Property Crime. Accessed on December 8th, 2015 from: http://www.usdoj.gov/criminal/cybercrime/reporting.htm.

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

(b) United Kingdom

The inadequacy of existing criminal law to address computer offences has led the UK government to enact various legislations to keep abreast with cybercrime activities. The legislations include the following:

The Computer Misuse Act of 1990, which was the first piece of UK legislation designed to specifically address computer abuse. The Act makes provisions for securing computer materials from the activities of hackers. For connection purposes, Section (1-3) of the Act has set out three computer misuse offences: namely, "unauthorized access to computer materials, unauthorized access with intent to commit or facilitate the commission of further offences and unauthorized modification of computer materials[17].

The UK also introduced the Privacy and Electronic Communications Regulations[18] (EC Directive) 2003, an Act which tries to address the problem of spam activities. According to the Act, Regulations 22(1) admonishes all companies seek for the permission of clients or an individual before sending emails or SMS messages to them. On the subject of emails, the law states that "a person shall neither transmit, nor prompt the business transaction of, unwanted communications for the purposes of direct marketing by means of electronic mail unless the recipient of the electronic has previously notified the sender that he consents for the time being to such communications being sent, or at the instigation of the sender".

Another cybercrime law adopted by the UK government is the European Convention on Cybercrime designed to provide a common international framework to deal with

[17] Computer Misuse Act 1990. Accessed on December 8th, 2015 from: http://www.legislation.gov.uk/ukpga/1990/18/pdfs/ukpga_19900018_en.pdf
[18] United Kingdom Privacy & Electronic Communications Regulations (EC Directive) Act, 2003. Accessed on December 7th, 2015 from: http://legislation.gov.uk/uksi/2003/2426/pdf/uksi_20032426_en.pdf

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

cybercrime which was introduced by the European Union Committee of Ministers of the Council of Europe in November, 2001.

The treaty is wide-ranged and covers all aspects of cybercrime, including illicit access, unlawful interception of data, data intrusion, system interference, abuse devices, computer-related sham, computer related fraud, crimes related to child pornography and offences related to violation of copyright and related rights. This treaty is also designed to provide a common law enforcement framework for dealing with cyber criminals and to foster the sharing of information among all signatories.

The UK government in its efforts to enforce these laws has set up Serious and Organized Crime Agency (SOCA). Its major task is to prevent organized crimes including offences committed through the use of internet. The Child Exploitation and Online Protection (CEOP) Centre is another initiative dedicated to eradicate the sexual abuse of children as part of the UK government policing to track offenders either directly or in partnership with local and international forces. It has liaised with law enforcement agencies in Australia, Canada, the US and INTERPOL to address legal jurisdiction on cybercrime.

Laws are ever-changing and are developed to address current issues facing governments or organizations. The development and the growth of computer crimes over the last decades has necessitated the US and UK governments to implement policies and programmes to counter cyber intrusion, terrorism and the violation of copyright laws. Even though these countries have not yet succeeded to contain the situation, other countries should draw a lessons from their relentless efforts, especially African States. Given the serious nature of cybercrime and its implication for the Africa investments, a common platform (law)

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

should be created like the Council of Europe Convention on cybercrime to raise awareness among internet users and also to fast tract the rendition of cyber offenders among member states to minimize the incidence of internet fraud.

2.6 Cybercrime in Ghana

Warner (2011) says cybercrime is a relatively new phenomenon in Ghana. Cyber-fraud increased in the country between the year 1999 and 2000. During this period, electronic based crimes were primarily related to credit card fraud, which was initially facilitated by bellhops at international hotels chains who would share Western visitors' credit card information with scammers. In these instances, Ghanaian scammers would steal the number of Western credit cards, purchase goods from the internet, and have them shipped to Ghana. Since 2004, credit card purchases over the internet has dropped with the emergence of new forms of internet fraud through the use of social engineering tactics to hypnotize the potential victims.

Burrell (2008) asserted that internet scamming/cybercrime in Ghana was an extension of a more benign practice which involve writing to foreign pen pals via postal system. In a research to gather internet scamming strategies associated with West African countries, she gathered that scamming in Ghana initially involved writing to foreign pen pals (boyfriends, girlfriend's relationships) via the postal system. Some of the young people who were involved in this practice valued these relationships basically as strategic affiliation for realizing material gain. Hence, the scam that occurred from the pen pals exchanges reflected how scammers drew on established patterns of communications to sculpting their operational tactics for economic benefit. This practice continued until it was replaced with the modern day internet scamming.

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

Over the past couple of years, cybercrime has received significant attention from the general populace and State anti-crime agencies in Ghana. This finds expression in the frequency of its mention in the media, pronouncements by government officials and non-governmental organizations. In view of this, the researcher gathered secondary data from the CID to find out whether Ghana Police Service is also receiving formal complaints from the citizens. The statistics which covered the period of 2006 to 2011 are presented in table 1.

Table 1: Cybercrime Review (2006-2011)

Cases reported	**Frequency**	**Percentage**
Cases refused	2	1.2
Cases sent to court	15	9.3
Cases convicted	12	7.5
Cases acquitted	1	0.6
Cases awaiting trial	2	1.2
Cases closed	1	0.6
Cases under investigation	128	79.5
Total	**161**	**100.00**

Source: Statistics & Information Technology Unit (SITU), CID Headquarters, Accra.

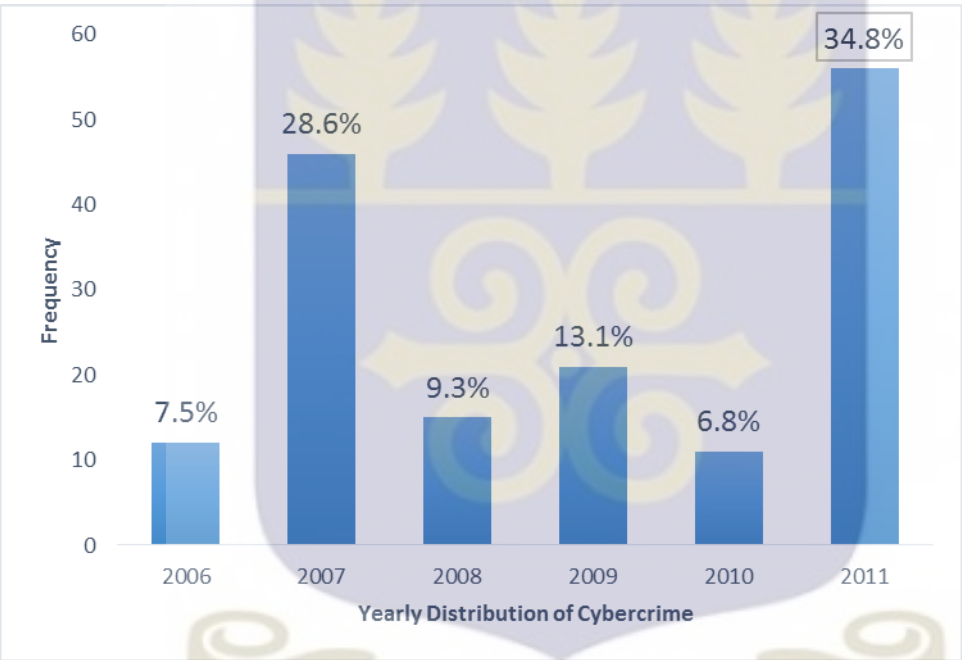
A total of 161 cases were recorded on cybercrime by the police across the country. Out of this number, 1.2% were cases police did not pursue for lack of adequate information or evidence. The data under review also shown that 9.3% cases have sent to court while 7.5% cybercriminals have been imprisoned. However, it is an interesting to note that 79.5% of the cases are still under investigation. This could point to the limitations on the investigative capacity of the CID personnel. The increasing use of technology by criminals, in areas like "Sakawa" and other computer assisted frauds means that some type

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

of crime can be committed with the degree of anonymity, sophistication and impunity because it poses a challenge for the police to track down the offenders.

In order to ascertain the patterns of cybercrime activities in Ghana, the investigator obtained the yearly distribution of the occurrence from 2006-2011, as presented in figure 2, below.

Figure 2. The Annual distribution of Cybercrime (2006-2011) in Ghana



Source: Statistics & Information Technology Unit (SITU), CID Headquarters, Accra.

The annual distribution of cybercrime (2006-2011) are depicted in figure 2. The modal years for internet fraud were 2007 and 2011. This could be attributed to the fact that Ghana Police Service step up public education about the menace and that may have motivated victims to report the crime or police vigilance led to the arrest of many suspects. However, police recorded lowest cases in 2006 and 2010. It could also meant that people

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

were not reporting cybercrime cases to avoid the frustrations of inconclusive police investigations.

2.6.1 Cyber-fraud Commonly Perpetrated in Ghana

Warner (2011), found out that there are three primary types of cyber-fraud commonly perpetrated in the country. The first of these is identity fraud. In this instance, Ghanaians will contact Westerners- often via social networking sites like Facebook or dating websites like Badoo.com or eHarmony.com and communicate under the guise of a false identity. This is the most common fraud in identity fraud known as "romance fraud". To buttress this point, Daily Graphic (03/10/13, page 71), reported that Police grabbed two persons for defrauding an America based Chinese businessman, John Moen, of $50,000. Yaw posed as a white lady on the internet and Moen allegedly expressed interest in marrying 'her'. The said amount, paid between June and September, 2013, was to facilitate the marriage arrangement. He came to Ghana and later realized that the wife-to-be, Helen Vorhanson never existed and that the whole idea was a scam.

Relying upon the same tactics of false identification; the second genre of cyber-fraud most frequently perpetrated in Ghana is that of fake gold dealers. Named the "Gold Coast" during its British occupancy, Ghana is well-known for its abundance of the ore. The cybercriminals advertise their fake gold samples on the internet. They offer competitive prices which are far below the World market price. According to Obiri-Yeboah (2013), the fraudsters generate fake licenses of Mineral Commission, Precious Mineral Market Company (PMMC), Geological Survey Department Certificates of ownership, Affidavit and other documents to convince their unsuspecting victims. In some instances, they are

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

able to lure their victims into the country and then show them samples of genuine gold. They then draft sale and purchase agreement to cover their transactions.

The third type of prevalent cybercrime in Ghana is that of estate fraud, whose victims are not typically Westerners, but instead, Ghanaians residing in the Diaspora. As it is common for Ghanaians living abroad to return to the country upon retiring, new enterprises have sprung up across the internet to cater for these wealthy Ghanaians' patrimonial real estate needs (Warner, 2011). Several cases have been reported wherein Ghanaians create fake construction firms that they advertise on the internet purportedly specializing in retirement housing for their compatriots returning to the country. Showcasing pictures of houses they supposedly built on the websites. Scammers sell the blueprints of such houses to would-be retiree. Thy also sell plots of land on which these houses will be built to the would-be retiree. Later, they send their clients receipts for building materials such as cement and tiles as proof of construction. After extracting much money from the distant clients, the 'company' collapses, the website is shut-down and the scammers disappear.

A speech delivered by the Inspector-General of Police, Mr. Mohammed Alhassan at the opening ceremony of a computer training for some selected police personnel at Tesano, Accra on Monday, 27th January 2014, observed that;

> The use of Information and Communication Technologies (ICT) in the developing world has undergone tremendous growth, bringing about a significant change in the way of life of people. 'What is worrisome is that the intended positive purpose of these technologies are sometimes turned into opportunities to facilitate the commission of complex crimes and criminalities, including 'sakawa' which has occasioned financial loss to so many individuals and organization most of which are usually unreported.

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

The internet connectivity, for instance, makes it much easier for criminals to act beyond national boundaries and this poses security operational deficiency and so victim's feels reluctant to lodge complaint at the Police Station.

The Vice Chancellor of the Valley View University, Professor Obour on his part reiterated that the challenges posed by modern technology have called for redemptive measures to keep the tempo of growing civilization. He wonder whether society is benefiting from the upsurge and sophisticated technology which brings with its numerous problem that call for huge financial resources to address (Daily Graphic, November 14, 2014: 32).

Duah (2013) delved into the growing threat of cybercrime and its implications for international relations. He observed that computer and the internet have presented a new way to engage in traditional crimes such as theft, fraud and piracy in the 21st century. These crimes due to the internet have become sophisticated with international dimensions. The study further revealed that the implication of cybercrime have been witnessed in areas such as economies of companies, governments, societal behavior, market values and the security of the nations. The researcher is calling for an international legal framework to prosecute cyber fraudsters irrespective of where the crime is committed. Even though the researcher is calling for international laws to deal with the menace, it would be more appropriate to gain an in-depth knowledge from the perpetrators and victims to raise awareness about the various trends of the phenomenon. This valuable information will inform policymakers on the need to regulate and implement extensive policies to help combat online-crime through global cooperation.

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

The media is often referred to as the mirror of society, reflecting events and issues that occur in society. Dugle (2013) examined the nature of coverage the press in Ghana gave to cybercrime issues through a content analysis of sampled editions of the Daily Graphic and the Daily Guide in 2011. The findings of the study revealed that cybercrime issues generally received low coverage due to the fact that the media landscape pay more attention to political nuances than the issues of national interest such as cybercrime. The results of the study also showed that even though the Daily Graphic published more stories on cybercrime than the Daily Guide, further examination of the five main categories (type, content, placement, source and author/writer of stories on cybercrime) indicate the two papers covered cybercrime in a similar fashion. Adequate press coverage of cybercrime issues can help minimize the practice and its effects on society. Such coverage can further provide education to the general public on the subject, and hence help citizens to take precautionary measures to protect themselves against the callous practices of internet frauds.

Quanson (2013) also examined the used of Information and Communication Technology (ICT) by the Commercial Crime Unit (CCU) of the Police Service to combat financial crime in Ghana. The study pointed out that CCU faced a lot of challenges in combating ICT-based financial crimes. Some of the major challenges highlighted by the researcher were lack of ICT trained personnel and how to use ICT to fight crimes, lack of genuine detection software, inadequate logistics to track cyber miscreants. However, the researcher failed to acknowledge other departments such as Documentation and Visa Fraud Unit, and the Intelligence Unit that complement the investigation and prosecution of online-financial crime activities.

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

Smith (2011) explored the motivations for the high prevalence of youth involvement in "Sakawa" conundrum in Ghana. The findings revealed that respondents were young men between 18 to 24 years, and they were also hailing from economically deprived homes. A large number of them were compelled to drop out of school due to economic difficulties in their families. With regards to the motivations for engaging in "Sakawa", the majority of the respondents explained that profitability, and identity flexibility were some of the motivating factors which accounted for their participation in cybercrime.

Looking at the pervasive nature of cybercrime, these few local studies mainly focused on the cybercriminals with less emphasis on the behaviors of victims and the efficacy of the existing laws to deal with the menace. This study is therefore aimed at filling the gaps in the literature by exploring the law, the views of victims and perpetrators in order to arrive at a comprehensive understanding of cybercrime in Ghana.

2.6.2 A Synopses of Media Reportage on Cybercrime Activities in Ghana

This section presents an overview of media reportage on cybercrime activities in Ghana. This gives us a sense of the occurrence of cybercrime.

(a) "3 Nigerians busted for stealing Gh¢3 million through ATM Fraud"
(Daily Graphic, Tuesday, December 16, 2014 edition, page 3)

Ghana has been described as a high currency circulation economy where greater volumes of transactions are done with cash. It has an adverse effect on the currency notes where people handling badly and often mutilated. In view of this, the Central Bank has to spend money to print new currency to replace the won out ones. This is costly exercise, and justifies the promotion and adoption of electronic banking practices by Bank of Ghana, thereby reducing the physical monetary economic transactions. Notwithstanding this

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

brilliant idea, criminals have generated cloned Automated Teller Machines (ATM) cards to withdraw money from individuals' bank accounts. What follows is an extract from a report by Daily Graphic.

> *Three Nigerians believed to be members of a gang that manufactures and uses cloned Automated Teller Machine (ATM) cards to withdraw various sums of money from the accounts of a number of bank customers were arrested. Briefing the media, the Director of the Commercial Crime Unit of the Police Service, C/Supt of Police, Mr. Felix Mawusi said the suspects were arrested while they were in the process of withdrawing money from an ATM installation. He said members of the gang usually hang around ATM installations and offer to help card users who struggle to withdraw money from their accounts. Unknown to the card users, the suspects have devices such as phones that have been fixed with micro-cameras which they used to capture details on the card and the Personal Identification Number (PIN). The camera is fixed not to make any sound or flash while taking pictures. With the aid of their ATM manufacturing devices and electronic software applications, the gang then used the electronic code data they had captured to read and write the PIN on a cloned card. A total of ₵3million was siphoned by the gang. Police received a number of complaints from three banks that triggered the investigation which led to the arrest of the suspects.*

The bulk of the Ghanaian economy is driven by SMEs and petty traders who are deeply rooted in using cash and see it as a convenient way of receiving and making payment. If this ATM scam continues, it will scare them from savings and jeopardizing the cashless system of payment the Central bank is working to establish, and by extension decrease the mobilization of funds for national development.

(b) "6 Busted over Sim Box Fraud"
(The Ghanaian Times, Tuesday, January 27, 2015 edition, page 3)

Tax is a vital source of revenue for most governments which enable them fund essential services and infrastructure for their citizens. The Parliament of Ghana, in 2008 passed the Communication Service Act, 2008 (754) with intended to raise additional revenue from communication services, provided by the mobile operators to their customers. This tax regime is being undermined by "Sim box" fraudsters where calls are being diverted.

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

Government is losing a lot of revenue which could have been used for the development of the country. In the January 27, 2015 edition of the Ghanaian Times reported the complexity of "sim box" fraud techniques in Ghana as follows:

> *Six people, including Dr. Alex Tweneboah, former president of the Ghana Real Estate Developers Association (GREDA) and lecturer at the Asheshi University were in police custody. The other five arrested in separate operations in Kumasi, Tema, Accra and Koforidua by task force made up of detectives from the CID Headquarters, Officials from the National Communications Authority and various telecom operators, with technical assistance from SUBAH Info Solution, Ghana Limited. More than 21, 000 assorted SIM cards of the various mobile networks, laptops, printers, internet modems and heavy duty batteries were found with them. The Director-General of CID, Mr. Agblor explained that SIM box "fraud occurs when individuals or organizations illegally terminate a voice call which is the preserve of registered licensed network operators and usually at lower costs than approved rates". Fraudsters then used to channel the national calls away from licensed international gateway operators and presented as local calls on unlicensed networks. The suspects were arraigned on two counts of illegal termination and operation of telecommunications without authority under the Electronic Transaction Act, 2008 (Act 772). Briefing the journalists on the successful operations by the task force, the Minister of Communications, Dr Omene Boamah hinted that the activities of SIM box fraud have cost the nation $33,592,320 or GH¢107,459,000 in revenue loss between July 2014 and early January, 2015. He added that the amount involved was worrying and urged the telecommunications operators to strengthen their software's to detect unregistered SIM card in the system.*

In the cyber world, people commit crimes that they would not otherwise commit in physical space due to their status and position. The narrative pointed out that a respected PhD holder, former CEO of Real Estate Developers Association and a Lecturer was among the perpetrators who use utilized the internet capabilities to siphon the State resources. The virtual nature of the internet and identity flexibility provides incentives for the upper class individual's to misconduct themselves in the hypertext society.

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

(c) "Doctor Sodomised a 16-year-old Senior High"

(Daily Graphic, Saturday, October 25, 2014 edition, page 3)

Since the advent of the internet, the world has become a global community. This is because through the worldwide web links information is passed on and received almost instantaneously or in real time. People in different locations are able to communicate with one another by exploring social media platforms such as Facebook, Instagram, Imo and many others to advance their lives. However the increasingly use of the internet has fueled sexual predators who prey upon children's naivety and seduce them into romance relationships. The Daily Graphic, an authoritative newspaper on October 25th, 2014 captured adolescent internet sex crime and it would be interested for readers to update themselves with this story and also to understand the dynamics of cybercrime in Ghana.

> *Dr. Ali-Gabass, a gynaecologist at the Effia Nkwanta Hospital in Sekondi, was said to have had a canal knowledge of his victim five times at Kasoa in the Central Region and Alajo in Accra between October 2013 and April 2014. The victim after fifth incident, started experiencing excruciating pains and the parents rushed him to Kole Bu Teaching Hospital for treatment. While receiving treatment at the facility, the victim was diagnosed with HIV and he mentioned Dr. Ali-Gabass as the one responsible for his complications. The police prosecutor charged the accused on two counts of defilement and unnatural canal knowledge. According to facts of the case, the victim had encountered with the accused on Facebook and they became friends. They had a chat online and communicated by phone for a while until in October, 2013 when the accused arranged and met the victim at Kosoa where he forcibly had anal sex with him in his car. Subsequently, Dr. Gabass was found guilty and sentenced to 25 years' imprisonment (Daily Graphic, 14th July, 2015:3).*

In predicting online victimization among juvenile population, Marcus (2008) concluded that victimization increased when juveniles maintain social network sites without parental control. Therefore, it is an imperative for Ghanaian parents to monitor their wards on the websites they visit to avoid sexual predators.

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

2.7 Cybercrime Legislations in Ghana

The rise in technology and online communication has not only produced a dramatic increase in the incidence of crime, but has also resulted in the emergence of what appears to be new varieties of criminal activities and these pose a challenge for legal systems, as well as for law enforcement (Brenner, 2007). These new types of crime have left government and the law enforcement agencies with many questions. For instance, how does one define what cybercrime activities are legal and what activities are not legal? How does one enforce cyber laws when the relationship between the victim and the offender is often virtual? The internet allows people to interact with each other across borders, so whose jurisdiction is it? This section reviewed some laws that have been enacted to deal with cybercrime issues in Ghana.

With the recognition that cybercrime is increasingly a real threat to the country, the government of Ghana, through the Ministry of Communication has come out with some Acts to regulate the conduct of people in the cyber space. These Acts consist of Electronic Transactions Act, 2008 (Act 772), National Information Technology Agency Act, 2008 (Act 771), Data Protection Act, 2012 (Act 843), and some related provisions in the Criminal Code. The subsections that follow hint on the spirits and limitations of these acts.

2.7.1 Electronic Transactions Act (ETA), 2008 (Act 772)

The Parliament of Ghana in December, 2008, passed the Electronic Transaction Bill into law. The primary objective of the ETA is to secure the cyber space as a means of mitigating crime incidence that may affect the ability of the citizens to create worth.

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

The Act is divided into twelve groups of clauses. These are electronic transactions, electronic government services, the certifying agency, consumer protection, protected computers and critical database, Domain name registry, and appeal tribunal. Other clauses relate to the, industry forum, the liability of service providers and intermediaries, cyber inspectors, cyber offences, and miscellaneous matters.

The law enforcement is dealt with in the tenth group of the clauses and the Act empowers security agencies in the course of the execution of court warrants to seize a computer, electronic record, programme, information document or thing if they reasonably believe that an offence has been or is about to be committed, (ETA 2008, Act 772, clause 98). The law enforcement agencies may also request the preservation of evidence by providers of wire or electronic communication services or a remote computing services pending the issuance of a Court Order, clause (ETA 2008, Act 772, clause100). The Courts is empowered, upon application of a law enforcement agency, to order an electronic communication service providers to disclose the contents of an electronic communication, that is in transit, held, maintained or that has been in electronic storage in an electronic communications system, if the disclosure is relevant for the investigative purposes in the interest of national security, clause (ETA 2008, Act 772, clause 101). However, the scope of the enforcement of the Act is limited by the area of jurisdiction as it's contained in clause 142 (2):

This Act apply if, for the offence in question:

(a) The accused was in the country at the material time;

(b) The electronic payment medium, computer or electronic record was issued in or located or stored in the country at the material time;

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

(c) The electronic payment medium was issued by a financial institution in the country; or

(d) The offence occurred within the country, on board in Ghanaian registered ship or aircraft or on a voyage or flight to or from this country at the time that the offence was committed, whether paragraph (a), (b) or (c) applies.

Traditionally, the legal jurisdiction involves territories with the scope of country being defined by the limit of its boundaries. This territorial notion is ineffective to prosecute cybercriminals. Determining where cybercrime is committed can be difficult since the perpetrators and the victim can be located in different countries. The offenders may also utilize computer systems in different countries to attack their victims.

Another pitfall of the Act is that punishment is not clearly stated as in the drug trafficking law and this allows judges to exercise their discretional powers to make pronouncement on cyber offences. For instance, under the Narcotics Drugs Law (P. N. D. C. L 236), Section 2(2) states that "a person found guilty of narcotic offence is liable on conviction to a term of imprisonment of not less than ten years". Additionally, properties acquired by scammers by fraudulent means are not seized or confiscated unlike the Drugs Law, Section 11 to 14 which stipulated that properties acquired by drug traffickers should be seized. Obviously this law provides a vent for the criminal as the weight of the punishment does not commensurable with the nature of the cybercrime. Therefore, it is not surprising that the Ministry of Communications (2014), concluded in their final draft report on Cyber Security Policy that 'even though the ETA has a provisions for law enforcers to fight against cybercrime, however, this is not adequate and does not address fully all aspects of cyber security especially the multi stakeholders approach' (Ministry of Communication final draft on Cyber Security in Ghana, 2014: 6).

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

2.7.2 National Information Technology Agency Act (NITA), 2008 (Act 771)

The National Information Agency is a Ghanaian public institution established by Act 771 in 2008, as the ICT policy implementing arm of the Ministry of Communications. Its mandate is to regulate and monitor the activities of companies in the electronic industry of ensuring quality information delivery and standard of efficiency. The agency is further empowered to give accreditation to individuals who want to conduct legitimate business online.

Under this Act, the functions and responsibilities of the agency are captured in clause 3 which stipulates that the Agency shall;

(a) Perform the functions of the certifying Agency established under the ETA, 2008 (Act 772).

(b) Issue licences and ensure fair competition among licence holders in the cyber space.

(f) Monitor, enforce and ensure effective compliance with the conditions contained in licences and tariffs; (National Information Technology Agency Act, NITA 2008:3).

(h) Maintain registers for approval given for equipment used under the ETA, 2008 (772)

(n) Establish quality of service indicators and reporting requirements that apply to the licence holders under the ETA.

It's interesting to note that fake websites are being created everyday by the internet hackers and duped innocent people without NITA detection or apprehension. This could be attributed to the inadequate skilled manpower or technical enabling environment to track the perpetrators.

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

2.7.3 Data Protection Act (DPA), 2012 (Act 843)

The Data Protection Act is one of the key legislations to improve legal certainty and transparency in the cyberspace. The Data Protection Act 2012 (Act 843) was passed by parliament in 2012, to protect privacy of individual and personal data (Data Protection Act 843, 2012:5). The Minister of Communications on Thursday November 18th, 2014 inaugurated a 11-member governing board of the Data Protection Commission (DPC) chaired by the Supreme Court Judge, Justice Date-Bah to regulate the processing of personal information on the internet (Daily Graphic, 25/04/15, page 3). The Commission has the power under the clause 3 of the Act to:

a. implement and monitor compliance by individuals who utilize the electronic industry
b. make the administrative arrangements it considers appropriate for the discharge of its duties;
c. investigate any complaint under this Act and determine it in the manner the Commission considers fair; and
d. keep and maintain the Data Protection Register.

The privacy fortified the human dignity and guaranteed other key rights such as freedom of association, speech as enshrined under Article 18(2) of the 1992 Constitution of Ghana. The information and communication technologies are being used by numerous anti-social elements in aiding their illegal activities. Daily Graphic (14/11/2014, page 32) explained that data in the wrong hands have caused untimely death and jeopardized many lives. Therefore, it is an imperative that strong provisions are made to protect people against the abuse by those institutions that keep their information on the internet such as schools, hospitals and governmental organizations. The intended purposes of the Data Protection

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

Commission are yet to be fulfilled because data are still collating from the various institutions which controlled individual's information online.

2.7.4 Criminal Offences Act, 1960 (Act, 29)

The growing Internet penetration in Ghana had opened up the country into a new online trading platforms, which had empowered the average Ghanaian to transact various business operations. Even though the online portal serves as a medium of exchange for goods and services, most transactions take place offline. As a result, some Sections of the Criminal Offences Act (29/30) are recaptured in the Electronic Transactions Act (Act 772) to prefer charges against cybercrime suspects. These Sections include: 20, 21, 23, 122, 124, 133, 137, and many others.

Crimes committed under these Sections of the Criminal Offences Act 29/60 which have been reiterated in the Electronic Transactions Act (Act 772) are bailable offences and carry lesser punishment which cannot deter fraudsters from committing such offences. Besides, Danquah and Longe (2011) were of the view that the criminal code under which cybercrime suspects are currently charged has existed under the fraud laws established in 1960 which gives room for defense lawyers to often win and acquit their client because some of the facts do not support the prosecutor's evidential claims.

2.8 Conceptual Framework

This section presents the conceptual framework that explains various aspects of cyber criminality.

The discipline of criminology has been concerned throughout history with attempts to uncover the underlying causes behind law-breaking behavior. Thus, theories about crime

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

purported to locate the forces that propel or incline people toward transgressing society's rules and prohibitions. Such explanations have, inevitably, been based upon data relating to criminal activity in 'real-world' settings and situations. The emergence of the Internet poses challenges to the existing criminological perspectives in so far as it exhibits structural and social features that diverge considerably from conventional terrestrial settings. It is by no means clear whether and to what extent established theories are compatible with the realm of cyberspace and the crimes that occur within it.

In this regards, Jaishankar (2008) posited the need for a separate theory of cybercrimes because the general theoretical explanations were found to be inadequate as an overall explanation for the phenomenon in the electronic society. In view of this, he propounded the Space Transition Theory and argued that people behave differently when they move from one space to another.

(a) Space Transition Theory

The postulate of the theory posited that *persons with repressed criminal behavior (in the physical world space) have a propensity to commit crime in cyberspace, due to their status and position (Jaishankar, cited in Schmallager & Pittaro 2008:283).* There is a presumption that individuals feel varying degrees of self-reproach if they commit criminal acts. In the context of repressed criminal behavior within the physical space, they are concerned with their social status based on others people's perceptions of their personalities. Typically, most individuals would weigh both material and social risks of being a criminal as opposed to being a law abiding in the physical space. So these same people who are concerned about their social status are not bothered about their social standing in the cyberspace because there is no one watching and stigmatized them.

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

The second postulate emphasizes that *identity flexibility, anonymity and lack of deterrence in the cyberspace motivated the offender to commit crime*. These provide the offenders the choice to commit cybercrime which tends to be consistent with the notion that most members of any society are honest because of the fear of being caught (deterrence factor). Cyberspace on the other hand changes the situation and makes room for no deterrence factor. Anonymity may be used to act out some unpleasant need or emotion, often by abusing other people; it can be used to express honesty and openness that could not be discussed in face-to-face encounter.

The third assumption is that *criminal behavior of offenders in cyberspace is likely to be imported to physical space in which physical space may be exported to cyberspace as well.* This posit is advanced on the premise that the growth of e-business and internet usage has made it easier for organized crime gangs to facilitate and cover up their criminal activities which may be usually included fraud, money laundering, intimidation, theft and extortion. Also online child predators eventually carry out their activities physically after initiating the crime online.

The fourth premise *indicates the intermittent ventures of offenders into cyberspace and the spatio-temporal nature of cyberspace provides the chance to escape.* This posit seeks to advance the argument that while people do not live in cyberspace, they visit and exit at their own free will, given the very dynamic nature of cyberspace such as the ability to publish a website and subsequently remove very quickly, there is a lot of difficulty in determining the location of crimes or criminals on the internet.

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

Finally, *strangers are likely to unite in cyberspace to commit crime in the physical world.* Jainshankar (2008) explains that the internet is an effective medium for criminal recruitment and dissemination of criminal techniques for likeminded people. A lot of social sites and newsgroups are not moderated thereby creating an excellent platform for fraudsters to collate and share other people's prospects. This creates an environment for individuals to spy, sabotage and possibly leak sensitive information.

Space Transition theory provides us to some extent with an insight into the activities of cybercriminals in the electronic society. However, Burrell (2008) study on internet scammers in Ghana has questioned the integrity of the theory. She observed that the scams that occurred from the penpal exchanges reflected how scammers drew on established patterns of communications as resource for modelling their strategies for economic gain. It means that social deviants exhibited in the physical world by these miscreants are being transported to the cyber world.

Another contemporary theory worth mentioning is Network Society theory by Manuel Castells (2000). He argues that Networks constitute the new social morphology of our societies and the diffusion of networking modifies the operations of organized criminal groups on the globe. Crime is as old as humankind but organized crime; a networking of powerful criminal organizations and their associates in shared activities throughout the planet is a new phenomenon that profoundly affects international security.

(b) Network Society theory

Within the theoretical model, he presents the Space of Flows, as the central tenets of the theory. Space of Flows is essentially an understanding of how network society functions through three levels of communication.

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

The first layer is based on information technologies (consisting of electric impulses, being the actual means of communication used by a network), such as microelectronics, telecommunications, computer processing, as well as broadcasting systems. This creates the actual physical space for communication. Because of the innovation of portable devices criminals are able to communicate over vast distance and integrate diversified interest.

The second phase of the Space of Flows is compose of nodes which in effect defined the parameters of the network. Applying this to the cybercrime community, the nodes are the scammers who communicate within their shared values and penetrate the global economy.

The third level of the Space of Flows is the dominant interest. This level is important because in order for the theory of space of flow to function; it is an axiom that space societies are symmetrically organized around the prevailing themes which define the network. For instance, the Mexican drug cartels, the Nigerian "419" networks, the Ghanaian "Sakawa" networks and the myriad of regional and local criminal groupings who have come together in global template as a result of flexible communication gadgets. In the "Sakawa" philosophy, people play an auxiliary roles to flourish the idea. It is believed that there are some security agents who aide the perpetrators to acquire police criminal report to authenticate that they are not criminals; the bank officials also connive with the perpetrators to withdraw money being realized; whereas postal agents help the fraudsters to clear their goods; internet café administrators also contributing their quota to the "sakawa ideology". In view of this, the organized criminals use internet extensively to collaborate and connect with their counterparts across the globe, thus increased insecurity in the digital world.

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

Classical theories of crime on the other hand, emphasize the social and environmental forces that influence individuals to commit criminal acts. This section is specifically focused on Strain and Differential Association theories to explain why some people are cyberdevaints.

(c) Strain theory

The Structural Strain theory emanating from Structural Functionalism was proposed by Robert K. Merton following his adaptation of Durkheim's Anomie Theory. In his two famous studies, *The Division of Labour* (1893) and *Suicide (1897*), Durkheim explained that anomie occurs during a period of profound social change. It may bring loss of direction in society when social control of individual behavior has become ineffective. In times of rapid change, social disorder, economic collapse or even boom, people become more confused, depressed or excited and this results in higher rates of personal disorganization such as violent crime or suicide. He further posited that anomie could also be the result of social instability when those regulations that restrained individuals' desires and expectations within achievable limits break down, and leads to individuals' pursuit of unattainable goals which in turn led to feelings of disillusionment with themselves and society and further led to a high incidence of suicides (cf. Smith 2011).

Merton (1938) used this Durkheimian understanding of anomie to develop his theory to explain the causes of deviance in many societies (cf. Hilbert 1989). According to Merton, in every society there are cultural goals or things worth striving for such as wealth, money, prestige and institutionalized means such as getting education, working hard, disciplining oneself, pursuing honest vocation for achieving these goals. Anomie occurs when there is a breakdown or an acute disjunction between the cultural goals and the socially structured capacities of members of society to attain these goals. Which means some people cannot

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

achieve the culturally approved goals through culturally approved institutional means, hence they resort to unapproved means to acquire the cultural goals that have been internalized. For some people there is structural strain between the goals and means of society. Merton identified five responses to these goals/values and means/norms dilemma, four of which turn to be deviance in an anomic society. These include Conformity, Innovation, Ritualism, Retreatism and Rebellion, but for the purposes of this study, the emphasis would be on the Innovators.

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 ways 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 (cf, Schaefer, 2005:182). Some examples are drug dealers, armed robbery, prostitutes as well as those engaged in cybercrime.

In Ghana today, there is no limit set on what people can acquire in terms of material wealth. Abotchie (2012), argues that to the Innovators, while the urban culture emphasizes material success, the reality is that the social structures within the society place limitations on the approved means. He further stresses that due to the intense competition that exist within urban communities, Merton's innovation becomes the most common form of adaptation.

Many sociologists have applied this theory to explain deviance in society with a varying degree of success but it fails to explain how deviant behavior is learnt through deviant subcultures and exposure or association with other deviants.

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

(d) Differential Association Theory

Another famous classical theory for explaining criminal behavior is Edwin Sutherland's Differential Association which was developed in 1939 and has received a widespread popularity and acceptance in criminological circles (cf. Vold & Bernard, 1986:205). According to Regoli and Hewitt (1997:181), 'no single idea in modern criminology has had impact on how people reflect on crime as differential association'

According to Sutherland, criminal behavior is learned in the same way as law-abiding values are learned, and that, this learning activity is accomplished in interactions with others through a process of communication within intimate groups. He further argues that, just as one can be socialized into good behavior, so also can one be socialized into bad behavior. The theory of differential association consists of nine principles:

1. Criminal behavior is learned; it is not inherited. This means that the person who is not already trained in criminal act does not invent such acts, just as a child does not make courteous remark unless he has been trained or socialized to that effect.
2. Criminal behavior is learned in interaction with others through communication. This communication is verbal in many aspects but also includes communication of gestures often described as non-verbal communication.
3. The learning occurs within the intimate groups: Sutherland claimed that, only small, face-to-face gatherings influence behavior. Consequently he focused on peer or family groups as the most likely sources of initiation into delinquent values and activities. This means that, impersonal agencies of communication such as picture shows and newspapers play relatively unimportant part in the genesis of delinquent behavior.

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

4. When criminal behavior is learned, the learning includes (a) Techniques for committing it, which are sometimes complicated, and sometimes very simple; (b) the specific direction of motives and drives, rationalization and attitude.
5. The specific direction of motives and drives are learned from definitions of legal codes as favorable or unfavorable. This means that, when one's associates define the legal codes as things to be observed, the learning of the criminal acts may be impeded. The reverse is true.
6. A person becomes criminal because of an excess of definitions favorable to violation of law over definitions unfavorable to violation of law. This is the core principle of differential association theory. It reinforces the belief that the definitions favorable to the violation of law can be learned from both criminal and non-criminal people.
7. Differential association (tendency towards criminality) varies in frequency, duration, priority and intensity. This means that the longer the time, the earlier in one's life, the more intensely and more frequency people are exposed to a set attitude about criminality, the more likely it is that they will be caught up in the fray.
8. The process of learning criminal behavior involves any other learning. This implies that, the mechanisms for learning criminal behavior are the same as those for law abiding values and other socially relevant skills. The suggestion is that, in as much as the content of what is learned is different, the process giving rise to criminal behavior is the same as any other law-abiding behavior.
9. Both criminal and non-criminal behaviors are expressions of the same needs and value. Put differently, the goals of criminal and non-criminals are usually the same. What is different is the means they adopt to pursue this same goal. For instance

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

thieves generally steal in order to secure money. Honest laborers likewise work with the monetary value in mind.

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 neighborhood.

Differential Association has been criticized by some scholars who say it is defective as it fails to consider the issue of persons who commit crimes purely out of their free will. Sutherland was also criticized for failing to account for people who commit crimes due to such personality traits like aggressive. However, the theory has been vital in explaining how delinquents acquire their criminal behaviors.

(e) Routine Activity Theory

The final theory, the Routine Activity theory proposed by Lawrence Cohen and Marcus Felson in 1979 was discussed to address the dynamics of cybercrime activities in Ghana.

The theory states that a crime occurs when there is a convergence of; motivated offender, suitable target and the absence of capable guardian. Offender with the inclination to commit crime is motivated by the fact she or he is in the right place at the right time to move against his target when there is no one around to stop the perpetrator.

The authors explained what constitutes a suitable target. They identified four items: value, physical visibility, access and inertia are likely to affect target suitability. For example, if a

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

gang of robbers want to steal something, they have to know that it is there in the first place, thus physical visibility to attack. Access, is also important for deciding the suitability of a target. For example, if a house is left unlocked it is much easier to gain access than the house that is locked. The authors further explained that high value items, such as cars and electronics are more likely to get stolen than the less valuable item.

The guardianship emphasis is on deterrents measures, like the police patrols, effective laws, security guards, neighborhood watch, vigilant staff, friends, neighbors and CCTV systems. In conclusion, the authors argued that the mere presence of one of these preventive elements would deter potential offender from being perpetuating the crime.

The Routine Activity theory was modeled by Reyns, Henson and Fisher (2011) to study cybercrime victimization. According to Reyns et al (2011) , the *online exposure to motivated offenders* include: (a) the amount of time individual spent online each day, (b) number of online social networks one's owed, (c) number of times each day the individual updates his or her online social network accounts, and (d) the number of photos the individual has posted online.

Online proximity to motivated offenders. Within a system such as the Internet, victims and offender can come into virtual proximity. For example, chat rooms bring together users from various physical locations (different cities, states or countries) to participate in real-time communication within the same online forum. Online proximity to motivated offenders can be measured by variables such as: (a) whether the individual's allows other internet users whom he or she does not know, that is strangers to access his online social network, which may include personal information (contact information, photo, interest);

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

(b) the number of friends that a person has across his/ her online social networks; and (c) whether the potential victim has ever utilized an online service in acquiring friends for his social network.

Online guardianship. In online environment, the presence of firewalls, security programs, police patrols and effective law mechanism can prevent intruders having access into people's accounts so that only approved parties can view profiles/information. Absence of these trackers can create an opportunity for cybercriminals.

Online target attractiveness. Target attractiveness can be described as the material or symbolic desirability of persons or property, targets to potential offenders, as well as the perceived inertia of a target against illegal treatment (Cohen et al., 1981). In the case of online victimization, certain information might facilitate the offender's pursue at the victim or make the individual a more desirable target (for example, posting relationship status, photos, sexual orientation), thereby increasing an individual's attractiveness as a target.

The researchers found out that individuals with multiple social networking accounts had a greater probability of suffering an interpersonal victimization, including online harassment. Another study testing the applicability of routine activity theory to explain cybercrime affirmed that students that disregard their participation in online activities, and do not use computer-security software are more likely to be victimized (Choi, 2008). Holt and Bossler (2009) also advised that people whose regular activities place them in situation where they have the possibility of interacting with so many people are standing the risk of being victimized.

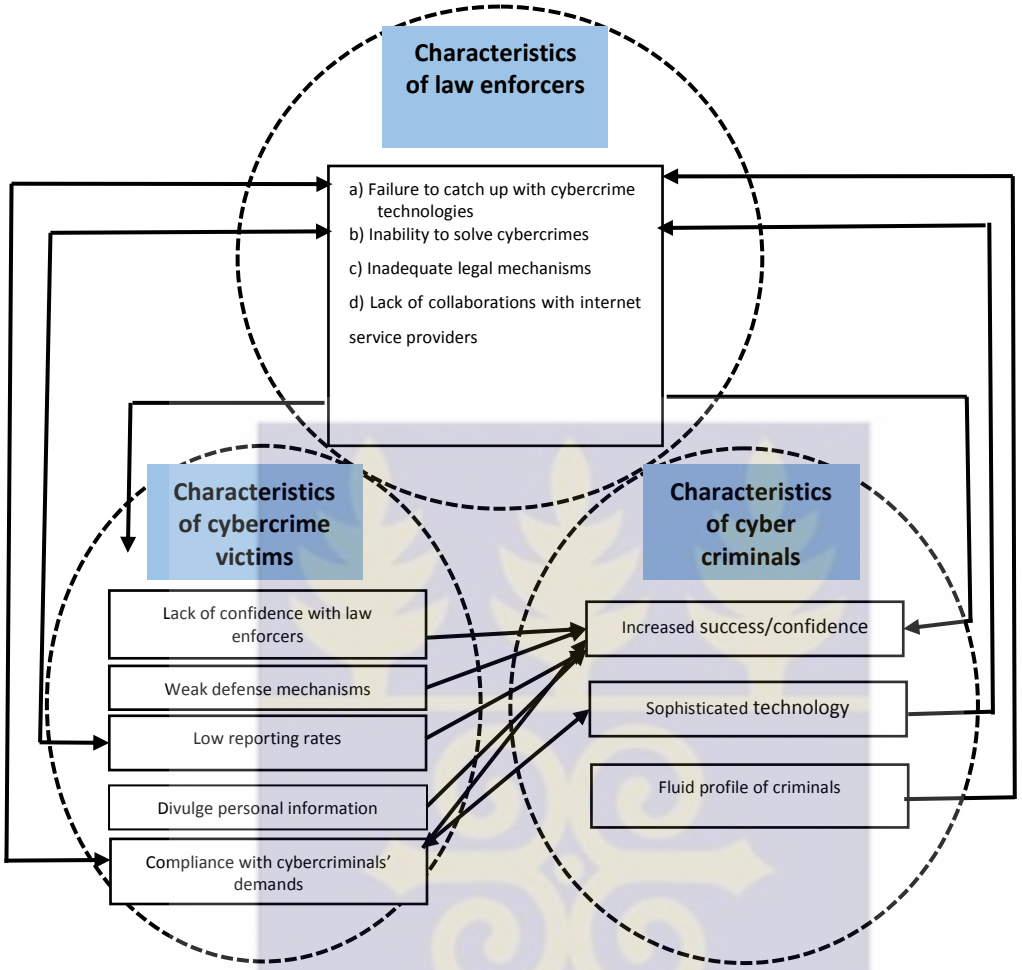
University of Ghana http://ugspace.ug.edu.gh

However, despite the studies that have found evidence supporting the use of routine activity theory in explaining cybercrime victimization, Yar, (2005) criticized that the routine theory cannot be applied to the study of online victimization. He argued that because cybercrime exists in a world without any physical or time constraint, new forms of crimes have emerged which requires a new theory to explain.

This theory is significant for the explanation of the three dimensions to the study; that is law, victims and perpetrators. In cyber world, victims become suitable target through increasing time spent on the internet, and the use of online services such as banking, shopping which makes user prone to phishing attack. In addition, the behavior of some victims can attract fraudsters to garner information about their daily life situation on the internet. In future, scammers use these information to hypnotize the person by way of relinquishing his or her wealth to them. For instance, people post sensitive information on their social networking sites like their marital status, work opportunities, bank details and other social achievements. All these are attractive indictors. Moreover, individuals become vulnerable because there are no effective laws to punish the offenders. In the same vein, Ghana Police Service cannot mount patrols on the internet society to track the activities of cybercriminals due to inadequate skilled manpower and lack of modern equipment. The situation has created a vicious circle of cybercrime because it increases the offenders' confidence to continue attacking innocent people on the cyber world. The characteristics of offenders, victims and the law enforcement agencies are presented in diagram one.

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

Diagram 1: The vicious Circle of Cybercrime Activities in Ghana



The diagram capturing the inter-linkages of factors that explain cybercrime

The diagram tries to visualize the theoretical framework on how the behavior of cybercriminals, victims and law enforcement agencies have reinforced one other and formed the vicious circle. The factors which contribute to the structural uniqueness of cybercrime in Ghana are examined in the next sub-sections.

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

The Characteristics of Law Enforcement Agencies.

The law enforcement agencies, especially the police is lacking behind about the technological capabilities to deal with the rapidly growing cybercrime due to the failure of the organization resistant inertial to change structures and practices. Brenner (2004) noted that failure by the police force to adapt to the technological driven operations make them inexperience in cybercrime management. Another characteristics exhibited by the law enforcement agencies is that cybercrime legislations are not well developed to contain the situation. Commenting on legal issues, the Ministry of Communications 2014 cyber policy report revealed that the Electronic Transaction Act 772, 2008 is not adequate and does not address all aspect of internet security. Thus, law enforcers have to use their discretion in prosecuting such crimes. Given that the majority of internet infrastructures in Ghana are owned by private sector, many cybercrimes cannot be solved because service providers may feel reluctant to disclose their subscriber's information to the security agencies. Law enforcement agencies' lack of ability to solve cybercrime reinforces cybercriminal's confidence as well as victims' unwillingness to report such crimes.

The Characteristics of Cybercriminals

The fluid nature of cyberspace has also hampered the law enforcers' ability to solve online crimes. There are numerous services that will mask a user's IP address by routing traffic through various servers, usually for a fee. This makes it difficult for police to build up criminal database. In addition, some cybercriminals are highly skillful and adopting sophisticated technology to swindle their 'client' thereby minimizing the probability of getting caught.

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

The Characteristics of Victims

Cybercrimes are among the most under-reported forms of criminality in Ghana. An inferences could be drawn from Table 1 of the study where 161 cases of internet fraud were recorded by the Ghana Police Service, which covered the period of 2006 to 2011. The low figure does not motivate the police to add up their operation on the internet as compared to the public perceptions and media sensationalism about the crime. Victims' unwillingness to report online fraud as a results of lack of confidence with law enforcers further encourages offenders' behavior. Weakness of defense mechanisms corresponds to likelihood attacks. While some weaknesses are technological, others are behavioral in nature such as divulging sensitive information on the internet. Scammers take advantage of Internet user's ignorant by tricking them and harbor their personal information fraudulently.

The above discussion has indicated that in the absence of appropriate measures, the elements of the vicious circle of cybercriminal activities can lead to public distrust of law enforcement agencies and that will increase the offenders' confidence which resulted in serious online fraud in the country.

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

CHAPTER THREE

RESEARCH METHODS

3.0 Introduction

The end results of scientific investigation is useful only to the extent that the most efficient techniques and procedures are adopted in the planning and execution of the field operations, as well as, in the analysis of the data collected (Kumekpor, 2002). Creswell (2003) further echoed that the selection of the research approach does not simply inform the research design but it gives the researcher the opportunity to critically consider how each of the various approaches may contribute to, or limit his study. Basically, there are three purposes for conducting social research. One of them is to offer description. An example is a census which describes population demographics. The second purpose is to explain things, and a study conducted in this mode usually emphasizes on causal relationships, measurement and statistics. It also employs hypothesis and deductive approach to arrive at a conclusion. It further explains depended and independent variables, for example, why bribery and corruption are higher in the public institutions than the private institutions in Ghana. The third reason is exploratory. Neuman, (2003) advised that exploratory researches are carried out to explore a hard-to-reach population, dispel some misconception on phenomenon. This research is exploratory in that it seeks to examine the dynamics of cybercrime activities by looking at the principal actors, that is the offenders and victims who at the moment are hidden populations. It is therefore important to opt for an appropriate research methods to shed light on this social problem which is largely characterized by public speculations.

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

This chapter introduces the research design, the study area, the sampling techniques, number of respondents, sources of data, data collection techniques, instrument of data collection, data analysis, ethical considerations, and problem encountered on the field.

3.1 Research Design

Research design is a procedure for enquiring into a study that spans the decision from broad assumption to detailed method of data collection and analysis (Creswell, 2009). As the population under investigation are hidden, the qualitative approach is applicable for exploratory studies such as this where the area of research is so new, vague or centered on criminal behavior. Sometimes, victims feel ashamed of reporting the incidence to the police as a result of their social status (Warner, 2011). As Glickman observed, "interviewing scammers resembles infiltrating the Mafia, not part of the training of social scientists" (cf . Smith, 2011:13). Any attempt to elicit the view of people whose activities are seen not only as immoral but criminal is a laborious task. However, Neuman (2003) argued that in analyzing criminal behavior, the socioeconomic context in which an individual find himself/herself influences our understanding of why the person engaged in that act. Therefore, the researcher developed some close-ended questions to generate basic statistics to enhance the analysis of the socio-demographic characteristics of the offenders and the victim which served as frame of inferences. It means that the investigator adopted mixed method approach but greater emphasis was placed on qualitative than quantitative data collection and analysis.

To achieve this strategy, Creswell et al (2003) Concurrent Embedded mixed method approach was adopted as the design for the project. This involves a process of gathering qualitative and quantitative data from the field concurrently. The approach guides the

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

research and given less priority to (either quantitative or qualitative) within the predominant research interest. The nesting method provides a supportive role to the dominant method to enhance the understanding of data analysis. Thus, Morse (1991) noted that a primarily, qualitative design could embed some quantitative data to enrich the description of the sample participants. Considering the time frame, the design helped the researcher to administer both the questionnaires and interview questions on a single phase without undue hindrance.

3.2 Study Area

The study was situated within the Accra metropolis. A preliminary information gathered from the Criminal Investigation Department (CID) of the Police Service indicated that the majority of cybercrime cases occurred in this vicinity, and it is frequently mentioned in media reports of having high prevalence rate of cybercrime. Strategically, the location offered the researcher an opportunity to interact with the various police units combating cybercrime in Ghana.

Accra is a highly urbanized city in the Greater Accra Region. It is a Metropolis that hosts the capital city of Ghana. It covers an area of 200 square kilometers and is made up of ten sub-metros namely; Ayawaso Central, Ayawaso East, Ayawaso West, Ablekuma North, Ablekuma South, Okaikoi North, Okaikoi South, Osu klottey, Abbosey Okai, and Ashiedu Keteke (www.ama.gov.gh, 2015).

Accra is also a regional capital of the Ga ethnic group. The original occupants of Accra are the Ga. Some of the indigenous Ga communities in Accra include; Osu, La, James Town, Chorkor, Teshie, New Town, Bubuashie, etc. However, due to its cosmopolitan nature,

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

people of all ethnic backgrounds have come to settle in Accra. Areas such as Legon, Dansoman, Cantonment, Lapaz, Nima, Tesano, Madina etc. are inhabited by individuals from different ethnic background.

According to the Ghana Statistical Service report (2014) on 2010 Population and Housing Census, the population of Accra Metropolis is 1,665,086 representing 42% of the region's total population. Males constituted 48.1% and females represent 51.9 percent. It has a youthful population (below 23 years) of 50.94% depicting a broad base population pyramid which tapers off with a small number of elderly persons (60+) constituting 5.9 percent.

The Metropolis has a household population of 1,599,914 with an average household size of 4 persons per household. Children constitute largest proportion of the household composition of 35.5% while grandchildren consist of 6% of household population. Spouses form about 11.1%, nuclear households (head, spouse(s) and children) constitute 26.9% of the total households (Ghana Statistical Service, 2014).

On literacy and education, 89% of the population are literate while 11 percent are non-literate. The number of non-literate females (98,439) was more than twice that of males (39, 567). Five out of ten people (52%) indicated they could speak and write English.

With regards to the economic activities, about 70.1 percent of the population aged 15 years and above are economically active while 29.9% are economically inactive. About five out of ten (57.8%) unemployed are seeking work for the first time. On the occupation status, only 1.7 percent are engaged as skilled agricultural and fishery work, 38.5% in

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

services and sales industries. Craft and related trade constitute 20.1%, and 17.2 percent are engaged as managers, professional, and technicians. The private informal sector is the largest employer in the Metropolis, employing 74% of the labour force followed by formal sector with 16.9 percent.

The District analytical report of the 2010 Population and Housing Census further revealed that the population of 12 years and above (73.5%) are using mobile phones. Men who own mobile phones constitute 49.9 percent as compared to 50.1 percent of females. Persons using internet facilities in the Metropolis is 19.4 percent compared to 18.6% in the whole region (Ghana Statistical Service, 2014:40).

The city is also characterized by over-population and over-urbanization. According to Abotchie (2012), over-urbanization occurs where the jobs available in the urban areas cannot cater for the number of people living in the city. The unemployment situation and the large percentage of youth population has some serious social and economic ramification for the metropolis.

3.3 Sampling Techniques

As the population under study was clandestine (the Victims and Offenders), the researcher employed two non probability sampling techniques for the selection of respondents, and these were purposive and snowballing. Snowball sampling technique also called 'chain sampling' or social networking by other scholars is a method of recruitment particularly suitable for identifying participants with a very specific characteristics or hidden groups who may be difficult to identify with other recruitment methods (Hennink et al, 2011). It means that the researcher can identify an individual member of a particular social network

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

and using the snowball effect to trace the other members like friends, families, personnel and colleagues in order to identify possible respondents. An advantage of this method is that potential participants are typically linked to the study by a familiar, trusted person who can describe the interview process and alleviate any concerns such as fear, thus increasing participation in the study. However, a snowball technique can take time as participants are identified one at a time and that is why Hennink et al. (2011) suggested that this method may be more suitable when recruiting for in-depth interviews.

In this study, the researcher gathered detailed information about the cybercrime offenders and the victims from the CID headquarters and used the report to contact some of the respondents. Moreover, because the interview schedule was face-to-face, friendly relationships were established and it encouraged some interviewees to link the interviewer to other social networked members. Besides, the social networking approach helped the researcher to blend with police informants to identify some of the principal actors (offenders) for the study.

Purposive sampling technique was also used. Taking into cognizance the nature of the research, it was an important to seek out relevant people with the required knowledge for the study. However, Kumekpor (2002: 137) argues that it is not always the case in research that certain characteristics or phenomena are distributed randomly or uniformly in the universe, and even hard to reach population. In such cases, 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 suited for the research outcomes.

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

3.4 Sample Size

A total of 26 respondents participated in the study. The number consists of 11 cyber offenders, 6 internet fraud victims, a legal practitioner, and 8 Police personnel were selected from four Units at the CID headquarters who specialized in handling internet fraud cases. These departments are: Commercial Crime Unit (CCU), Documentation and Visa Fraud Section (DVS), Intelligent Unit (IU) and Legal and Prosecution Unit (LPU). Two officers were selected from each unit. The four senior police officers heading these units were purposively selected to enrich the discussion. The assumption is that the higher the rank the more knowledge one can acquire on the job. Another four staff were randomly selected amongst the junior ranks to share their thought and experiences about this emerging crime. Overall the size of the population is rather small; but given the qualitative orientation of the study and the fact that the group under study is evasive, the size can be considered as adequate particularly as data saturation was experienced during the field interviews.

On preliminary visits to the Cocoa Affairs Court Directorate in Accra, the researcher contacted three judges and surprisingly, they all advised that "Court 8" judge who is an expert in cybercrime should rather be consulted. So the investigator had to settle on her to shed light on legal issues relating to cybercrime in Ghana.

With regards to the number of cyber offenders, the researcher settled on 11 respondents, because the concept of saturation occurred. It is the point in data collection when no new or relevant information emerge from the interviewees (Bryman, 2008). Hennink et al. (2011:88) argued that "after reaching information saturation, further data collection becomes redundant because the purpose of recruitment is to seek variation and context of

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

participant experiences rather than a large number of participants with the same experiences".

Although the interview schedules took place at different locations in Accra, after reaching the Ninth respondent, the investigator realized that the subsequent candidates had almost similar responses to the questions being posed on them. To determine the point of Saturation, the principles of grounded theory developed by Glaser and Strauss in the early 1960s was followed. It is a step-by-step of categorizing, coding, constant comparative analysis, sampling and saturation of data. Moreover, Strauss (1987: 5) elaborated that 'grounded theory is not readily a specific method but rather it is a technique of doing qualitative analysis which involves the progressive identification and integration of categories of meaning from the data'.

The initial three interviews conducted on the field helped the researcher to fine-tune the set of questions guiding the interview schedules. In each interview, a verbatim transcript (word-for-word) was produced through readings from the data. Verbatim transcription is an essential tool for analysis as it captures information in participants' own words, phrase, expression and cultural meaning. At the coding process, various categories of information were identified and descriptive labels were also attached to discrete instances of phenomena. At the comparative stage, serious reading occurred while the researcher skimmed the transcripts by moving back and forth between the identification of similarities among and differences between emerging categories. At the point of saturation, after reaching the 9th respondent, I realized most of the responses kept repeating in the subsequent interviews; no new category were identified from the codes and the variation for existing categories also ceased to emerge. So further interviews

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

would simply add time and cost without adding to the range of strategies already identified. Therefore, Corbin and Strauss (2008) concluded that the number of participants in qualitative study is effectively guided by the diversity in the information gained.

The internet fraud victims were difficult to reach. The information gathered from the CID revealed that victims are usually a high profile individuals or rich expatriates who cannot face the embarrassment of people knowing that they have been duped. Moreover, foreign victims who wanted to pursue the case were being advised by their Ambassadors to pull out for lack of confidence in the Ghanaian legal system, which has been tainted with corruption and undue delay of cases. These factors might have been accounted for the low response rate. However, sample size is not always drawn to only estimate the distribution of certain traits in the population but also to gain an in-depth understanding of social phenomenon or development (Becker 1998, cited in Smith 2011:17).

3.5 Sources of Data Collection

Secondary and primary data were used for the study. Secondary data were obtained from books, articles, newspapers, organizational reports and internet sources to review the literature. These were analyzed in chapter two to portray that cybercrime is a global trend. Primary data were also collected through preliminary field investigation, face-to-face interviews and questionnaires. The table 2 showing the classification of respondents and the types of data elicited from them.

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

Table 2: Summary of Data Source

CATEGORIES OF RESPONDENTS		NUMBER	(%)	SAMPLING TECHNIQUES	TYPE OF DATA COLLECTED
1	Police personnel (key informants)	8	30.8%	Purposive	Qualitative
2	Legal practitioner (key informant)	1	3.8%	Purposive	Qualitative
3	Offenders	11	42.3%	Snowball	Quantitative & qualitative
4	Victims	6	23.1%	Snowball	Quantitative & qualitative
Total		26	100		

The table 2 depicts 4 categories of respondents, namely; police personnel, legal expert, scammers and cyber victims. The 2013 Annual Report of the Ghana Police Service highlighted that the basic function of the Commercial Crime Unit (CCU) is to investigate all criminal cases related to commercial activities. The Documentation and Visa Fraud Section (DVS) handling visa and documents fraud including cyber fraud. Legal and Prosecution Unit (LPU) prosecute cases and offer legal advice to the various units concerning case docket and appropriate legal instruments prefer against culprits. The Intelligent Unit mounted surveillance, conducted crime analysis, gathering and disseminating criminal information to other stakeholders. The researcher purposively selected officers who constituted 30.8% of the entire data understudied from the four departments to unearth their views on the subject matter. The information collated from the police published data served as a road map to trace some of the offenders and the victims to generate quantitative and qualitative records to explain their demographic backgrounds and every day meaning of internet fraud. All the 26 respondents took part in the qualitative part of the study. For the quantitative aspect, 17 out of the 26 respondents participated and they were made up of the victims and the offenders

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

3.6 Data Collection Technique

The data were collected over a period of 9 weeks (i.e. from March to April, 2015). Four sets of interviews were advanced to the selected respondents; the offenders, victims, police and the legal practitioner. Hinnink et al. (2011:84) advised that 'the focus of a researcher in the qualitative study is to gain detailed understanding of certain phenomenon, to identify socially constructed meanings of the phenomenon and the context in which the phenomenon occurred'. To achieve these, an in-depth interview (one-to-one) technique was explored with the used of interview schedules to gain detail insight into the research problem from the perspective of the studied participants.

3.7 Research Instruments

The main instruments adopted for the data collection were interview guide and the questionnaire. The interview guide allowed for face-to-face encounter to emerge between the investigator and all the participants. Since the population is unknown, personal conversation helped to establish good rapport, thus quality responses were assured. The flexible nature of the interview guide further allowed the interviewer to probe deeply into respondents' beliefs, attitudes and inner experiences by following up questions to clarify vague statements on cybercrime. The closed-ended questionnaire on the other hand was designed to collect and quantify the socio-demographic characteristics of the offenders and the victims. The questionnaires were distributed after the researcher had explored the snowball technique to trace the offenders and the victims. A total of 23 questionnaires were filled which comprise, 16 questions for offenders, and 7 questions for victims respectively. Self-administered procedure was followed because of the respondents' educational background. In this instance, the respondents answered the structured

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

questions by themselves. This afforded the researcher an opportunity to collect them back before the interview continued.

3.8 Data Analysis

Essentially, qualitative analysis involves a process of discovery that enables the researcher to remain close to the data and form an evidence-based understanding of the research issues. As stated earlier, Grounded qualitative procedure was explored and most of the processes have been explained during the saturation process.

In the data analysis, each of the in-depth interviews was transcribed as soon as collected. It allowed me to identify new issues which fed into the subsequent interviews, leading to greater depth in the information collected as the study progressed. Through the readings, codes were identified and it involved ideas, opinion shared by the respondents. Strauss (1987:27) stated that 'the excellence of qualitative research rests in large part on the excellence of coding'. Therefore, a codebook was introduced to keep all codes relevant to the study. Besides, since code development is an evolving process, codebook was a vital reference for qualitative analysis, to keep track of changes that occurred throughout the project. All the colloquial style of language and phrases expressed by the participants were preserved. These words reflected the participants' emphasis and emotions which holds culture meanings that enriched the analysis. Comparison as an analytical tool was used to stimulate thinking about the properties within categories and subcategories. And thus, thematic areas emerged. The final aspect was the 'art' of the qualitative analysis in which the researcher interpreted the lived experiences of the respondents from the social and cultural meanings that underlie people's behavior. The procedure helped to address the

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

research objectives and also provided better understanding on cybercrime activities in Ghana.

The descriptive statistics generated from the questionnaires were also analyzed and presented in the form of bar graphs and pie charts to explain the results in relations to the demographic variables of offender and the victims.

3.9 Ethical Considerations

Kumekpor (2002) emphasized that the most important elements in the research enterprise are the respondents, and everything must be done to alleviate their fears and anxiety. Neuman (2003:116) also argue that "ethics defined what is or is not legitimate to do or what moral research procedure ought to be involved by the investigator". He further advised that ethics begin and end with the researcher's integrity and moral values. Bryman (2008) also warned that the fundamental ethical principles of social research are: never coerce anyone into participating; participation must be voluntary at all times. Permission alone is not enough; people need to know what they are being asked to participate so that they can make an informed decisions.

Having embedded with these great scholars thoughts, an introductory letter was obtained from the Sociology Department, University of Ghana, and signed by the thesis coordinator to authenticate that the researcher was not an imposter. In addition, an ethical clearance was obtained from University of Ghana Ethical Committee for Humanities (ECH) whose primary goal is protecting research participants from physical or psychological harm. On that note, a Protocol Consent Form was filled out and distributed among the participants. The Section 'C' of the form captured the interviewer's and supervisors contacts addresses

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

so that participants could call for further clarification or concerns about the study. Moreover, privacy, anonymity and confidentiality of the participants were adhered to by using pseudonyms to protect the respondent's identity.

3.10 Problem Encountered on the Field

A major challenge of the study was the fact that the success of the research depended a lot on the willingness of respondents to collaborate with the researcher and provide detailed responses. However, some respondents refused to be audio-taped, the reason being that their voice could be easily identified. This meant that the researcher had to take a lot of notes and this hampered the smooth flow and pace of the interview process. Most worrisome, the Offenders were skeptical whether the researcher was gathering the information for security agencies. However, this obstacle was overcome through reassurance of utmost confidentiality, and pseudonyms were used to represent respondents to hide their real identities. Also, interviews were usually done away from the area where respondents reside to avoid suspicion from others.

One other difficulty was the lack of current, reliable, and accurate cybercrime statistics from the Ghana Police Service to serve as catalyst for comparing and contrasting media reports about the growing tempo of the menace. In their defense, however, one personnel from the CID headquarters explained:

> My brother, it is difficult to build an accurate data on cybercrime; some of our units initially responsible for handling such cases have been merged and it has affected our work. So for now, we classified the internet crime under traditional fraudulent activities. As you can see from my machine [computer], since 2012 we did not have a column [space] for such specific cases (Informal conversation at the CID headquarters, 22/01/2015).

Another pitfall was the fact that all cybercrime victims interviewed were Ghanaian citizens. They were identified at the various police offices/Stations where they lodged the complaints. However, the background checks revealed that the majority of the victims

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

hailed from outside the borders of Ghana. All attempt by the researcher to get foreign victims proved futile because the police had lost contact with them. Besides, those who reported the case to the Ghana police opted to stay out based on the advice they received from their Ambassadors and High Commissioners for lack of confidence in the Ghanaian criminal justice system. Also, the investigator wanted to access the expatriate victims' case dockets/extracts that are under the police custody to make inferences, or content analysis, but one officer explained that they are yet to classify the information for public consumption and that was worrisome situation because some of the cases happened way back in 2006.

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

CHAPTER FOUR

DATA PRESENTATION AND DISCUSSION OF FINDINGS

4.0 Introduction

The intent of this study was to explore the dynamics of cybercrime activities in Ghana. To be abreast with the everyday meaning of the issue, four major stakeholders were contacted to unearth their views. The objectives which informed the research were organized around the live-experiences of cyber offenders, victims, and how the law enforcement agencies are responding to this new social phenomenon. This chapter is organized under four subheadings. The first part involves the discussion of quantitative data or attribution of the scammers. Part two covers the dynamics of cybercrime in Ghana-the meaning, motivation and processes. The stakeholders in the cybercrime industry: scammers, victims and police were captured in part three of the study. The final part of the chapter captured the conclusion under the major thematic areas; that is offenders, law enforcers, and the victims.

4.1 Part I: Discussion of quantitative data/attribution of the scammers

The data in this section is organized to address my first objective which focused on the social characteristics of the fraudsters.

The background data were gathered on the perpetrators to determine its influence on their ability to commit cybercrime. The information included fictitious names, age, marital status, religion, education, location, employment status, number of years spent in cybercrime, and money realized. All these profiles have been highlighted in table 3.

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

Table 3: The Profile of Scammers[19].

Respondents		Age	Marital status	Religion	Highest level of education	Location	Employment status	No. of years spent in cybercrime	Money realized
1	Doe	22	Single	Christian	University student	Bubuashi	Unemployed	4	"a lot"
2	Ayiteh	24	Single	Traditional	SHS Dropout	Lapaz	Unemployed	6	Gh¢64500
3	Ben	17	Single	Christian	SHS graduate	Dome pillar 2	Unemployed	3	Gh¢8170
4	Umar	18	Single	Islam	JSH graduate	Newtown	Unemployed	2	Gh¢7200
5	Yeboah	24	Single	Christian	JHS graduate	Newtown	Unemployed	4	Gh¢40600
6	Ken	27	Married	Christian	University graduate	Tesano	Private teacher	6	"infinity"
7	Rauf	22	Single	Islam	SHS graduate	Nima	Unemployed	4	Gh¢16300
8	Reginald	23	Single	Christian	JHS graduate	Kotobabi	Lottery vendor	5	Gh¢11610
9	Figo	33	Married	Islam	SHS graduate	Mile 7	"Susu" collector	4	Gh¢10000 +
10	Fred	17	Single	Christian	SHS graduate	Alajo	Unemployed	2	Gh¢ 4200
11	Cosmos	22	Single	Christian	SHS graduate	Alajo	Unemployed	3	Gh¢36900
	Total amount realized by the scammers								**Gh¢ 199480**

Source: Field work. (The names mentioned above and subsequently used are all pseudonyms)

Note: "a lot", "infinity", means the two respondents could not quote any amount because they have gained a lot from their victims.

[19] All the foreign currencies were evaluated and converted into Ghana cedis

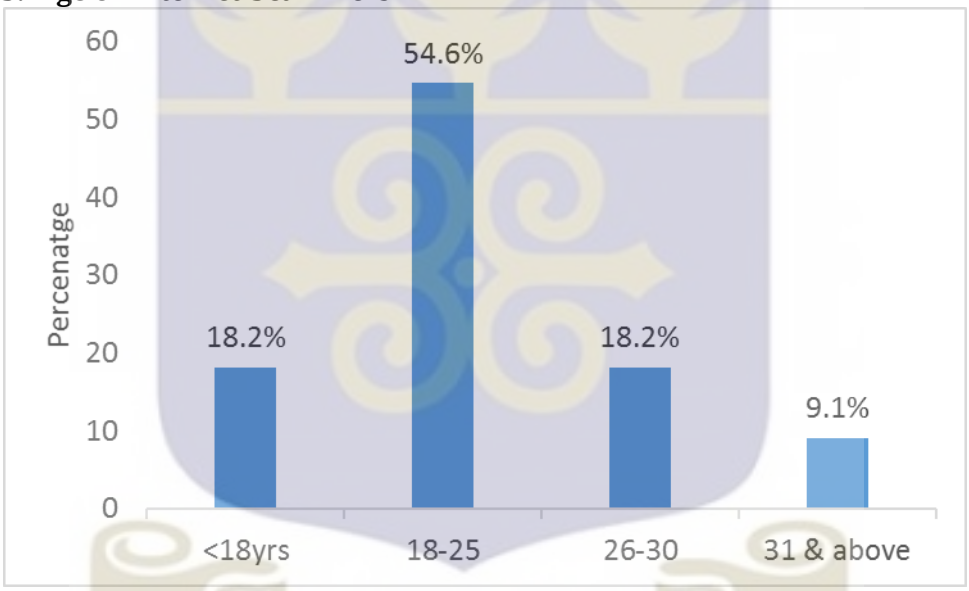
University of Ghana http://ugspace.ug.edu.gh

The profile of the 11 scammers were analyzed and presented in the form of Bar graphs and pie charts.

4.1.1 Age of Internet Scammers

The age of cybercriminals were obtained to ascertain which categories of people experience the effect of cybercrime activities in Accra. Some school of thought believe that cybercrime is predominantly committed by the youth. This ties in with the literature where Smith (2011) indicated that "Sakawa" is mostly committed by people between 18 to 24 years. Figure 3 depicts the age distribution of the internet scammers.

Figure 3. Age of Internet Scammers



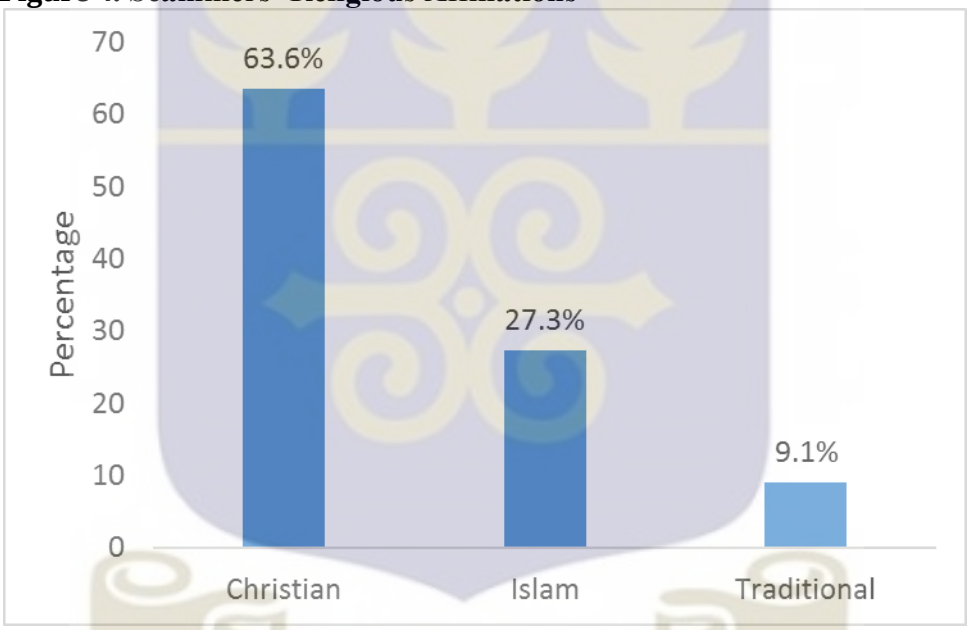
The majority of the respondents fall within the ages of 17 to 30 with an average of 23 years. All over the world, the youth form a valuable assets because they regenerate society. The indulgence in "Sakawa" activities by the youth have some negative repercussion for their future and the coherent nation building.

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

4.1.2 Scammers' Religious Affiliations

Religion as defined by Nukunya (2003:55) 'as beliefs and practices associated with the supernatural'. It plays a vital role in shaping individual's character, teaching morals as enshrined in the 'golden rule, do to others what you want others to do unto you. Moreover, the general assertion is that people from religious backgrounds are taught the moral values which enable them to lead a conforming life. It is therefore important to find out the extent to which religious affiliation impacted on the behavior of the cybercriminals. Data on religious affiliations are presented in figure 4.

Figure 4. Scammers' Religious Affiliations



Drawing from figure 4, out of the 11 respondents, 7 of them, representing 63.6% were Christians whiles Islam constituted 27.3%. Going by Ross' (cf. Abotchie, 2012:11) admonition that belief systems rather than secular laws as potent mechanism to control behavior because God is omniscient, one would expect to find an impact of Christian, Islamic, and Traditional Africa Religion beliefs systems on the lives of the cybercrime perpetrators. This however was not the case. Neither the fear of punishment for violating the relevant doctrines of religion, nor the desire to be the beneficiaries of the

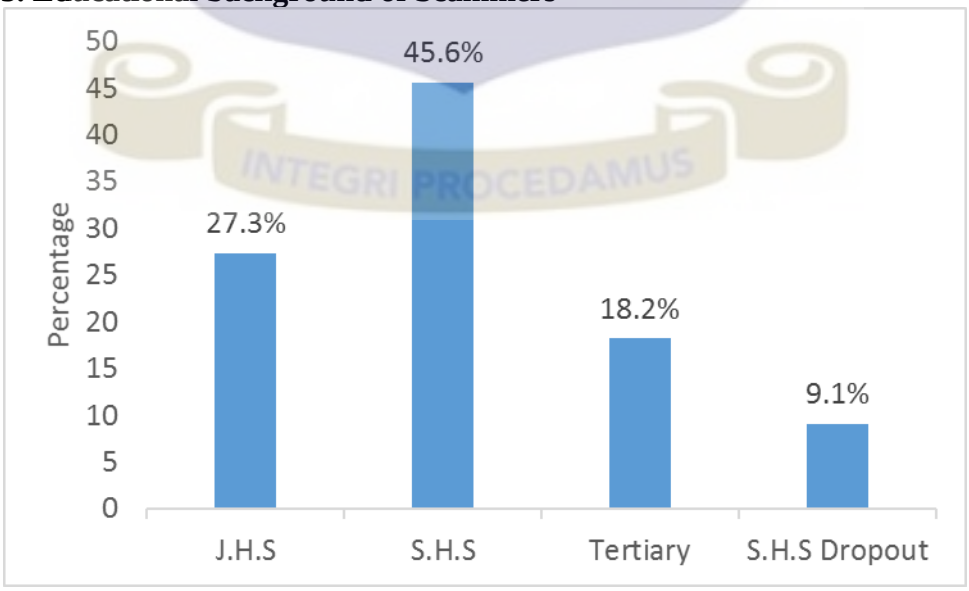
University of Ghana http://ugspace.ug.edu.gh

God blessings for conforming to the doctrines was at play. The data gathered indicated that all the respondents have affiliated to spiritual growth but they are not committed to the doctrines, and part of the explanation for this state of affairs perhaps may be attributed to fact that most of the churches are now Preaching prosperity and less emphasis is placed on salvation which ensures conformity.

4.1.3 Educational background of Scammers

Formal classroom education plays a vital role in shaping individual growth and development. Nukunya (1992) observed that formal education is an essential vehicle for the acquisition not only of wealth and power but also for prestige'. Therefore higher education gives market value which invariably put the person on a pedestal to earn a good income which in turn is a prerequisite for respectable life style and family. The individual mode of adaptation is conformity to the social norms. In views of this, the study looked at the educational background of the culprits and how it affects their daily life. The data on the variable are depicted in figure 5.

Figure 5. Educational background of Scammers



Foot notes: *J.H.S refers to Junior High School. S.H.S also refers to Senior High School*

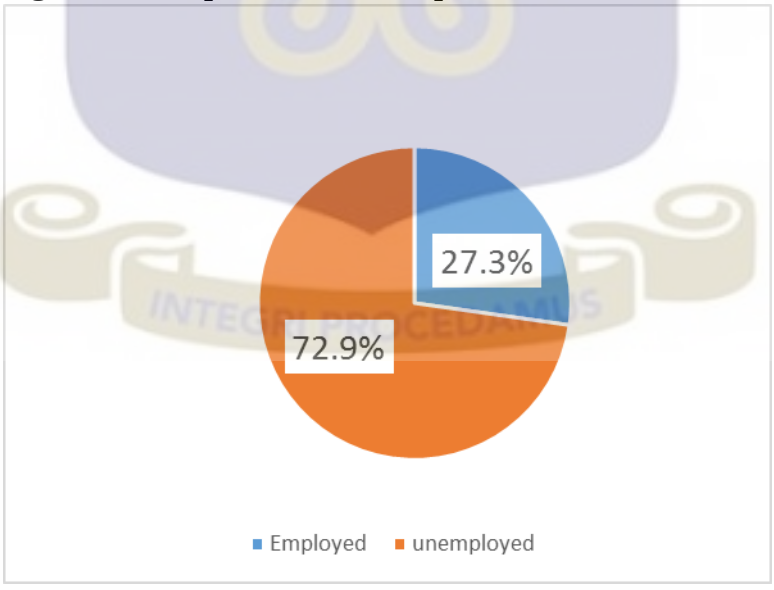
University of Ghana http://ugspace.ug.edu.gh

Figure 5 shows the educational level of the respondents. 45.6% of the respondents were Secondary School leavers whiles 27.3% also completed Junior High. One ramification is that the majority of the 'Sakawa' boys may not be in position to get a better job that can earn them a good salary to cater for their needs. So their career opportunities may be bleak. But what is noteworthy about the educational attainment of informants is the conspicuous absence of people who have never been to school as well as university graduates. In view of this, the cyber offenders are able to communicate and explore the internet for their personal gains.

4.1.4 Occupation of the Respondents

Employment plays a critical role when it comes to the criminal issues because of the general assumption that those who engaged in such deviant acts are mostly unemployed. The respondents occupation are shown in figure 6.

Figure 6. Occupation of the Respondents



It emerged from the study that internet fraud is predominantly among people who have attained some level of formal classroom education and are willing to work but unable to find payable work. The reality is that there are few job opportunities in the labor market

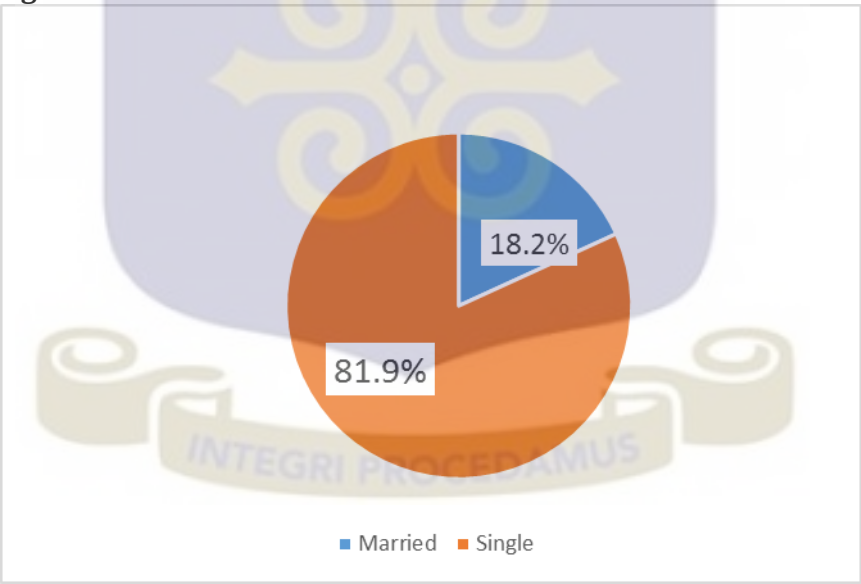
University of Ghana http://ugspace.ug.edu.gh

which requires highly skilled manpower. In this survey, 72.9% of the respondents were not in any form of employment. Even though 27.3% of the respondents were employed but these jobs are not self-rewarding from the Ghanaian perspective and this may affect their income and expenditure levels (cf. table 3 of the study).

4.1.5 Scammers Marital Status

Travis Hirschi 1969 theorized that individuals who commit themselves in conventional activities such as marriage, promote conformity to the societal norms and leave no chance for delinquent acts (cf. Siegel & Senna 1994: 195). Hence, the investigator sought to find out the accurate applicability of this statement. Figure 7 presents the marital status of the cybercriminal respondents.

Figure 7. Scammers Marital Status



It is surprising to see that those who are single and presumably with less economic burden are involved in 'Sakawa'. Ideally, the married people who are unemployed would be expected to delve into this uncompromising behavior since they have heavy financial burden. The data point out that 81.9% of the informants have not emotionally attached to any women yet and this could be a contributing factor. It could also mean that singles do

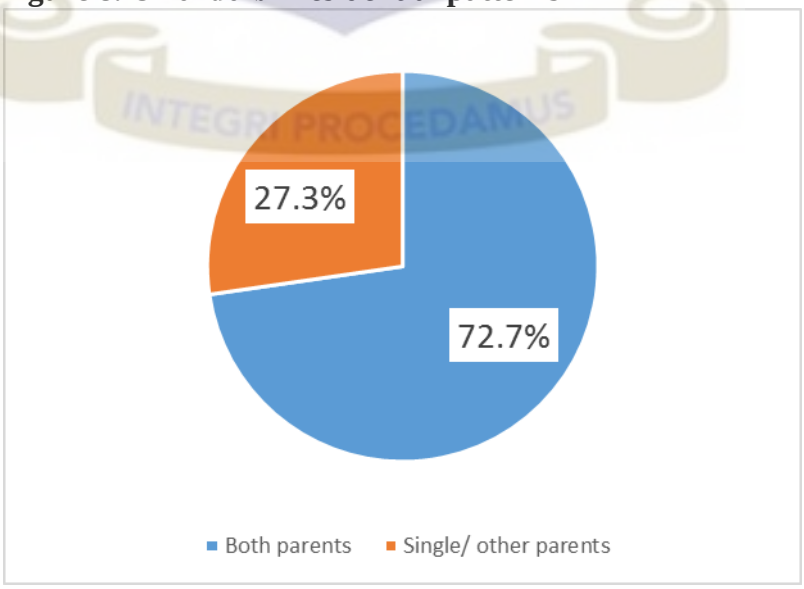
University of Ghana http://ugspace.ug.edu.gh

not have a sense of shame as they are alone. Another reason why they engaged in "Sakawa" business could be that some of them have become the bread winners of their nuclear as well as the extended families. This argument is also in tandem with the 2010 Population and Housing Census where dependency ratio stood at 43% (Ghana Statistical Service, 2013:56). The burden exert pressure on them to adopt nonconforming behaviors to achieve this goal.

4.1.6 Offenders Residential Family patterns

Families are one of the strongest socializing forces in life. They teach children to control unacceptable behavior, to delay gratification, and to respect the rights of others. Two parent household provide increased supervision and surveillance of children while single parenthood increases likelihood of delinquency and victimization simply by the fact that there is one less person to supervise adolescent behaviors (Wright & Wright 1994). So this has been in criminological cycles been cited as one of the predisposing factors of juvenile delinquency. The researcher developed an interest to probe into this assertion. Figure 8 presents data on the distribution of offenders family residential patterns.

Figure 8. Offenders' Residential patterns



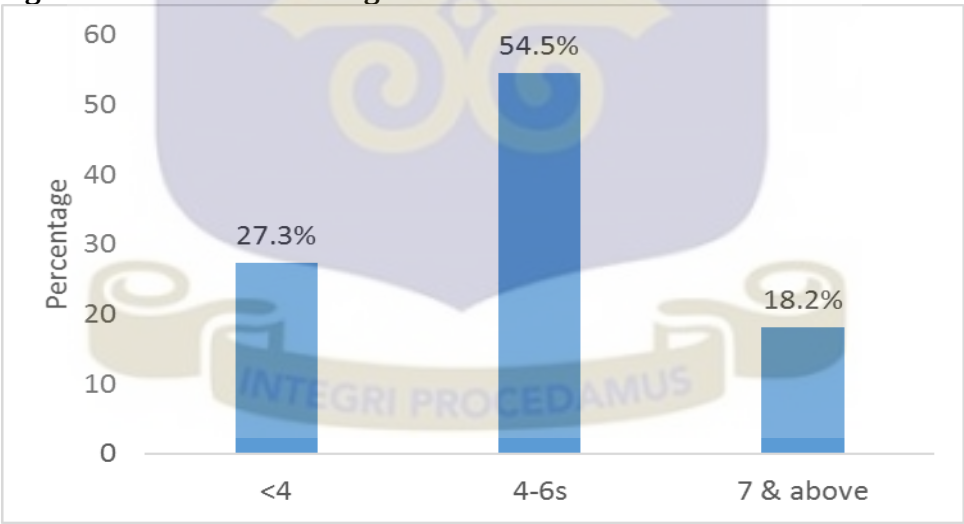
University of Ghana http://ugspace.ug.edu.gh

The data suggested that 72.7% of the perpetrators were under the direct supervision of both biological parents' whiles 27.3% lived with single parents. The results is contrary to what Wright and Wright predicted in 1994. Part of the explanation could be that when children begin to innovate to make ends meet, parents lose their moral authority to supervise them.

4.1.7 Number of Siblings

In the literature, Smith (2011) further argued that children who find themselves in the "Sakawa business" came from large families. As a result, their parents cannot cater for their needs. Ideally, these people will embrace cyber fraud as an easiest way for amassing wealth. With this in mind, the investigator sought to find out whether or not scammers came from small/large family. Data on this issue are presented in figure 9.

Figure 9. Number of Siblings



The information gathered from the field reaffirmed the Smith (2011) argument that about 81.2% of the perpetrators have more than four siblings. This meant that children are competing for the scarce resources at home and that may pushing them to commit online fraud to make a living.

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

4.1.8 Summary

This section discussed the socio-demographic attribution of the scammers. The findings revealed that "sakawa boys" fall within the ages of 17 to 30 with an average of 23 years. Almost all the perpetrators affiliated to various religious sects but they are not adhere to the doctrines which ensure conformity to the societal norms. The findings further shown that there is a conspicuous absence of scammers who have never been to school. 72.9% of the respondents were unemployed while 81.9% unmarried. The offenders' family residential patterns indicated that 72.7% were under the direct supervision of both biological parents yet they engaged in scamming activities. Large family size affected scammers' to achieve their basic needs.

4.2. The Socioeconomic Status of the Scammers' Parents

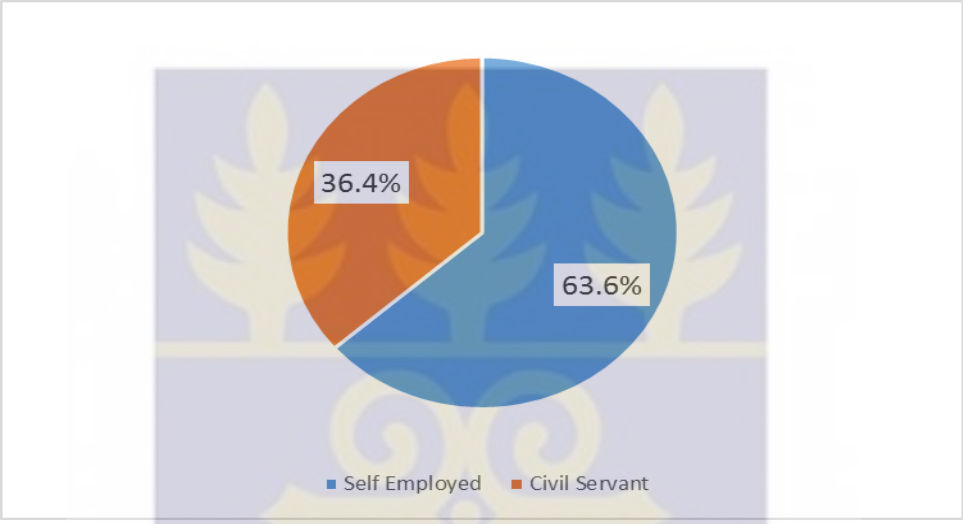
This aspect sought to examine the socioeconomic background and normative patterns surrounding the upbringing of the perpetrators, and how childhood experiences might have impacted on their current behavior. Legally, the majority of the participants are adults and they are responsible for their actions because they are more than 18 years as enshrined in the 1992 Constitution of the Republic of Ghana. However, information gathered from the field show that most of these "Sakawa boys" are still depending on their parents for their basic needs and a sense of direction. Cohen (cited in Bartollas, 1990:55), argued that parents in the lower socioeconomic class lack the resources to prepare their children for success in middle-class status. Thus, as the children repeatedly fail in life, they responded by forming oppositional subculture in which delinquency is valued positively. It means parents' economic power influence juveniles' success. So, the researcher investigated the parents' occupation and their income levels.

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

4.2.1 Parents' Occupation

Maccoby and Levin (1957) emphasized that jobs with higher socioeconomic status reward self-direction and self-control which parents' value and passed it on to their children. To assess this notion, a question was posed to learn the kind of job scammers parents are engaged in. Data on this issue are presented in figure 10.

Figure 10. Parents' Occupation



Foot note: *civil servant means a worker who receives monthly salary*

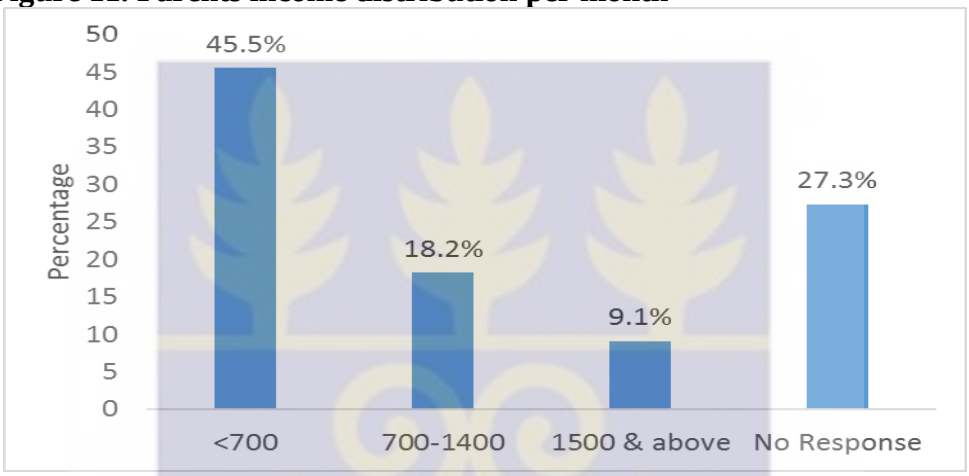
The results of this study shows that there seems to be a correlation between occupation of parents and offenders predisposition to cybercrime. This is because the majority (63.6%) of the perpetrators had their parents falling into a category of self-employed, (most of whom had limited economic gains for their children out keep). The investigator further discovered that 36.4% of the respondents were in the civil servant who and found themselves in the lower structure of their organizations with associated low wages. To the greater extent, cybercrime activities are economic issues and this gives credence to Merton's stage two (innovative) mode of adaptation of his Anomie Theory.

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

4.2.2 Parents income distribution per month

The researcher wanted to find out whether the perpetrators have fair idea about their parent's income since their income level is a hub around which other things worth striving for in life can be accomplished. Figure 11 explained the income distribution of the scammers parents.

Figure 11. Parents income distribution per month



According to the responses in figure 11, 72.7% have fair idea about their parents' incomes whereas 27.3% were not aware of their parent's income. The figures revealed that most of the perpetrators parents earned an average income below Gh¢700 per month which is not enough considering the current weak microeconomic indicators, such as the free fall of the cedi, high inflation, high cost of borrowing, and inexorable utility tariffs which are withering away the purchasing power of the parents. This supports the circular argument that poor is poor and thus has no knowledge to break out of the poverty cycle because he is less able to organize himself/herself with others of his kind to improve their lots and so poverty is self-perpetuating. The synergy drawn from the parents socioeconomic status presuppose that the offenders coming from poor homes are more likely to experience poverty and that can trap them to delve into internet scams to survive.

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

Part II: Dynamics of cybercrime in Ghana- the meaning, motivation and processes

Cybercrime is a relatively new crime in which government agencies, law enforcement bodies, business and academics have been deliberated over in an effort to come to an overarching definition. In view of this, the part two of the study focusing on scammers understanding of the concept, the motives behind their operations and the strategies adopted to co-opt the victims.

4.3 Exploring the meaning of cybercrime[20]

Discussing the meaning of cybercrime is fluid because it is an emerging crime, and that is why in the literature, Olayemi (2014) concluded that it would be appropriate to describe various elements constituting cybercrime than defining the concept. However, the German sociologist, Max Weber maintained that unlike phenomena studied in the natural sciences, human beings have important qualities like thinking and feelings, and as such, these need to be connected to their social actions. (in Giddens, 1994:709). This approach to attempting to comprehend social meaning of behavior and actions is known as *Verstehen* which is the German word for understanding. For Weber, the concept of *Verstehen* is the interpretative understanding of social action, and it involves the researcher looking not only at the individual actor but also understanding the larger culture in which the actors exist which constrains their thoughts and actions. After an exhaustive interaction with the "Sakawa boys", the investigator came to the realization that there is no unified definition for the term and the scammers understanding of the concept is based on the purposes for which they are utilizing the internet. To Doe, (scammers), Sakawa means; "disguising yourself for personal gain. I for instance, disguised myself to be a woman and then chat with other males online". However, Ayiteh (scammer), looked at it from the market value

[20] The Respondents are identified by their pseudonyms, and can be found on Table 3

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

and explained that "when we talk about internet fraud it is about stealing someone's credit card details and using it to purchase things online". Ken (scammer) on the other hand, took us a step further and argued;

> If I would be much more elucidative, the perspective that the Whiteman has given to cybercrime is different from what we the 'sakawa' boys know it to be. The main motive behind cybercrime is fraud. Fraudulency means you are deceiving someone online and everything you are saying is plausible but within you it is false.

Figo, also posited that;

> The common name for the cyber fraud in Ghana is 'sakawa', a Hausa term which literally means 'putting inside' but technically it represents the act of deceiving someone with the intention of gaining some financial benefits or any form of assistance.

Even though there was no uniformity about the definitions, there are observable similarities. All their actions come into fruition with the aid of computer and internet. Thus, a common theme in most cybercrime operations is the defrauding of victims for profit, be it economic or social.

4.4 Motivations that Predispose the Offenders into Cybercrime

The love of money, according to the scripture, "is the root of all evil" (1Tim. 6:10, KJV), but as hard as we try, everybody needs it and much of it too. Nobody was born a criminal, society turns people into criminals as they grow. We see a lot of flashy things around us and naturally we are drawn to them and we pray to have all of that, so there is always a threshold everybody wants to achieve. But no matter how successful you want to be in life, there are rules or institutionalized means such as getting formal education, working hard, disciplining oneself and perseverance to achieve the material things worth striving for in life. However, it seems the Ghanaian youth nowadays rather prefer the easiest way out to make money and one of such ways is internet fraud. Therefore, the researcher was curious to find out the motivational factors that predispose the youth to engage in sakawa

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

"business". The respondents provided several reasons but the recurrent inspirations for engaging in cyber fraud included the lack of job opportunities, inadequate legal framework, anonymity and accessibility. These motivations are explored further in order to achieve the second objective of the study.

4.4.1 Employment opportunities.

Work is a fundamental law of creation for the preservation of life. It gives individuals in society certain status and recognition, which means that work is a societal requirement for social respect as well as the survival of society. It is an observable knowledge that economic factors play an important role in the evolution of crime trends. In analyzing the socio-demographic characteristics of the cyber offenders, it was revealed that more than 72% of the participants were unemployed in spite of their educational achievements. Employment possibilities are precondition for "sakawa boys" to attain their physiological needs. Conversely, unequal economic opportunities exacerbated by stark developmental fundamentals compelled some of the youth to engage in nonconforming behaviors to make a living as articulated by the sociology scholar Rober K. Merton (cf. Schaefer, 2005:182). To buttress this argument, some of the scammers had this to say;

Yeboah

> Sakawa is not something evil, but some people see it as a bad thing. Sakawa is also helping especially the youth because some of us can not earn monthly pay to survive. So we use it as a career or source of income.

Fred reiterated; "Some of us come from poor home and we couldn't get support from anywhere. So when the idea of sakawa came, I can now feed myself and look after my younger brothers".

Ken looked at the purported benefits beyond the individual level, and he explained that;

> Sakawa is helping Ghana's economy to grow. The mysterious increase in inward remittances and cash flows over the years may have been partly as a result of significant number of fraudsters

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

> receiving remittance from the clients and pals via taxable wire transfers. This may also have accounted for a certain level of stability of the local currency. Even now, I don't request for money because of security issues. Instead, I tell my mugu (girlfriend) to send me phones/laptops, so all these expensive phones you see around, a lot of them are the product of sakawa business, and is good because it is helping people to afford things otherwise they couldn't buy from the original stores in the State (European /US market).

Over the years, Ghana has experienced economic downturn and successful governments outlined an austerity measures such as structural adjustment, deregulations, and retrenchment of workers to improve the fiscal policy. The latent function is that the practice has increased unemployment and other social upheavals. Enterprising individuals especially the youth, devising many fraudulent schemes to raise funds to cushion their economic hardship. Later, justification is given to the illegitimate acts and that is why in the narrative Yeboah claimed that 'Sakawa is not something evil because it is a source of employment for the youth'. Ken neutralized his unofficial behavior to the general public that "Sakawa" is a means 'through which people can afford quality things otherwise they couldn't buy from the original supermarkets in Europe'.

4.4.2 Anonymity

Another key motivation is the fact that technological revolution and the increasing use of internet has created new phenomena that are notably distinct from conventional crime. While people do not live in cyberspace, they visit and exit at their own free will, given the very dynamic nature of cyberspace such as the ability to publish a website and subsequently remove it very quickly. There is a lot of difficulty in determining the location of these crimes and it has created a "safe heaven" for the criminals to continue attacking innocent people in cyber space. On the side of Cosmos, a 22 year old internet fraudster is worth re-echoing to authenticate this assertion. He confessed; "in the sakawa business, your identity must be unknown". When the investigator probed further about how one personality could be anonymous on the internet, he remarked;

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

> That is the issue. We have some dating sites for example, big and beautify people (bbp.com), senior people meet.com, black people meet.com, and Christian mingle.com. But before you can chat with the person you have to register on that site. One funny thing is that you cannot use Ghana's Internet Protocol (IP) address to register on these sites because the Web administrators don't accept IP address from Africa. They know that most Africans are scambacks so you can't register there and you must not be there (that web sites) in the first place. However, certain applications (software's) like Virtual Private Network (VPN) and the Proxy can break the kernel and you can hijack into the data base and finally register. During the registration process you can opt for different name and locations, like the Britain or US IP address and that could be displayed over Ghana's information. So their system cannot track that you are chatting from Ghana.

This revelation supports Middleton's (2002) argument that computer allows criminals to operate wherever they wish to venture. As the new peril, scammers can come into our homes, businesses or secured government and military bases without being physically seen. They can wreak havoc of changing formulas, designs, altering financial data and obtaining copies of vital documents without your knowledge. In the online environment, the researcher appreciated the fact that there is a "geographical switch" where the perpetrators pretended to be living in Europe or the United States of America. The proxy software's enables criminals to hide/change their geographical locations.

4.4.3 Inadequate legal framework

Traditionally, legal jurisdictions involves territory, with the scope of the country's being defined by the limits of its boundaries. This territorial notion is ineffectiveness to prosecute cybercriminals. Determining where cybercrime is committed can be difficult, since the perpetrators and the victims can be located in different countries. Also, the perpetrator may utilize computer system in several countries in the course of attacking victim and this poses a challenge for the security personnel to apprehend the offenders. When interacting with the respondents, majority mentioned the poor legal regime as a motivation for engaging in the crime as Doe revealed; "stealing something physical can be dangerous because you can be arrested by police or people around you, but with the internet, it is easy to get away with the act". During the preliminary enquiry, the researcher

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

had the opportunity to interact with the Director in-charge of ICT at the Ministry of Communications and he emotionally asserted;

> Though the print and electronic media have increased the awareness of cybercrime, there is no law dealing with the issue. Recently the Ministry embarked on operations and we arrested sim box fraudsters but later they were acquitted and discharged. The judge argued that the prosecutor could not established the prima-facie (adequate facts) to support the case brought before him. The judge further bemoaned that the Criminal Offences Act (Act 29/60) needs to be amended to embrace the hi-tech crimes. So all our efforts to thwart the perpetrators became fruitless.

In the constitutional society, laws are enacted to regulate how citizens must live. As Ghana strives to become knowledge economy, it is extremely important for the nation to implement policies that will promote legal certainty in the cyber world. Law enforcers operate on the legal principle 'no crime without law'. Thus, if cybercrime legislative instruments are inadequate, it demoralizes government agencies to fight the menace as posited by the respondent that 'all their efforts to thwart the perpetrators became fruitless'.

4.4.4 Easy access to Internet

Gone are the days when the only way to communicate with someone was through the telephone (fixed line), mails, or directly. These forms of communication made it difficult for people to scam. At that time, most fraudsters were more confident tricksters who used ways and means to dupe their client. One major disadvantage in this way of scamming is your presence at the scene which could be easily identified. Now, the penetration of laptops, and smart phones applications allow individuals to send messages and get quick response which give them room to outwit and convince people to do their bidding. According to the respondents, a minimal capital was required. In most cases, the availability and affordability of internet cafes and only few equipment needed like webcam and voice recorder to capture some of the conversation, serve as inducement for the individuals getting involve in the 'sakawa' business. To cross check the cost of

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

browsing per hour, the investigator visited the Busy Internet and Vodafone Internet Café, and the prices ranged from Gh¢1.50 to Gh¢2. To my surprise, all the respondents were in agreement that it was relatively cheaper considering the fact that the retention rate could be very high.

4.4.5 Summary

The findings of the discussion show that the meaning of cybercrime is culture specific and individuals understanding of the concept depend upon the purpose for which they are utilizing the internet. The study further discovered high rates of unemployment, anonymity, inadequate legal framework and easy access to internet facilities are factors motivating the youth to engage in internet scams.

4.5. The Modi operandi/the process of becoming internet scammer

After an intensive interaction with the internet scammers, it was found that there is no standardized methods of operations. They adopt varied degrees of tactics to swindle, coerce, and hypnotize their clients to relinquish their wealth. However, there are some recurrent patterns of behavior fraudsters employed and these schemes are presented in the next sub-sections.

4.5.1 'Sakawa' is learnt behavior

This nexus was rooted from the great sociological thinker, Edwin Sutherland that criminal behavior is learned in the same way as law-abiding values are learned through the process of differential association. The learning activity is accomplished in the interactions within intimate groups.

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

The simple explanation then is that some young people engaged in sakawa because some friends or close allies were into it. Thus, as they "roll" together, the "sharpening of iron by iron" takes place. They get awed by glitz and glamour friends present and end up being wooed into practicing sakawa. In fact, that is one of the very popular ways by which most young people get into the act. During the interview, Doe admitted; "I engaged in sakawa when I was in secondary school. I learnt it from my friends and they even created the email account for me, and forwarded some materials that enabled me visit some "pono" sites".

Narrating his story on how he became a scammer, Ayiteh explained;

> I don't know but I will say peer pressure. Way back in JSS, I had a friend who was doing this and anytime we come to school he shows flashing things, and moreover he was my close friend. So we moved together and later I just decided to be like him. In the beginning, I didn't know that the whole business was a scam. So we were doing like register with a site, get some people, talk to them and when your luck shine you get something out of it if not then you have to endure and stay in it.

Ben (scammer), disclosed that he became internet fraudsters by accident.

> One day, I was in the house and I had a call from my friend that I should come to the café and assist him to attach a document to an email message that he wanted to send to a friend in Germany. After sending the email, he requested that I should give my bank account number to him because his friend is sending him money from abroad which I did. Three days later, he called that the friend had sent the money. So we went to the bank and withdrew the cash, totaling Gh¢6800. He dashed me Gh¢600 out of the total cash. I was very happy but he confided in me that it was sakawa deal. He started telling me about the money so far realized from this "business". I developed interest and he taught me how to answer questions, sending and replying messages and all of a sudden I became an expert. Thereby earned a total of $1900 from the business.

When non criminals interact frequently with criminals, the tendency of that person becoming criminals is very high because during interactions ideas are shared, especially when the criminal is a close friend or a friend to the non criminal. This is because the principal part of learning occurs in intimate groups where there is frequent communication and once the behavior is learnt there is a desire to practice. The evidence gathered from the ground suggest that the majority of cyber fraudsters learnt the act from their

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

contemporaries. So parents should monitor their children about the kind of friends they associated with, like the adage goes, 'birds of feather flock together'.

4.5.2 The Process of Registration

Technological advancement has created another society for mankind. To become part of this hypertext world, one has to open an electronic mail account. This email will help you connect to the social networking sites like Facebook, Twitter, and many others. These social webs create a platform for people to compete and abreast with current issues in the global environment. Background information and profile pictures are some of the requirement for the registration process. It informs people in the cyberspace about your interest, weakness, achievements, and this is where criminals also take advantage of posting false materials on the internet and exploit "cyber citizens". Doe admitted;

> Though I am a man, when you visit my profile, you will discover a white lady picture. The truth is that no Whiteman wants to marry black person. So is like I will give you what you like and get what I want.

Ken, an internet fraudster unveiled;

> In the sakawa business, we called something format; that is police format, soldier format, nurse format, business format, and the most popular one is gold format, especially when you are in Africa.

These formats are social engineering strategies, fraudsters adopted to update people about the kind of job they are doing which in actual fact is a hoax.

4.5.3 The process of engagement

After the registration, the whole "business begins with the sending of a number of email messages to the numerous recipient around the globe. The electronic mailing enables the perpetrators to reach many potential victims within a short time. The information sent out there must be persuasive as noted by Ayiteh;

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

> The information you are sending is about you. So you write sweet words about yourself; is like I am gorgeous, smart, intelligent, etc and post it into your email account. So when the person read your profile and he is interested, he will send you a friendly request. You reply him, and as time goes on, you start sharing ideas and pictures.

On the other hand, some scammers send a friend request based on the person's achievement. Rauf (scammer) argued;

> Categorically, every scammer has a taste/interest. When I go to the internet, I look for people who are estate developers, a nurse, medical doctor, person working in automobile company, or an individual who has a long term financial security. For instance, if the person is working in the automobile industry, the tendency for him making about $4000 a month is very high, and I will target him/her.

This assertion is in tandem with the Cohen and Felson (1979) Routine Activity theory which states that individual behavior facilitate criminal action. The investigation revealed that scammers go after individuals who posted sensitive information on their social networking sites and they serve as bait for the fraudsters to garner intelligence about their daily activities.

4.5.4 Process of defrauding a victim

Although information channeling out by the conmen are false with intent to defraud, some people have a tendency to reply them. In life, communication brings trust and commitment. When these elements are established in the relationship, there is a zeal for the partners to impress upon each other, and that is where "Sakawa" boys take advantage by telling their problem or put in some business proposals. Notwithstanding the strategy that is used, the fundamental principle is to gradually drain the wealth of the victim over time. Figo (scammer) further explained;

> When you send the friend's request and the person replied, you exchange contacts (mobile phones or private email). It means that the friendship has been established, and from there if you think the person can offer some help, you bring in a business proposal that can earn you money. That is the scamming aspect of the internet fraud. Initially, I will say I have a land full of gold. Before I can extract the gold from the soil, I need an excavator, registered license from the Land Commission and a Certificate from the Mineral Commission as a gold dealer. So getting these may cost about $80,000. The client will request for land pictures and other documents that will make him feel like this deal is real, and we falsify these documents and email to them. When he is convinced, then he starts releasing the money bit by bit because at each stage you have to update him about the progress of the work. This trend will continue until he comes into his senses that the transaction is fake and at that moment, I will be okay to cut ties with him.

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

Scammers almost always initiate communication with the victims. They make unsuspected victims believe that they have a strong feeling for them. As time goes by, fraudsters established a strong bond with their victims to generate trust, confidence, and romantic liaisons. This psychological strategy can last until the desired trusted-level is achieved. The next stage is where the scammer request money from the victim by chipping in some business proposals. The more successful the scammer is convincing the victim about the profitable ventures, the more the victim is lure into the scam. This 'cycle of lure' continues until victim lose hope on the deal that is why Figo, revealed, 'when you bring in a business proposal and he (victim) is convinced, then he starts releasing the money gradually and this trend will continue until he comes into the realization that the transaction is fake'. Given the amount of time and effort undertaken by scammer to set the groundwork and establish trust, Cukier and Levin (2009) explained that it takes time for many online victims to realize that they have been scammed, making this activity profitable for scammers.

4.5.5 Summary

Cybercrime is the art of learning and the learning activity is accomplished within intimate groups. The perpetrators adopt varied degree of modi operandi to bait their 'client' through online registration, and process of engagement. In an attempt to connect to the cyber world, personal profile is a precondition for registration but criminals take the opportunity of the virtual internet to impersonate other people's identity to commit crimes. Besides, they persuade their 'clients' with some cache words. In relation to the 'process of defrauding a victim', scammers win the trust of the victim before asking for other assistance.

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

Part III: Stakeholders in the cybercrime industry in Ghana- Scammers, Victims and law enforcement agencies

Cybercrime presents a daunting challenge to all facets of human endeavors because there is no boundary in the cyberspace to limit people's behavior. As a results, more and more criminals are exploiting the speed and the convenience of the internet to commit various crimes which pose real threat to the victims. But to understand the complexity of cybercrime industry in Ghana, the researcher broadening the scope of the study by looking at opportunities explored by criminals to commit cybercrime as well as victims who narrated how they were conned. In addition, effort was also made to enquire from the Police and the Judiciary about their readiness in responding to the situation. The next subheadings expatiated the discussion.

4.6. Opportunities explored by fraudsters in their operations

Castells (2000) claims that we are passing from the industrial age into the information age. This historical change is brought about by the advent of information technology, and the traditional social institutions are withering away. The network society has created a single platform for instantaneous encounters between spatially distant actors. Individuals are also exploring the possibilities for ever-new forms of association and business exchanges. However, criminals have taken the advantage of this knowledge base society to promote their nefarious acts. So the investigator developed key interest to enquire from the scammers about the various opportunities they explore to reach their potential victim on the internet. The discussions revealed that most fraudsters take the opportunity of gold market, romance, business and internet shopping to co-opt their partners. The next sub-sections present discussions on these four themes.

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

4.6.1 Gold fraud

Ghana is blessed with the abundance of gold ore and sakawa boys are utilizing this opportunity to advertise fake gold products on the internet. Most of the victims in gold fraud are foreigners. As the Akan proverb goes "ohohor ani akese nso enhunu adie" literally meaning "a stranger's eyeballs are big but it does not see". A lot of foreigners perceive Ghana as place where gold is "a kicking object". This is due to the country's name before independence as Gold coast coupled with the operations of mining giants like Newmount Ghana Limited, AngloGold Ashanti and other medium mining companies. As narrated by Ken;

> Like I told you earlier, during the registration, I opted for a gold dealer 'format' because the White people know that in Ghana we have an excess of gold so the tendency for someone to trade in gold in Ghana is very high. Moreover, this makes it possible to trace and obtain a list of gold dealers email addresses from the web.

In the gold scam, there are several schemes adopted by the fraudsters to scam the investors; some are into production, buying, and smelting of gold into bars as an avenue to make money. They offer competitive prices which are far below the World market price. They generate fake licenses of Mineral Commission, Precious Mineral Marketing Company (PMMC), Geological Survey Department certificates of ownership, Affidavit and other documents to convince their unsuspecting victims. After the client has paid the initial deposit for the consignment, a story is then fabricated to explain a major setback that has affected the export or the delivery process which may also require extra fees. This unending strategies would be continued until the client becomes frustrated by which time a colossal amount would have been realized by the scammer.

4.6.2 Romance fraud

Online dating is now one of the emerging ways by which people start a relationship. Many husbands and wives discover these romantic sites as an alternative to the traditional way of

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

finding suitors at social gathering like festivals, funerals, churches, work places, and tertiary institutions. The internet has added glamour to the whole idea of courtships because partners who are far away can talk to each other live through the webcam application. Bored lads and lasses can sail into any of these fantasy world to soak sweet words from their lovers.

On the other hand, charlatans have also mingled with this romantic paradigm to outwit their partners and in the end defraud them. It is one of the common socially engineering practices 'sakawa' boys use. People who patronize dating websites abroad are usually susceptible to this type of fraud. The romance fraud is popularly referred to in Ghana by 'sakawa boys' as 'come and marry', and according to Ayiteh, "come and marry is a situation where a desperate man in the State (US or Europe) wants to pick a woman in Ghana and we do everything possible to bring him down". Some of the dating sites the researcher discovered from the field are ChristianMingle.com, mingle2.com, seniorpeoplemeet.com, blackpeoplemeet.com, bigandbeautiful.com, upforit.com, flirt.com and match.com. Doe observed;

> These sites are advantageous because it is not everybody that gets access to them. But if you don't have credit card, you cannot chat with those over there. We called some people hackers or scambacks and they have access to a lot of people's credit card information. So we use our 'Liberty Reserved' account to pay hackers online. The Liberty Reserve is a form of currency to hackers internationally. The scambacks generates the credit card and email into your email account and that allows you register at the dating sites.

After the perpetrator has succeeded with the registration, he then advertise on the website pretending to be woman seeking a partner. The investigator had the privileged to access two of the respondents' profiles and Cosmos wrote;

> **I am looking for the right man**
>
> When you meet me you will see that I am a kind and very easy-going person. Friendly, responsive, always ready to support, listen, amuse you, I like jokes and laughing. I am a bright girl and very playful, very kind and self-loving. I can tell you secret. I am very tender, like flower of violet. I'd like to meet someone kind, honest and caring, preferably without any bad habits, in good health and

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

> ready to start family. I also hope that this special man will be optimist and sociable, with good sense of humor. My goal is creating family with warm relations, based on mutual respect, understanding and trust so I'm waiting for the adherent to start the process.

Fred also posted;

> **I am very simple woman and also very serious in life. I am looking for soul**
>
> I am a nice woman, caring, honest romantic, submissive, loving and faithful. I am open hearted and have much love to share with an honest and serious man with no games. I will make sure that I treat you with love, respect, affection and obedience, always be honest and faithful to you. I promise you that you will never regret a bit falling in love with me, because you will have all the feelings that will make you feel ran and with my love close to you will never ask for love from any woman. Am a young lady who like to walk with my man, visit new places and really enjoy making kisses. I am feeling very lonely here and I need a man with love, caring and handsome like you to make me happy, this is the right time for me to share my love life and fantasies with a man and you are the right man for me, my heart is open for you today and forever. Write soon and I will reply you with sweet part of my heart, bye.

Interested dating partners reply with their email addresses and sometime live chat videos from the website. It is often said that love is blind, this makes a romance fraud complicated, because at the initial stages, victims view and treat their relationships as a private affair and thus find it unnecessary to discuss with any third party. After the fraudster has endeavored to establish relationship with the victim under the purported love, the fraudster would resort to any of the following tricks to extort monies and other items from the victim;

1. Financial support to take care of sick family member (mother, father, or sibling)
2. Money to pay school fees
3. Request for laptop computer, digital camera, mobile phone, etc.
4. Money to buy property such as an estate house and land for the benefit of the two parties.
5. Money to facilitate a trip to join the partner
6. Money to bribe law enforcement officers for being involved in one offence or the other.

In addition, the findings also suggest that some scammers combined the two modes that is romance fraud plus gold fraud to deceit their client; what I called the "roma-gold fraud".

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

This happens after the romance fraud has been executed to its apex, and is no more effective in extorting money from the victim. The perpetrator would proceed to introduce gold deal, either by mentioning the availability of family gold or less expensive gold. Any show of interest in the gold deal by the victim would mark another beginning of demanding for money ostensibly for the purchase and shipment of gold to the victim.

4.6.3 Online shopping

Many companies in the traditional business environment were unable to sell their goods or render services directly to consumers. Companies dealing in manufacturing and the intermediate goods have to hire the services of middlemen to advertise the product in the real world. The internet revolution allows these companies to set up a business website to market their goods without the services of others. The prospective buyers need to be hooked to internet banking where one's account is linked to the credit card payment system which contains his/her personal identification number. The credit card holder can utilize it to order goods and services online, but sakawa boys have infiltrated into this business echelon. Criminals use victims' credit card to purchase items including expensive vehicles and household items which are subsequently shipped into Ghana. The imposters are able to operationalize their activities without physically possessing the magnetic stripe which stores the account holder's information. The software applications and internationally criminal networks organizations aided the fraudsters to generate credit-card numbers using the same algorithms as the ones used by the banks. Figo (scammer) explained the mode of operation;

> You see, the internet and its security are made by man. People go and learn about computer networking and hacking. In the U.S Central Bank for example, some people can hack into their system and obtain credit card numbers. With the aid of "liberty reserve account", we purchase the credit card details from the scambacks and these include; the user account number, name, age, pin code and the expiring date. So after the card had been generated, I use it to order goods from these international supermarkets. The procedure is very simple. The shop attendance will request for your

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

> credit card number and feed it into their data base, when it is genuine, they would just take out their money and deliver the goods to you. Besides, we contract agents to facilitate the shipment process.

Over the past decades, global action has been required to address challenges such as illicit drug trafficking and other international organized crimes through the development of international agreements. Nonetheless, it has become truism that cybercrime today also presents a unique challenges that need global solutions based on universal laws and values to fast track the rendition and extraction of perpetrators. No country can solve cybercrime problem on its own, and Figo's narrative has shown that he 'purchases some of the tools and methods from other criminally minded people in different jurisdictions to aid the commissioning of the credit card fraud'. Ghana law enforcers have limited power to apprehend Figo accomplices even if he tells the truth because international treaties admonish that every sovereign country is independent from others.

4.6.4 Collaborations with Security Agents and Financial institutions

Security agents are protective organizations, but when the same law enforcement agents become partners in crime, it raises a source of concern. The criminals are able to take the opportunity to further exploit individuals online. The informants describe Ghana Police Service and Ghana Immigration Service as accomplices. Some corrupt police officers serve as informants in providing useful information that prevents their possible arrest. The Immigration officers also aid offenders by providing residential permit to authenticate their nationality status. Moreover, some bank officials or money transfer agents also connived with the perpetrators by assisting them to withdraw the money they have realized at a fee, whereas the postal agents help in clearing goods in exchange for compensation. Cosmos noted;

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

> In order to be successful in this 'business' you need to be an influential person. Internally, we call something 'document'. In everything you need some information to support your action. You need to employ a graphic designer, you need someone who knows certain personalities in Ghana; like police guys, and bank managers. The one who is designing for you is going to charge you directly. A guy leading you to the police or bank manager will charge you 10% of the money. The manager is also going to charge either 10% or 20% of the booty depending on the bank you are dealing with. We bribed police officials to obtain a copy of police report to confirm that you are a Ghanaian dealing with gold business. At times, the client can send the money through Western Union, but that one you need personnel within the company (Western Union) who understand scam, so that they would forge an ID for you. What they do is that, they have genuine Ghanaian ID numbers which people normally use to withdraw money from their office; they would just put off the person's name and replace it with your name and that is all.

Doe, also recounted his experiences with the Western Union staff;

> If the money is not enough, may be $100, the bank will not request for anything. However, if the money is huge, for that one it requires for special arrangement, and that is where you need to contact somebody at the bank. I remember in 2010, I encountered such problem at the western Union. I hit an amount of $8000, so I went to the bank to withdraw the cash but one of the officials at the counter was asking me a lot of questions. Quickly, I pretended I had a call and walked out from the banking hall. I called my friend and briefed him about the issue. He drove to the bank premise and introduced me to one of the staff. We stroke the deal and in the end I bought her a Toyota Matrix saloon car after she helped me in other deals. My friends used to tease me whenever they see the car around.

Without a doubt, bribery permeates almost every strata of public life in Ghana. bribery occurs when a gift, or a valuable consideration given in cash or kind to a person occupying a position of trust with the intention of influencing him or her to act in a way favorable to the interest of the giver (Abotchie 2012: 147). The internet scam has reached level where bank officials, police, and post office administrators have been compromised with kickbacks in lieu of the presentation of correct documents to support sakawa boys to withdrawal the remittances received from their victims abroad, as narrated by Cosmos and Doe. If this misconduct continue, it would create an administrative bottleneck to fight cybercrime in the country.

4.6.5 Local and International networking among the perpetrators

Cybercrime perpetrators are very dynamic, as the crime is difficult to commit alone. They, therefore, need both local and international collaborators to make their deal easy. The Majority of the culprits revealed that they have both local and international associates who

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

shared their dreams. Local networking is necessary to acquire more knowledge and skills, especially when dealing with difficult client; whereas the international networking is useful for easy credit card top-up, internet shopping, shipment of goods, and a cloned credit card generation.

Some views articulated by the scammers are highlighted below: Reginald explained;

> I don't have friends outside the country but I have a lot of friends here and we share ideas. For instance, when I meet a 'stubborn client '(difficult person), I contact some guys, we will discuss it, and I take it up from there.

Yeboah admitted;

> This romance scam had helped some of our friends to travel to Europe and America. So we share ideas, like money laundering, someone's bank statement and credit card top-up (cc top- up, that is stealing money from someone account to another). Our friends do it outside for us because it is easy over there than doing it in Ghana.

Ayiteh also noted:

> The people who normally give out the credit card are from Vietnam. The hackers take money but the Vietnam man will not accept the local currency. They have a web site where you can purchase a software in the form of dollars called 'Liberty Reserve'. So when you buy the LR, they put it into your account, and later you also transfer into the hacker's account. The hacker will send you the credit card details.

These exposé supported Castells (2000) Network Society theory which explained that the diffusion of society has modified the operations of organized criminal groups in the globe. The flexible communication gadgets enable cybercriminals to communicate over vast distance and integrate diversified interest. The scammers utilize the internet to achieve their criminal goals. The sophisticated nature of the crime requires a lot of stakeholders such as the bank officials, police officers, friends, and internet expertise to accomplish the deal. As these players are coming on board, the crime developed into dominant interest or ideology known as "Sakawa".

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

4.6.6 Summary

The section has been looking at the comparative advantage scammers explore to reach out their potential victims on the internet. The information gathered discovered that "Sakawa boys" utilize Ghana's reputation in gold business to deceive investors on the internet. The E-love network has created an alternative medium for new romantic endeavors. However, this global industry has become avenue for cybercriminal activities which poses serious threat for online daters worldwide. The spatio-temporal nature of cybercrime requires a lot of criminal networks before fraudster can execute the act. The study further found out that some security personnel, money transfer outlets, and postal service administrators are collaborators of cybercrime industry in Ghana.

4.7 Resort to Occultism

Initially, the researcher did not focus on the spiritual dimension to the issue because this assertion cannot be explained from the scientific procedures. However, I discovered from the field that some of the perpetrators consult their spiritual fathers before they commit themselves' into this activity. The understanding of cybercrime dynamics in Ghana is quite different from the traditional cyber fraud known in other jurisdictions because of the alleged spiritual paradigm which informs the scammers' world view about the issue. Figo's (scammer) explanation supported this point that cybercrime is 'any fraud type such as lottery scam, auction, and romance scam. But once you attempt to woo your client through spiritual coercion then it moves from the realm of ordinary fraud to what we call "Sakawa". So it is the merging of 21st century technology and perhaps an old-age African traditional practice'.

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

Most Ghanaians believe in supernatural charms and mystical forces for success in many endeavors. This belief has been appropriated by sakawa boys to achieve their results. The reactions observed from the informants revealed that most of the rumors were indeed, a reflection of the reality. Fred, answered the spiritual question in a philosophical puzzle and it would be useful to quote him verbatim;

> Though I am a Christian, Christians believe that we have two worlds; that is physical world and the spiritual world. The spiritual world controls the physical world. So we commandeered the spiritual world to fast track the process for us.

Rauf confessed;

> The occultism exist for real, I have used it but I have stopped because of the fear of repercussion. With the aid of spiritual power, the money come fast. I have a friend who uses shear butter to smear his body and says incantations in his room, and he can receive money sometimes thrice in a month.

Reginald posited; "I seek spiritual guidance to help me get something out of this scam activities. I believe in black magic and it really works". Ben observed, "The spiritual aspect helps the client to be stable even if the person knows the deal is a scam". Ayiteh also explained;

> The spiritual motive is not limited to traditional charm alone. Way back, I used to consult Malams and later one Pastor. But now I have stopped because it got to the point where the requirements for the rituals were too much.

Other informants said they did not subscribe to any mystical powers/ prayers but agreed that they knew those who did and did not see any problem with it. Thus, the assurance that someone will necessarily respond positively to a scam message, that one is more likely to maintain anonymity and therefore annul all attempts by the security agents to arrest the offender provides a fertile ground for sakawa boys to resort to the occult practices.

Furthermore, I discovered from the informants that those who engaged in occultism performed certain rituals, including offering parts of their body for sacrifices. Some of the human parts allegedly offered for sacrifices included left finger or the right toe. With the left finger, the sakawa boy is instructed to wear a ring and never take it off. If the person takes the ring off without necessary rituals, he will go mad or in the extreme case, die.

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

These sacrifices are in stages, with the majority instructed to fast for 30 days without taken in any solid food, plus other spiritual directions. Others chew fresh meat such as mouse, black cat, and reptiles like lizard. A person's level of sacrifices determines how rich and wealthy he becomes.

One would think that after performing all these sacrifices, the money would begin to flow for these young people, but that is not the case. Most of them have to endure seasons of waiting to see their martyrs bearing fruit but some even have to wait for more than a year. This means that they have to depend on friends and family for assistance. Others receive support from their mentor "sakawa men" who have already made it. In an interview with Cosmos, he narrated how hard it was for him to wait for more than a year before his rainy days began.

> After I performed my rituals, which involved chewing the fresh of Cat for six days, I was further instructed not to bath for another six days. I also slept in darkness for two months". I nearly gave up because the instructions were too much to bear. And the money too was not forthcoming. So the year in which I performed the rituals, I didn't see top [nothing happened] until somewhere in March, 2012. My friend who is now in Libya supported me a lot and even paid some of the amount demanded by the Mallam.

Although he did not disclose to the interviewer how the money started coming, he mentioned Gh¢23,000 as the first amount he received from his client. This is the part where pain is quickly forgotten and sudden joy takes over. So a follow up question emerged on how the scammers spend their monies. Unfortunately, most of these young guys do not put their money into any profitable ventures. Ken confessed; we have a term called "chicken feed" (which means spending extravagantly) and it is a good sign of showing appreciation by organizing parties, chasing women, acquiring expensive cars, buying iPhones for friends who helped you during your "broke days", and before you realized the money is got finished". Ayiteh emphasized; "these monies never went into any lucrative business. It was just for my stomach and the things I wear". Yeboah; "I use the money for clubbing and other stuff". Nonetheless, Doe has managed to put up five bedroom apartment in Accra. One unique attribute about sakawa boys is that they would never turn their back on their own, especially when the person is hit by unforeseen

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

circumstances as posited by Ken, "the job is very risky so we form an association to support one another during difficult times".

4.7.1 Summary

It was observed from the conversation that Ghanaian youth are engaged in sakawa rituals to possess the minds of the foreign partners and later drained their resources. However, sakawa is a game where the scammer is both the victim and the villain. The perceived occult dimension can destroy the life of these young people. Apart from the physical harm, the young guys who patronize 'juju' priest are being exploited in another way, by expending considerable amounts of their limited resources for such blessings which have an unimpressive rate of success. So on the narrative, Rauf confessed that 'though the occultism exist, I stopped because of the fear of repercussion'. In the same vein, Ayiteh rescinded his decision of consulting spiritual leaders because the "requirements for the rituals were too much".

4.8. The live experiences of the cybercrime victims

The internet has become a double-edged sword of providing opportunities for the individuals and organizations and also bringing with it an increased information security risks and challenges. The emergence of cybercrime activities in Ghana has occasioned financial losses to many individuals and organizations. As a result of trying to understand further the scope of cybercrime, it was one of the objectives of the research to unearth e lived experiences of the cybercrime victims to serve as buffer against future occurrences. However, as the researcher did indicate in the earlier submission, victims were hard-to-reach population and this has accounted for the low response rate. The explanation gathered from the field revealed that victims are usually a high profile citizens who sometimes cannot share the embarrassment of being defrauded online. This has prevented

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

most victims from reporting their ordeal and preferring to silently bear the pain. Besides, foreign victims are also not cooperating with the Police for lack of confidence in the Ghanaian criminal justice system. This notwithstanding, some fascinating stories emerged from the interview conducted which showed the varying approaches being used by the scammers to outwit local victims. Table 4 provides the profile of the victims, but for the purpose of ensuring privacy, names of the respondents have been altered.

Table 4: Victims' profile[21]

Respondents		Age	Gender	Marital status	Religion	Education	Location	Employment status/business	Type of fraud	Amount lost
1	Mina	43	Female	Married	Christian	University Graduate	Airport	Fishing industry	Business	Gh¢5000
2	Ama	25	Female	Single	Christian	Diploma	Teshie	Nurse	Romance	Gh¢7740
3	Dolin	45	Female	Divorced	Christian	Master's Degree	Keneshie	Internal Revenue Service	"vehicle for sale"	Gh¢6200
4	Beatrice	21	Female	Single	Christian	Univ. Student	Odorkor	Unemployed	Lottery scam	Gh¢1000
5	Joseph	52	Male	Married	Christian	University Graduate	Cantonment	Senior Police officer	US Green Card	Gh¢6450
6	Culture	33	Male	Single	Christian	University Graduate	Dome	Accountant	Rent	Gh¢4000
Total amount lost by the victims										**Gh¢30390**

Source: fieldwork. (The names mentioned above and subsequently used are all pseudonyms)

4.8.1 The socio-demographic background of the victims

The IC3 2012 Annual Report indicated that the majority of victims who filed the complaints fell within the ages of 35 to 59 years. This has informed the researcher to look

[21] All the foreign currencies were evaluated and converted into Ghana Cedis

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

at the impact of age differential on the cybercrime victims. The age distribution of the respondents is a reflection of the IC3 2012 report that the older people are more susceptible to the cybercrime victimization. The age of respondents ranged from 21 to 52 with an average of 37 years. The finding also supports Umar (an internet scammer) view that 'he goes to internet café mostly in the night and search for client whether male or female who is above 40 years. His reason being that these age categories have worked and earned some money but the younger ones have nothing'.

Even though the researcher did not find any female perpetrator, interestingly, they are more prone to 'Sakawa' victimization in Ghana. Out of the six respondents, four (4) were female. Our predictable acumen guide us to consider that women are emotionally expressive than men. Saha (2014) studied about the risk of Indian women in the cyberspace and he reiterated that women are too emotional and they cannot distinguish fictitious activities from the reality. For this reason, it becomes easy for the culprits to win their heart. In an emotional state, women tend to reveal secret about their lifetime achievements. This is not only restricted to personal information, they even tend to reveal bank details, property details, details about the family background, exchange of photos, and mobile numbers. After receiving these information, miscreants used as a workable instrument to drain their properties.

Almost all the respondents had university degree and apart from the Beatrice, they are gainfully employed with an average income of Gh¢2,100 per month. Similarly, the participants were all Christian. According to the Ghana Population and Housing Census report (2010), Christians constituted about 70 percent of the population, especially in the

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

southern belt of the country and this could be the reason why the responses were skewed towards the Christian sects.

4.8.2 Types of Internet crimes gathered from the victims

Strategies adopted by fraudsters to entice the victims ranged from abnormal profitable ventures, romance, "vehicle marked for sale", lottery scam, U.S Green Card lottery, and rent apartment scam. The subsequent subsections discuss these schemes.

4.8.2.1 Bogus Business Proposals

By nature, everyone is seeking for the best for him/herself. As a result, criminals put forward some colossal business proposals or transactions that look like manna from heaven. This brings about the temptation for people to keep the perceived proposal from others in order to make maximum gain out of it. Madam Mina fell into this ploy. She shared her experiences with the investigator.

> It's unfortunate that I was victim to this incidence and it all happened in September, 2013. I checked my email and I received a message from a man called Prince. He wrote; Mina how are you? Please forgive me. My phone got missing and I lost all my contacts that is why you were not hearing from me since I returned to Germany. I discovered your email address from one of my old dairies and I decided to say hello to you and this is my German private number (I burnt those materials recently so I can't remember the number but it started like +49201…. The victim said).

Madam Mina said she tried to figure out the person after reading the message but the name was not familiar. Upon several thoughts she considered that the man could be one of her numerous customers. She called Mr. Prince on his cell phone but as they were conversing the voice sounds strange and that created her doubt. So Mina asked, who are you? The narrative continuous;

> Then Prince said, "ahhhh, se won kae me a ebeye me yeea" (is an Akan language, literally, if you don't remember me it will pain me). So I accepted that he was a true friend. Since then, we communicated a lot on phone, Facebook and WhatsApp. Later on, he called me and said, Mina, business has been slow, things are not well so I have stopped my previous work, and I am now working with white men operating in the tourism industry. We have even decided to penetrate into

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

> the Ghana tourism industry. Then I said, that could be wonderful because we have so many tourism sites and places in Ghana we have not touched on.
>
> He said in the conversation, yea, that is true but there is a product my people (white men) need so if you can get this product for us, you are going to make it. Initially, we ordered the product from Zimbabwe but now they have stopped supplying us. Then I said, what is the name of the product? He said, the name of the product is 'Fishing Chamdize'. I was confused because I had been into the fishing industry for a number of years but haven't come across such products. I tried to find the name of the product on the internet but I didn't get it. My husband is a nautical engineer and I contacted him but he too couldn't found it. I informed him that the product is not on the Ghanaian market. He replied that I should contact one Mr. Owusu at Koforidua, and he will show me the sample of the product. I called Mr. Owusu cell phone and we agreed to meet on weekend (that was Saturday) at Koforidua. When the time was approaching, Mr. Owusu called and told me that because of his busy schedules, we should rather change the venue to Aburi which I agreed. Finally we met somewhere at Aburi Senior High school. He shown me the sample and it was labeled 'Fishing Chamdize' then he said, only 20 cartons are available at the moment. Each carton contained 30 bottles and the unit price was Gh¢15. So the total cost for the first consignment would be Gh¢9000.

On her return to Accra, Madam Mina called the supposed friend (Prince) in Germany and briefed him about the whole process. Prince told her that his people need the products badly so Mina should try and export the consignment for the mean time. The goods valued at $32000. Mina called Mr. Owusu and he delivered the goods to her in Accra. She made a part payment with the tuned of Gh¢5000 and promised to settle the balance within three days. Coincidentally, Madam Mina went to the Ever Green Mall on the same day to purchase some few items, and she discovered a similar bottle labeled 'Viniguard', so she became suspicious. She bought one of the 'Viniguard' and compared it with the 'Fishing Chamdize' and found out that the two products were the same. It was at this stage she realized that she has been duped. She started calling the scammers (i.e Mr. Owusu and Mr. Prince) but they sometimes switched off their phones or at times, it rang and nobody answered. What follows was the strategy she adopted to arrest the culprits.

> I sat for a while and I prayed to God that he should give me wisdom to deal with these criminals and indeed Lord shown me the way. I sent a text message to Mr. Owusu and I said, please your balance is ready but I have been trying to reach you on your cell phone and it wasn't going true. Within a short time, he replied, telling me he is busy and that he will send his son to receive the balance on his behalf.
>
> When I got that response, I drove to the Airport Police Station and lodged complaint. I narrated the whole story to the police officers and they were shocked. Later, his son called, that I should meet him around Trasaco Villa on the Tema Motor Way. The Station Officer detailed three CID men to

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

> accompany me. So we drove toward the area. I got out from my car and I met the guy (son), while I was about to pay the remaining amount, the CID people came out from their vehicle and arrested him. In his confession statement, the culprit admitted he was part of the syndicate and through the effort of the police, Mr. Owusu also arrested. Finally, I was able to get my money back and the police took over the case. The investigation revealed that all the guys were living in Tema.

In the text, the criminal used receptive Akan language of "se won kae me a ebeye me yeea" to win the trust of the victim. The sentence tries to portray that the scammer knew the victim very well, or they shared certain needs and aspirations. Thus, when Madam Mina was doubtful about Prince credibility, later she 'accepted him as true friend' as a result of 'language game' expressed by the first offender (Prince). After initiating online friendship over several days, Mr. Prince enticed Madam Mina by introducing a promising business proposal as he put it, 'there is a product my people need so if you can get this product for us, you are going to make it'. The prime objective of every businessman/businesswoman is profit maximization which moved Mina to pursue the $32000 deal without checking the backgrounds of her business partners, and later she was conned.

4.8.2.2 Fraud through Romance

Perpetrators use the promise of love or romance to entice and manipulate online victims. A perpetrator scouts the internet for victims, often finding them in chat rooms, on dating sites and even within the social media networks. These individuals seduce victims with small gifts, poetry, claims of common interest or promise of constant companionship. Once the scammer gain the trust of the victim, he then begins requesting for money, asking victim to receive package or seeking other favors. This crime not only affects the victims financially but there are emotional and mental implications. Ama elucidated how she got herself in online romance and being swindled.

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

> It happened when I received a message from the man called Julius living in abroad on my Facebook account. I read the message and the person wrote, O' you are beautiful, responsible and you don't look like the classic girls in the U.K. So I want to be your friend and I accepted his friend request. That day we chatted for a while and I logged off. The next day he requested my phone number. Initially, I did not want to give my number to him but upon further appeal, I changed my mind, and I said let me give him a trial.

According to Ama, they became friends for almost three months and later Julius expressed his desire to marry her. Ama accepted the proposal and she admitted that though the two did not meet physically, they were living as husband and wife. The gentleman introduced her on phone to one of his uncles who resides in Accra. The said uncle used to call Ama and even promised to visit her at home. After Julius wooed the trust of Ama, he took the opportunity to chip in some business proposal where he only benefited. She continued with the narrative to authenticate this assertion;

> One day, I had called from Julius (the supposed lover) that he wanted to ship some items including three accident vehicles and other home appliances to Ghana but the price of the freight was quite expensive, so I should help him to finance the shipment process. Fortunately for him, that month I received my two years' salary arrears and I agreed to help. He promised to pay my money back and share the profit that will accrue from the transaction. Also, he has documented one of the vehicles in my name as part of his commitment toward the relationship. I was convinced that Julius was a nice man and I transferred $1800 into his foreign account. The next day, I was trying to find out whether he has received the money but his phone was switched off. I further sent him an email and Facebook messages and yet he did not respond. I called his uncle 'line' too and it was off. I narrated the story to my friend Agnes and she told me the deal could be 419 scam.
>
> I reported the matter to the Teshie Police Officers. Subsequent investigation proved that all the emails, text messages, and the phone numbers were initiated from Ghana when the culprit claimed to be in the United Kingdom but the police could not arrest the offenders and that ended the matter.

Romance scam, or 'sweetheart' swindle, is emotionally devastating type of fraud because dating websites allow fraudsters to cast their nets wider and disappear more easily than the traditional scams. The romance component of the online scam acts as an inducement to lure the victim, before committing other type of fraud such as financial fraud. In the narrative, Ama succumbed to the perpetrator's request after he gradually prepared her mind that she is a marriage woman as the victim admitted, "though we did not meet on the physical world but we were living like husband and wife".

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

As the Ghanaian custom demand that one of the purposes of marriage is not only for procreation but also it's the means to offer support for each other, and that was why Ama extended her financial support to the fraudster.

4.8.2.3 Vehicle marked "for sale" scam

Under this type of fraud, an attempt by person to sell a vehicle could make the person end up being defrauded. The question is how does a vendor of vehicle becomes fraud victim? Every "for sale" invitation is accompanied by telephone number and that was how Dolin became victim and she explained;

> I was selling my Toyota Camry (that is 2008 model), so I pasted my contact on the back screen. One day I got stuck in traffic and had a call from guy, called Ayesi, and that he is interested in the vehicle. I directed him to my house and inspected the vehicle. Then he told me, his brother who is outside the country will make the payment, so he is going to give out my mobile number to him. I said, alright. In an hour later, I had an international call, and the man introduced himself as Mr. Asibey, a Ghanaian domiciled in US and senior brother to Ayesi. We negotiated the price of the vehicle and finally settled on Gh¢37,500. Though my initial target was Gh¢30,000, so I considered this as a great deal. He promised to pay the amount in the following day.
>
> Thereafter, he called again and confirmed his desire to buy the vehicle but due to one reason or the other he does not want to pay the money involved through Ayesi, rather, he want to send the money directly to me. Also to avoid the payment of commission on money transfer, the cash would be concealed in a luggage and send through the courier service, registered with my name. Then I said okay. Four days later, he signaled me that the luggage has been sent to Fedex Courier Service and the delivery charges have been added to my money so I should pay for the cost of the delivery as well. Subsequently, I received another call from Fedex agent purported to be working at 'AFGO' terminal at the Kotoka International Airport and that I have a parcel with them and I should pay Gh¢5,600 into their MTN Mobile Money Transfer Outlet to enable them deliver the goods. After paying the said amount, all the three people in this syndicate switched off their mobile phones. I tried, tried, tried but all effort proved futile. So in short, I went to the CID headquarters and lodged complaint but I got a feedback that the people were scammers.

Ghana is progressively becoming a nation of technological addicts as evidenced by the fact that now many people spend longer hours on the internet. The addiction has impacted on the way we buy and sell our properties. On the online business, everyone wants to sell for the best price, and invariably, wants the whole process to be quickly and painlessly as possible. However, Madam Dolin could not benefit from this electronic base marketing as she attempted to use mobile phone to sell her private vehicle. From the text, scammers

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

worked together to create a 'fraud ring' and shared data on how best to scam the woman. The first accomplice (Ayesi) interacted with the victim in the real world but the woman did not border to find out where he lives. Police could had been using the information to trace the criminal when the untoward happened. After Mr. Ayesi succeeded convincing her, he handed over to the main offender (Asibey) to assure her that he would buy the vehicle. The third collaborator defamed the reputation of Fedex Courier Service to defraud the victim. The scammers' operation was successful because they hypnotized the victim with the huge profit margin as she reiterated 'though my initial target was Gh¢30,000, so I considered this Gh¢37,500 as a great deal'.

4.8.2.4 "Mobile Phone scam"

In the mobile industry, Ghanaian customers are able to choose among multiple service providers and actively exercise their rights of switching from one service to another. This development has created fierce competition among the telecommunication operators to market their services to the greater number of people and increase their subscriber base. In order to achieve this feat, these companies adopt various methods of reaching out to many individuals as possible to persuade them to join their network. Amongst the methods employed is by offering reward packages to their loyal customers. On the other hand, scammers also work behind this idea to con subscribers. They circulate text messages that falsely indicated that the receiver had emerged as a winner in promotion being run by the network provider. To redeem the prize, the victim would be asked to buy a recharge cards and send the pin codes to the sender of the message as prerequisite for processing the reward. The victim would be further promised a refund of the credit card when the process is over. To be surprised, the fraudsters will continue to create another condition for the potential winner until the person becomes aware that she has been defrauded.

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

Beatrice, a 21 year-old university student was conned under this type of falsehood and she volunteered to express the ordeal to the investigator.

> On the 29/09/2014, I received a text message on my MTN mobile phone indicating that I had won Gh¢12,000 from the MTN Mobile money promotion. When I received the message, I thought it was true. The text required that I should send MTN recharge cards worth Gh¢1,000 to the two MTN mobile numbers before the code would be given to me to the withdraw the money.

Madam Beatrice said she called the mobile number which was used to send the text message and realized that it was one Mr. Fordjor who claimed to be the manager of MTN promotion in Accra. She then sent the MTN recharge cards to the supposed Manager. After receiving the recharge cards, he further demanded to have sex with her before releasing the code. Immediately, something just trickled her mind that she has been defrauded. She made a report to the Odokor Police. She continued to explain how event unfolded leading to the arrest of the perpetrator.

> The police advised me, and I told him that because of my busy schedules, it would not be possible to travel to Kasoa and I pleaded with him to rather visit me at Odorkor, and he agreed. So the next day he set off and gave me a call, described the attire he was wearing for easy identification.
>
> My father, together with some plain cloth personnel from the Odorkor Police Station came around and monitored the fraudster. He alighted at the Odorkor Main bus stop. He called my phone and I answered. So we finally met. As we shook hands, the police officers arrested and handcuffed the fraudster and sent him to the Odorkor police station.
>
> At the police station, he mentioned his named as Kingsley, and denied being called Mr. Fordjor. Consequently, he was arraigned before Cocoa Affairs Circuit Court and sentenced him to 18 months imprisonment with hard labor.

This narrative shows, among others, that Ghanaian police is quite effective in dealing with cybercrime. Unraveling crimes in cyberspace requires more than being an expert in computer programming or encryption techniques. Someone must embrace the vision for the case, marshaling the needed resources to move the investigation forward. Besides, intelligence gathering play a crucial role because of the changing environment in cybercrime. In the text the victim did well of providing the right information to the police. Police further acted upon the information and advised the lady to accept his 'sexual request' which led to the scammer's arrest.

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

4.8.2.5 America Green Card Lottery scam

Every year, the America government allocates Green Card Visa to individuals who are randomly selected from countries with low rates of immigration to the United States. The exercise helps applicants acquire permanent residential status. There is mad rush of Ghanaians exploring this opportunity but scammers have created dubious websites, posing as U.S officials and extorting money from the applicants. Joseph became victim to the US online Green Card visa application and what follows is the interview granted to the researcher.

> One day I was browsing on the internet and a message pup up in the home page. I read over and it was an advert concerning the US Green Card lottery. When I clicked on the message, it routed into another web site called the usafif.org. At first, I was uncertain to heed to their quest but I received another message from officers claimed to be an Immigration experts from the US Homeland Security Department and that they have considered my application, so I should complete the registration and forward my personal detail to them. This motivated me to log into the usafif website again and started the registration process.

The victim paid a registration fee of $1500 through credit card transfer. This package would allow his nuclear family to join him in the US after he has won the lottery. However Mr. Joseph could not fulfill the dream and expressed his sentiment. The story continued;

> After the payment I did not hear from them. So I asked somebody who had an idea about this America Green Card and he told me that the process do not start during the period I had started, rather it would be later part of the year, 2013. So from that time I got to know that the people were scammers. Though I am a police officer, there was little I could do to retrieve my money. The mere fact that the person is holding a phone or laptop down the street does not necessarily he has committed cybercrime and therefore should be arrested.

Due to advancement in technology, cybercrime is now easier to commit. Getting internet connection is very simple, so all that criminal's need is a phone, tablet or any eligible device which has internet on it. This has made cybercrime difficult to detect because scammers are sitting comfortable in their homes or public places where may be a policeman might sitting closer to the fraudster, probably exchanges pleasantries, and yet duping people of huge sums of money. For that reason, the victim explained the challenge

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

cybercrime pose to even security personnel, "though I am a police officer, there was little I could do to retrieve my money. The mere fact that the person is holding a phone or laptop down the street does not necessarily mean he has committed cybercrime and therefore should be arrested".

4.8.2.6 "Rent apartment scam"

The growing internet proliferation has opened the country to new online trading platforms, which have empowered the average Ghanaian to transact various business operations. Customers are increasingly turning on to websites such as OLX.com and other free online classifieds to purchase goods or rent an apartment thereby cutting middlemen or agent out of the trade. Unfortunately, this has also given scammers a new avenue to find victims who are looking for good deals online. 'Culture' had been a victim to this type of fraud in an attempt to hire apartment via the internet and he spoke to the investigator;

> I became an internet victim when I was looking for apartment. Because of the high percentage being charged by the 'rent agents' (i.e middlemen), I decided to look for the apartment on the internet. So I registered with the OLX.com; an internet trading portal. I posted on the platform that I am looking for a room to rent or basement style with bathroom, kitchen, and toilet. I also added my contact details. Three days later, I had a call from one Mr. Quaye, introduced himself as a landlord and he got my details on the OLX website, and so if I could come around Alhaji Tabora No. 3, a suburb of Accra to have a look at the room. I met the man in the supposed house, negotiated the price and finally settled on Gh¢100 per month. Then he said, I need this money to pay my children school fees that is why I have reduced the amount, so I should pay four years advanced fee. Considering the serene environment, the amount was quite cheap. The next day, my junior brother accompanied me to the house and I paid Gh¢4000 out of 4800 to the landlord. He acknowledged with the receipt to indicate that I have paid such amount. Then he said, the keys and the tenancy agreement would be ready on Sunday (that is four days after the payment). Later, I called to find out whether the documents are ready but his mobile phone was unavailable.

Linking the expression to his body language, the investigator further probed to find out what happened subsequently.

> So on weekend, I went to the house and met a fair lady. She asked me, gentleman how may l help you? I narrated the story to her and she said; this is my house and I have only one tenant. She pause, scratched her head and said; O' the 419 people have been using my house to bait innocent victims, and this is about fourth incidence. She also tried the supposed landlord telephone number and it was switched off. She led me to the 'Hong Kong' Police Station and I lodged a complaint but the officer failed to arrest him.

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

Ghana's prospects of becoming a cashless economy could be undermined by internet fraudsters. This is informed by the fact that when people's activities in the information superhighway cannot be protected by law enforcement agencies, it created mistrust in the system. Consequently, government would lose revenue mobilization from the online classified agencies because customers would not patronise the cyberspace.

4.8.3 Summary

Understanding who the criminal is likely to target can assist in taking preemptive actions to forewarn and prepare for all forms of attack. Intelligent criminals always target people whose circumstances are loaded with some form of vulnerability. Users of internet facilities have to be on guard against all forms of solicitation that come from strangers with very enticing dividends. One nature that the criminals prey upon may be people's kind-heartedness. It is a judicial notice that Ghanaians are hospitable, honorable and above all, the virtue of being brother's keeper. The stories pointed to the facts that some of the victims were trapped in, on an attempt to help or respond to other's needs without due diligence. There are other users who see the internet as a genuine platform with which to make money. Usually, they gain some profit at the initial stage of the transaction. This success takes them deeper into the fraud as they build more relationship with the scammer and become embroiled in legal and financial entanglement out of which only the perpetrator will make profit. Information gathered, also shows that people become victims to the internet fraud because of unrealistic benefits, and Mina for instance, developed interest to stay in the business because of colossal profit, tuned of $32,000. Culture also admitted, "Considering the serene environment, the amount was quite cheap" and Beatrice on the other hand confessed; "though my initially target was Gh¢30,000, so I considered this Gh¢37,500 as a great deal".

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

The investigation further revealed that victims have been interacting with people they have not come across in the real world. Besides, all victims subscribed to more than one social networks as a way of keeping in touch with, and tracking of different spheres in their lives; for example, one social network for the family, one for business, and one for lovers/friends. In explaining the Routine theory, Reyns et al. (2011), warned that individuals who normally used multiple social networking sites are prone to crime because they are likely to come into contact with so many people on the social space including miscreants.

Since the victims were drawn from the police source, the researcher wanted to find out the outcome of the cases, but only one offender out of the six cases was successfully put on trial and imprisoned. So when the question was put to Mina about the police reaction and response, she responded;

> Even though I got my money back, I was quite disappointed because the police could not pursued the case further and I didn't know why they stopped the prosecution. Because I was insisting that the conmen should be jailed to serve as a warning to others. When I contacted the officer in charge of the case, he said, ohh, Mina, thank God you were able to retrieve your money. Pursuing this case in court would be a herculean task.

Ama added;

> I reported the matter to the Teshie Police Officers. Subsequent investigation proved that all the emails, text messages, and the phone numbers were from Ghana when the culprit claimed to be in the United Kingdom. However, the police could not arrest the offenders and that concluded the case.

Dolin also reechoed the same outcome and she said;

> So in short, I went to the CID headquarters and lodged a complaint but later I got a feedback that the people were scammers and since their mobile phones were not active, it would be very difficult to track them.

Joseph admitted, "Though I am a police officer, there was little I could do to retrieve my money".

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

Culture could not hide his frustration and he explained;

> The police investigation was like go and come, go and come. I didn't see any serious outcome. Even the CID man who was handling the case told me that it would be very difficult since I didn't know where the man was staying. And also, he is not a magician to locate the man but I should pray that one day I will meet him somewhere. However, I suggested to him that he should contact the telecom company and cross-check his contact detail but the investigator said it will be very difficult task. So later I stopped going to the police station because going there every day was like, I am wasting my precious time and money.

It was only Beatrice's case that the police arrested the culprit but the approach was conventional policing operational tactics. This explains why in the literature about 79.5% of the nationwide cybercrime cases are still pending for investigation. This outcome pushed the study further to enquire from the Police administration on how they are responding to this developing situation.

4.9 Responses and Challenges of Ghana Police Service towards Cybercrime

The Ghana Police service has, since its inception been in the frontline of the criminal justice system of Ghana. It is the most visible arm of government as the symbol of law and order, to the people. The Police Service is mandated by Article 200 of the 1992 Constitution of the Republic of Ghana, and the Police Service Act 1970 (ACT 350). The Constitution mandates the Service to operate on democratic policing principles. Whenever the ordinary citizen suffers from injury or loss of property through crime, it becomes an incumbent upon the police to investigate and establish the prima facie of the case. The Police Service Act 350 provides in Section 1 (1) states that "it shall be the duty of the police service to prevent and detect crime, to apprehend offenders, and to maintain public order and safety of person and property". This duty extends to the full range of prohibitions under the penal statutes. As cybercrime acts become ever more prevalent, Ghana Police Service as law enforcement agent increasingly face the question of what it means to 'prevent' and 'apprehend' in the context of crime with transnational element. Hence, the researcher developed interest to broaden the scope of the phenomenon from the

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

police perspective. As reiterated earlier, the police has no specific unit to handle cybercrime. However, it was found that four units are managing the situation and these include Commercial Crime Unit (CCU), Documentation and Visa Fraud Section (DVS), Intelligent Unit (IU), and the Legal and Prosecution Unit (LPU). The interview schedule was organized to find out the ordinary and legal meaning of cybercrime, the magnitude of cybercrime situation in Ghana, the demographic characteristics of actors (i.e victims and the offenders), and how police is reacting to the problem.

During the interview session, the head of the Commercial Crime Unit, made general observation which presupposes that the practice of cyber fraud is becoming severe and gaining grounds rapidly. He noted "it is becoming serious, formerly it was on small scale but now it is worse. Even people who are transferring money for goods bought outside get their monies being diverted into different accounts".

An attempt was made to find out how police officers understand cybercrime. Even though most of the respondents commented on the issue with different preambles, yet they all arrived at the conclusion that 'it is a crime committed via the use of internet and by extension making false representation'. As a result of the fluid meaning of the concept, further questions were posed to find out whether there is legal definition that support the officers' claims but the majority of the personnel acknowledged that there is no law in Ghana that clearly states what constitutes cybercrime, and outlines offenses and the punishments.

On the other hand, the head of the Legal and Prosecution Unit disagreed with that assertion. He argued;

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

> Crime is crime; whether stealing, whether murder, whether cyber, they are all crime, and a crime is any act that offenses the laws of the state. And we have the law passed in 2008, that is electronic transaction act, Act 772 and the various crimes that are committed by the use of internet have been defined in that act. So the police, when particular crime is committed by the use of internet we have clear definition of that crime in the act which gives the police power to investigate and prosecute such offenses in competent court of jurisdiction.

This answer allowed the investigator to probe further about the jurisdictional efficacy of the act and he opined;

> The law states that if the offense is committed by the use of computer, and it can be even an ATM card, mobile phone or any electronic device. It means that the person's 'mens rea' or the criminal intent for the commissioning of the act has been informed under the sovereign will of Ghana. And the role of service providers do not control over what customers are doing. The service providers open up the traffic for people, individuals buy their credit and connects to the cyber world and decide what they want to do. So the law enjoins us (police officers) that where there is need to access the information from service providers, we go for it. In the same vein, if the need arises to access information outside Ghana, we use INTERPOL to get the response.

It was obvious from the discussion that there are some misinterpretation about the phenomenon as the police officers provided loose and contradictory views. Though the head of the Legal and Prosecution Unit tried to salvage the image of the police service on how they are responding to the issue, his approach is still skewed towards traditional means of international cooperation which may not be sufficiently timely to ensure access to extraterritorial volatile data retrieval because cybercrime can occur within milliseconds.

The conversation was then shifted to the age demography of both offenders and the victims because some sociologists and criminologists argued that age distribution of crime is sufficiently invariant over broad range of other social conditions. Commenting on the age issue, the Director of Documentation and Visa Fraud Unit at the CID headquarters, explained;

> What I know and from what I have investigated, they are young men between the ages of 18 to 30 and the majority of them are secondary school leavers, but at the highest level there people who are working at the banks and other higher institutions using the internet to commit crime. The perpetuators can be grouped into two categories: that is technical and non-technical people. The technical people are the real hackers. They are the IT specialists as in people who have gone so much into IT like programmers, system administrators, computer security professionals, data based security administrators, and computer forensic. They can hack into an electronic payment system and transfer account from one data to another. The non-technical people are criminals in the real world who have fair idea about IT system and they use it to facilitate their heinous crimes. Now in Ghana, those we have mainly as the perpetrators of cybercrime are the non-technical people.

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

> People who normally fall victim of cybercrime in Ghana are the divorcees and they are mostly middle-aged women between 36 to 45 years. They are easily tricked by the cyber offenders on love relationships. You see, people at this age category simply don't think it could happen to them, and when it does, it takes them too long to lodge complaint. And in the end we find it difficult to adduce evidence to support their case.

These exposé correspond to the early findings where cybercriminals are primarily between the ages of 17 to 30, with an average of 23 years. Also victims are adults who occupy various positions of trust in the society and with an average age of 37. Online dating has become an accepted practice in the modern times: indeed, many find it preferable to traditional dating as it allows you to select candidate and break the ice without any social engagement. This makes it an ideal hunting ground for internet scammers looking for a quick score and not in the usual dating sense.

Responding personnel opened their remarks about the complex nature of cybercrime, and enumerated some challenges that affected the investigation, apprehension and prosecution of cyber offender in Ghana. The officers acknowledged that the police organization is understaff and this affects their effort to fight crime. The head of the Intelligent Unit observed; "in my opinion, the population is expanding at geometric progression as against slow expansion of police service and therefore the number of crimes are far outweigh the investigators". This concern also reiterated in the Ghana Police (2013) Annual Report where police-population ratio stood at 1:847 which remained far from achieving United Nations policing standard of 1:500 people.

Inadequate training or lack of technical know-how on the part of cybercrime investigators increase the level of sophistication. The traditional law enforcement methods have proven ineffective against the growing evidence of criminals using electronic devices to commit fraud. It is important for investigators to be ahead of the fraudsters to thwart their efforts. The head of the Legal and Prosecution Unit noted;

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

> Equipping investigators with technique to detect, analyze and retrieve falsified documents from any digital device is the way forward but many crime officer are not trained; many do not even understand what cybercrime is or what constitutes cybercrime. Ghana Police College is a higher learning institution of the Ghana Police Service and ran courses designed to update senior corps but cybercrime is not part of their syllabus, recruit training is also not part of it. On the Detective school, I even forced my way to teach but the training itself is not enough. I stand for two hours and that is all. We need computers to study how the whole crime is perpetuated, that is, going into how computer is hacked, how information is properly protected, but we don't have the equipment.

Other participants argued that 'you can have a good investigators but if you do not have the necessary investigation tools to work with and adduce evidence to support your case, the offenders can be discharged unconditionally'. The conclusion remark by one of the junior informants is worth quoting;

> We don't have the means to monitor what is going on within the internet cafés. People will sit down 24 hours browsing, and do all sorts of things without being detected. But on the other jurisdictions, they have a specialized unit that controls cyber information, and the Unit is connected into the Internet Service Providers portal to monitor what people are reading or twits over the internet space.

The final problem enumerated by the key informants was the difficulty of obtaining information from the telecom service providers. For example, one explained;

> The process of getting information from the telecommunication companies is very cumbersome: first, the investigator has to file an Ex-parte motion in court to declare his intention to access information from the Telco's: secondly, the investigator has to swear an affidavit in support of the motion thereof, and lastly, the court will order for the disclosure of information. In each process it can take you some weeks or months before you get a response, he added.

The complexity of cyber security threat requires unparalleled response from the law enforcement agencies because data can be altered within few seconds, and sometimes service providers do not store computer data for longer periods. The Article 100 (2) of Electronic Transaction, Act 772 states that "where an order from the Court is not obtained and served for fourteen days after the receipt of the written request, the electronic communication provider is not under any obligation to preserve the evidence". As a result, this conventional policing method of accessing information cannot be an effective mechanism to deal with this contemporary crime. The process of disclosing customer information by the telecom companies was supported by the documents gathered from the "Circuit Court 8" at the Cocoa Affairs which reflected in appendix i.

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

4.9.1 Summary

The discussion has discovered that cybercrime perpetrators are in two groups; that is technical and non-technical people. The non-technical people mainly employ social engineering tactics to defraud their client. The findings further shown that police service has been mandated to fight cybercrime in Ghana. However, the organization efforts are being limited by factors such as inadequate computer crime investigators, lack of ultramodern equipment, and lack of cooperation from the Internet Service Providers to adduce electronic evidence.

4.10 Cybercrime and Legal Mechanism

Law is a dynamic tool that enables the state to respond to new societal and security challenges, such as cybercrime. A discussions with some officers of the Ghana Police Service further revealed that when such cybercriminals are apprehended and processed to court, there are no sufficient legal bases to prosecute them as the legal system is not up to date to convict the scammers, and this contributes to the prevalence of the menace. The head of the Police Intelligent Unit remarked;

> This is an intelligent led operation and after we worked hard to present our docket before court, the judges still rely on the conventional procedural trial; that is the Complainant, the Prosecutor, and the Accused. So if one of the stakeholders is not around, nor represented, the judge will struck out the case, and from my experience, most of the cybercrime acts involve transnational element where either the accused or the accuser will be at different sovereign state and it has been a major setback to combat the internet fraud.

On the contrary, the Director in charge Legal and Prosecution debunked this assertion and explained that the Act 772 defined the various crimes that are committed by the use of internet. Although he did not quote the exact section to support his claim, he further gave a general view that the law further allowed the police to prosecute offender in the absence of victim or complainant. These contradictory views expressed by the officers influenced the researcher's decision to carve it as one of the focal points of the study.

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

In order to achieve this specific objective, Circuit Court Judge was consulted to throw more light on Electronic Transaction Act (Act 772), as an instrument for promoting legal certainty in the cyber space of Ghana. But as mentioned earlier, the investigator had to settle for speaking to the "Circuit Court 8" Judge at Cocoa Affairs Court Directorate because of her expertise on internet fraud. The synopses for the discussion were the criminalization of the cyber offences; admissibility of electronic evidence in the cybercrime proceedings, and jurisdictional issues.

Commenting on the issue, she expressed concern that 'criminals are now exploiting the internet to the detriment of the public and that if cybercrimes are allowed to continue, it would erode the public confidence in the online commercial activities such as trading, e-banking and other services, which would have serious consequences on the Ghanaian economy. Thus, it is high time we tighten up our laws to control the scourge'.

4.10.1 The criminalization of cybercrime

The technological advancements associated with cybercrime means that while traditional laws can still be applied to some extent, legislation must also contend with new concepts which were not traditionally addressed by the law. For instance, while the existing criminal law focused on physical objects of crime such as stealing, rape, murder and burglary; cyber law on the other hand are largely characterized by an intangible 'computer data' which also requires the introduction of specific offences, definition and concept to protect it legal integrity.

However, all these legal tussle would be understood on the Jerome and Hall criminal principle of 'nullum crimen sine lege' (no crime without law) which requires that;

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

> No one shall be held guilty of any penal offence on account of any act or omission which did not constitute any penal offence at the time when it was committed nor shall a heavier penalty be imposed than the one that was applicable at the time the penal offence was committed (cf. Ofori-Amankwah, 2012:10).

It means that what constitutes any criminal offences must be clearly defined by law. This notion allowed the researcher to enquire from the judge about the criminalization aspect of the Act 772 and she noted;

> Yes, we have the Act 772 which basically regulates the transactions that occur in the electronic space and the offences are stated under Section 107 to 137 of the Act. The only section utilized by the Police as far as this Court is concerned, is Section 102 (2), which states that "a provider of an electronic communication service shall disclose a record or other information related to a subscriber or customer to a law enforcement agency on receipt of Court order for the disclosure". But that does not mean the evidence gathered from the service provider is attainable in court. Section 106 of the same Act makes it clear that "Where a Court varies, evidence obtained solely on the basis of electronic wired transfer is inadmissible in civil, criminals or administrative proceedings". So the prosecutors need to furnish with us [judges] supportive documents to substantiate their case.

4.10.2 Electronic evidence in cybercrime proceedings

In criminal cases, the burden of producing evidence is the means by which the facts relevant to the guilty or innocent of an individual at trial are established. Therefore, the prosecutor has a duty to present sufficient evidence to support his claim beyond reasonable doubt. Electronic evidence is becoming central not only to the investigation and prosecution of cybercrime, but increasingly to crime in general as a results of the growing usage and application of communication technologies.

During the study, some police officers pointed out, 'even where the evidence was adduced, the courts sometimes gave little weight to electronic evidence, due in part to the lack of knowledge about the intangible nature of the electronic evidence'. Thus, a clarification was sought from the judge whether electronic evidence is admissible in court and she argued;

> In the Act 772, Section 7, allowed the admissibility of electronic evidence and set parameters or the criteria for assessing the weight of the evidence in terms of reliability, integrity, original source and any other information that the court consider relevant. However, due to the lack of computer forensics laboratory, it is difficult for investigators to collect such digital evidence. In addition,

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

some judges too need basic understanding of cybercrime in order to appreciate the electronic evidence.

Fighting crime is a joint effort between police and the judiciary. The court has a legal authority to punish the offender through fines or imprisonment to serve as deterrence to others. And so, if some judges 'do not understand basic tenants of cybercrime', it weakens the police determination to cramp down the menace.

4.10.3 Jurisdiction issue in cybercrime

According to the Black's Law Dictionary (8th edition), jurisdiction is the practical authority granted to formally constituted legal body or to a political leader to deal with and make pronouncements on legal matters and, by implication, to administer justice within the defined area of responsibility. Every country has jurisdiction over people within its territory. Conversely, no State can exercise authority over persons outside its boundaries unless international treaties. In the context of the internet, cyberspace has no geographical boundaries. It establishes immediate long-distance communications with anyone who can have access to any website. As internet does not tend to make geographical locations clear, the cyber citizens remain in physical jurisdictions and are subject to laws independent of their presence. Therefore, any related activities on the internet may expose the person to a risk of being sued in any country where another internet user may establish a claim. Accordingly, in each case, a determination should be made as to where an online activity will subject the user to jurisdiction in a distant country. As such, a single transaction may involve the laws of at least three jurisdictions: the laws of the State in which the user resides; the laws of the State where the server hosting the transaction is located may apply; and the laws of the State which the person or transaction takes place. So an internet user in Ghana conducting a transaction with another internet user in USA through a server in

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

South Africa could theoretically be subjected to the laws of all the three countries as they relate to the transaction at hand. With this scenario, a question was posed to the judge about the jurisdictional integrity of Act, 772 and the key informant acknowledged;

> Under Section 142 of the Act grants extra territorial powers but it is very difficult to enforce. The reality is that Ghana is yet to subscribe to any cybercrime convention that can facilitates extradition. So the window opportunity for the investigators are to explore the conventional treaties like INTERPOL to reach out the party concern.

She made a further observation;

> Criminal Offences Act, 1960 (Act, 29) actually deal with physical criminal behavior like theft, and a lot of sections have been modified to suit cybercrime offences. But the Sections give us [the Judges] a lot of discretionary powers without categorically defined how the case should be addressed.

In her concluding remarks, she called for specific cyber laws like the UK Computer Misuse Act which outline the various offences under clear subheadings.

Part IV: Conclusion of the Chapter

The final part of the chapter concentrated on the conclusion and it has been categorized to related to; (a) offenders; (b) law enforcers; (c) victims.

(a) Offenders

The proliferation of the internet café's in every nooks and crannies of the city, which by extension, have provided employment opportunities to some, has in fact become an avenues where criminal activities are nursed and nurtured. It is a place where, in most cases bright minds, including jobless graduates meet to brainstorm on the best way to make ends meet. After all, when the society refuse to listen to your needs, morality is thrown out of the window. In this instances, morality and all forms of decency are often placed at the back burners where the ultimate aim is to make quick money in a very big way for self-sustenance.

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

There is convincing evidence from the discussions that socioeconomic conditions create the right environment for cybercrime to thrive. When people are idle and have no job, they are more likely to engage in risky-gainful ventures like 'Sakawa'. Internet scams unfolded as a process, often occurring over several months. Scammers use legitimate websites as springboards for meeting their victims. The next stage involves initiating a dialogue with articulated words to persuade their partner, and later extract funds from them. Indeed, fraudsters are motivated with the fact that technology allow criminals to commit deviant act, by offering anonymity, increase flexibility, and transience which are difficult to detect by law enforcers. Moreover, a persuasive effort should be made by opinion leaders in the country to coerce the 'sakawa boys' to refrain from occultism aspect of the crime because of its devastating consequences. When the scammers send the emails and the money replies are not forth coming, they become desperate and the more desperate they are, the more they move from one spiritualist to the other. Now it is not going to be about the internet fraud, rather they would sacrifice innocent blood for money.

(b) Law Enforcers

Today, cybercrime and cyber security have become perhaps some of the most critical issues for almost all governments across the globe. For many informed governments, it has become a matter of life or death because the survival of their economies now revolves on the dynamics of ICT.

In the literature, it was reviewed that there are about 29 million mobile phones subscribers and 13 million internet user penetration in Ghana. The growth has brought along cyber-attacks on various information infrastructure as well as fraud perpetuated by criminally-minded persons popularly called 'Sakawa'. The biggest problem is that victims of

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

'Sakawa' and other cyber fraud activities had not found an advertised central point in the country to report the incidence. Even when these incidence are reported to the Ghana Police, it takes many days to apprehend any suspect because of the lack of technical know-how to trace these criminals using computer-based investigative skills. Worse of all, when such cyber criminals are apprehended and processed to court, there are no sufficient legal bases to prosecute them resulting in tarnishing Ghana's image as a cybercrime destination.

However, there is a growing indication that computer will continue to be a medium or vector for crime in the twenty-first century. With this new peril, law enforcers must adapt new investigation techniques to command the virtual society. Extricating crimes in cyberspace requires someone to embrace the vision for the case, marshaling the needed resources and specialist to move the investigation forward. Intelligence methods play a central role because of the changing and shifting environment of computer crime. Lastly, developing foreknowledge of dangers at the horizon, not when they are at the front door, becomes crucial in the cybercrime management.

(c) Victims

Unlike nuclear energy, electricity, or explosives, all of which posse a clear physical danger but computer systems in everyday life pose no intrinsic threat to our body make-ups. They cannot make us bleed, gasp for breath or cry in pain. Yet, they may conjure forces which can cause grave social, economic and political harm. Our dependence on internet in research, communications, and financial transactions produces vulnerabilities in cyberspace. Extending the rule of law into the cyber world is a critical step towards creating a trustworthy atmosphere for people and businesses to flourish. On the other

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

hand, the research has shown that the effective legal provisions on cyberspace are yet to be implemented in Ghana because the existence ones are inadequate to fight the menace in terms of jurisdiction and adduce of evidence in court proceedings. Therefore, it behoves on individuals and organizations to fashion out ways of providing an alternative security for their online data. To achieve this protection, an extra vigilance and due diligence should be a hall mark before people commit themselves into electronic transactions.

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

CHAPTER FIVE

SUMMARY, CONCLUSIONS AND POLICY IMPLICATIONS OF THE STUDY

5.0 Introduction

In this chapter, the researcher provides the summary, conclusions based on firsthand information gathered from the field and the policy implications of the study.

5.1 Summary of the study

Information technology is now accepted, not only as the common currency but indeed, represents the center of gravity for development in the 21st century. However, Ghana is gaining notoriety as a "safe heaven" for cybercrime activities locally referred to as "Sakawa. As a result, many companies in the western world have refused to accept credit card transactions coming from the country. This explains the difficulty Ghanaian business people face in an attempt to penetrate the electronic based economy. The researcher therefore found it expedient to understand the dynamics of cybercrime activities from the perspectives of offenders, victims and the law as precondition for workable policy direction to ameliorate the situation.

The study's objectives are to:

1. Understand the socioeconomic characteristics of the offenders and the victims
2. Identify the motivation that predispose the offenders to this crime
3. Establish the various forms of cybercriminal activities in Ghana
4. Find out the opportunities explored by the fraudsters in their operations
5. Explore the live experiences of the cybercrime victims
6. Examine the responses and challenges of law enforcement agencies to fight cybercrime

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

The study was conducted in Accra over a period of Nine months. The views of four stakeholders' were solicited. They include the scammers, victims, police personnel, and a legal practitioner. The research design for the study was combined method which utilizes both quantitative and qualitative strategies. Secondary data was sourced from the CID headquarters to trace some of the victims and the offenders. Purposive and snowball techniques were employed to recruit the participants. A total of 26 respondents took part of the study. In-depth interview and questionnaire were primary instruments used for collating the data. In the qualitative analysis, all interviews were transcribed and codified into themes. The descriptive statistics generated from the questionnaire were also analyzed and presented in the form of bar graphs and pie charts to explain the results in relations to the demographic variables of offender and the victims.

5.2 Conclusions

This section of the project presents the major conclusions drawn from the study which based on the objectives that underpinned the work.

5.2.1 The Socioeconomic Characteristics of Offenders and the Victims

The background information about the offenders and the victims were relevant to the study because the socioeconomic context in which the respondents found themselves influenced our understanding for their actions. The findings of the research have shown that all the scammers interviewed were males between the ages of 17 to 30 with an average of 23 years. The majority of the fraudsters are educated with technical knowledge and active imaginations, yet 72.9% were unemployed. Most of them were from economically deprived homes. In Table three, it was estimated that more than Gh¢ 199,480 had been realized by the criminals from the internet fraud. All the amounts were evaluated by

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

converting foreign currencies to the current market value in Ghana's denomination, and even two of the respondents could not quote any amount because they have gained a lot from their 'clients'.

On the other hand, the age distribution of the victims clearly pointed to the fact that older people are more susceptible to the cybercrime victimization in Accra. The victims were adults with an average age of 37 years. Out of the six respondents, four (4) were females. Almost all the victims had university degree and they are gainfully employed with an average income of Gh¢2,100 per month. Interestingly, all the victims were Christians. The total amount lost by the victims valued at Gh¢30,390 as reflected in Table four. Though the amount was not as huge as what the scammers have gained, it is an indication that 'Sakawa' boys have now turned against the Ghanaian citizens. The revelation has also debunked the perception that the US and EU citizens are more susceptible to the cybercrime activities in Ghana.

5.2.2 Motivations that Predispose Offenders to Cybercrime

Scammers were asked about their motivational drive and the findings revealed that unemployment, anonymity, inadequate legal framework and easy access to the internet eulogized the youth to engage in cybercrime activities. Besides, the anonymity has created a "geographical switch" whereby criminals can hide their real geographical locations. Furthermore, the findings discovered that "Sakawa" is a learnt behavior with persuasive dialogue.

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

5.2.3 Forms of Cybercriminal Activities Discovered

The investigation revealed that cybercriminals in Ghana engaged in different forms of internet crimes such as gold fraud, romance fraud, and online shopping to rip-off their client. The study further highlighted that bogus business proposals, romance, vehicle mark "for sale", mobile phone lottery, America green card lottery, and rent apartment scams are commonly internet fraud experienced by victims in Accra. The romance fraud is the popular social engineering strategy employed by scammers, as it was discussed on both victim's and offender's circumstances. In the real life situation, love facilitates trust where partners reveal their secret to each other. For that reason, the perpetuators explore that opportunity to trap victims.

5.2.4 Exploring Opportunities by Fraudsters

This objective also discovered the fact that criminals explore the abundance of gold ore in Ghana to scam investors by advertised fake gold samples on the internet. Again, internet has created a marriage market where many people meet their prospective spouse, and yet perpetrators manipulated online victims from this opportunity. Some software applications allowed fraudsters to withdraw money from people's electronic bank accounts. The investigation further revealed that the culprits were able to execute their operations through the networks of collaborations with security agents and some banking staffs. Global networking helps the offenders to exchange ideas to facilitate their illegal activities in the cyber world.

5.2.5 Live Experiences of the Cybercrime Victims

The findings demonstrated that the majority of victims heeded to the scammers request without due diligence. In addition, victims subscribed to more than one social network

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

which exposed them into contact with many people in the social web including miscreants. It is also an undeniable fact that the respondents have interacted with individuals they have not come across in the real world. Notwithstanding these factors, some people get lured into internet fraud because of unrealistic profit ventures. The live experiences further shown that victims were quite disappointed with the police for not arresting the culprits or put them behind bars.

5.2.6 Responses and Challenges of Police Service towards Cybercrime

From the investigations, it was found out that Ghana Police Service has no specific unit that advise the State and coordinate computer crime investigations. The police officers enumerated some factors that adversely affected their operations. These include inadequate capacity building on ICT skills, and inadequate infrastructure like the establishment of the state-of-the-art digital forensic lab. Police investigators also find it difficult to obtain information from the telecom service providers to authenticate their cases.

5.2.7 Cybercrime Law

This section focused on cybercrime law contained in the Act 772 as an instrument for checking criminal behavior in the cyber space of Ghana. The research findings indicated that the law need to be reviewed to accommodate the new challenges in the cyber environment such as a succinct definition of cyber offences, the admissibility of electronic evidence in court, and the explicit provision on the extradition of offenders.

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

5.3 Policy Implications

The research unveiled that cybercrime is a threat to the Ghana's economy, peace and security. Therefore any concrete policy direction should target the offenders, victims and the law enforcement agencies. Routine Activity theory predicted that the characteristics of these stakeholders' have a reinforcing effect on one another, leading to a vicious cycle of cybercrime. Inability by the police to be steadfast on cybercrimes has eroded victims' confidence in the criminal justice system which increased the criminals' confidence to continue their operations. On this note, the researcher recommends the following as mechanisms to combat the menace.

1. The Government in collaboration with the Attorney General's department should set up a periodic process of reviewing and enhancing Ghana's laws relating to cyberspace to address the dynamics of cyber security threats. In 2014, the Ministry of Communications appointed an Adhoc technical committee to develop a national cyber security strategy for Ghana and their observation also corresponded with the research findings. The Committee acknowledged;

   > The cyber menace in Ghana had been more of cyber fraud. The popular "sakawa" menace where cyber criminals tend to dupe unsuspecting internet users from Ghana and abroad of large sums of money remain prevalent because inadequate laws hampering the law enforcers to prosecute cybercriminals. The Electronic Transaction Act (2008), has provisions for law enforcement to fight against cybercrime. However, this is not adequate and does not address fully all aspects of cyber security, especially the multi-stakeholders approach to fighting the cyber menace. (Draft National Cyber Security Policy &Strategy; Ministry of Communications, 2014: 6).

2. In order to empower national law enforcement agencies to properly prosecute cybercrimes, the government should establish a progressive capacity building programmes for officers to acquire new ICT skills and effective ways of enforcing cyber laws. The training objectives must be abreast with the current trends in cybercrime investigation techniques, adducing and the storage of electronic evidence in courts.

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

3. The government should establish an ultra-modern national digital forensic laboratory under the auspices of the Ministry of Interior. This is to avail all law enforcers a platform for detailed investigations on cybercrimes.
4. The State should further educate the public on the nature, magnitude and consequences of cybercrime in Ghana.

5. The Government as well as Non-Governmental Organizations (NGO's) should come to the aid of the youth by providing them with social intervention programmes that will keep them busy to avert any uncompromising behavior as the common knowledge taught us that the 'devil finds work for the idle hands'. The effective implementation of economic modules outlined by the government such as the National Youth Employment Programme (NYEP), and the Livelihood Empowerment Against Poverty (LEAP) can translate into food on the table, more jobs and better educational opportunities which will ultimately minimize the tendency of the youth to go into cybercrime.

5.4 Suggestion for future research

This study mainly examined the dynamics of cybercrime activities in Ghana with the specific emphases on offenders, victims and the law. However, due to time and logistical constraints, the scope of the research was scaled-down to the Accra metropolis which limited its general applicability to the larger society. This fact notwithstanding, the study can be replicated in other parts of the country to broaden our understanding of the phenomenon.

Further studies should be conducted to find out the operations of the financial institutions that provide money transfers services to ascertain the procedure customers go through

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

before they withdraw money. The argument is that money transfer requires the recipient to produce a code number from the sender and the recipient's national identification number such as passport or voter ID card, in order to redeem the money being sent. Meanwhile, some of the internet scammers pose as females to deceive their victims and the money sent to them in the name of the females they present. The relevant question is, how do the scammers circumvent these requirements?

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

BIBLIOGRAPHY

Abbat, J. (1999). *Inventing the Internet.* Cambridge, MA: The MIT Press

Abbey, E., E (2014). "Government urged to finance cybercrime combat". *Daily Graphic,* January 28, pp. 32

Abbey, E., E. (2014). "3 Nigerians busted for stealing GH¢3 million through ATM fraud". *Daily Graphic, November 16, pp.3*

Abbey, E., E. (2014). "Two grabbed for defrauding Indian businessman". *Daily Graphic, September 15, pp.71.*

Abotchie, C. (2012). *Sociology of Urban Communities*. Accra: Hans Publication.

Abotchie, C. (2012). *Treatment of Criminals and Crime Prevention in Ghana*. Accra: Hans Publications

Adeniran, A., I. (2008). The Internet and Emergence of Yahoo-boys sub-culture in Nigeria. *International Journal of Cyber Criminology, 2(2), 368-381*

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.*

Adomi, E. (2007). "Overnight Internet Browsing Among Cybercafe Users in Abraka, Nigeria. *Journal of Community Informatics, 3(2).* Retrieved December 3, 2015, from http://ci-journal.net/index.php/ciej/article/view/322/351

Agbemabiese, J. (2013). "Cyber fraud. A new force and threat to Ghana's image and security". *Daily Graphic,* April 15, pp. 7

Agyemang, K. (2014). "Doctor Sodomised a 16-year-old Senior High". *Daily Graphic, October 25, pp.3.*

Aidoo, D., Akotoye, F., & Ayebi-Arthur, K. (2012). 'Academic 419': Locating computer crime in the use of ICT for management of educational system in Ghana- The case of University of Cape Coast. *Journal of Educational Management, 6:102-111*

Alhassan, A.,M. (2014). *Equipping the Ghana Police Service with Skills in Cyber technology.* "Speech delivered by the Inspector-General of Police on the occasion of the launce of ICT workshop", January 27, 2014, Tesano-Accra.

Anderson, J. (2010). *Understanding the Changing Needs of the U.S. Online Consumer, 2010.* En

Aronowitz, S., & Di Fazio, W. (1994). *The Jobless Future*. Minneapolis: University of Minnesota.

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

Awiah, D. M. (2013) "Police grab 2 for internet fraud". *Daily Graphic, March 10, pp.71*
Black Law Dictionary (2004). (8th Ed.). US: West Publishing Co.

Bartollas, C. (1990). *Juvenile Delinquency (2nd ed.).* New York: Macmillan Publishing Company

Bartlett, J., & Miller C. (2011). *Truth, Lies and the Internet.* London: DEMOS.

Baudrillard, J. (1995). '*Simulacra and Simulations'*. Michigan: University of Michigan Press.

Bauman, Z. (2000). *Liquid Modernity*. UK: Polity Press

Boateng, R., & Olumide, L. (2011). Sakawa- Cybercrime and Criminality in Ghana. *Journal of Information Technology Impact.* Vol. 11, No. 2, pp. 85-100.

Boateng, C. (2013). "Police Update Knowledge in e-crime combating". *Ghanaian Times*, July 30, pp. 16

Bokpe, J. S. (2015). "Tears flow for Ali-Gabass as he begins 25 years jail term for defiling boy,16". *Daily Graphic*, July 14th, pp. 3

Boradhurst, R. (2006). Development in the global law enforcement of cyber-crime, policing: *An International Journal of Police Strategies & Management*, 29(3), 408-433

Brenner, S., & Kopops, B. (2004). Approaches to Cybercrime jurisdiction. *Journal of High Technology Law, 4(1), 3-44*

Brenner, S. W. (2007). *Law in an Era of Smart Technology.* Oxford: Oxford University Press.

Brenner, S. W. (2010). *Cybercrime: Criminal Threat from Cyberspace.* Santa Barbara, CA: Praeger

Brenner, S. W. (2004). Towards a criminal law for cyberspace: A new model of law enforcement. *30 Rutgers Computer and Technology law Journal, 30, 1-9*

Bryman, A. (2008). *Social Research Methods (3rd. ed.).* New York: Oxford University Press.

Burrell, J. (2008). Problematic Employment: West African Internet Scams as a Strategic Misrepresentation. *The MIT Press. Vol.4, Number 4, Fall/Winter 2008, 15-30.*

Castells, M. (2000). *The Rise of the Network Society, The Information Age: Economy, Society and Culture, Vol. I.* Oxford: Blackwell Publishing Ltd.

Castells, M. (2000). *The Power of Identity, The Information Age: Economy, Society and Culture, Vol. II*. Oxford: Blackwell Publishing Ltd

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

Castells, M.(2000). *The End of Millennium, The Information Age: Economy, Society and Culture, Vol. III*. Oxford: Blackwell Publishing Ltd

Castells, M, Fernandez-Ardevol,M, Qiu, J. & Sey, A. (2004). *The Mobile Communication: A Cross Cultural Analysis of Available Evidence on the Social Uses of Wireless Communication Technology*. A Research Report Prepared for International Workshop on Wireless Communication Policies and Prospects at the Annenberg School for Communication, University of Southern California, Los Angeles.

Castells, M, Fernandez-Ardevol,M, & Sey, A (2007). *Mobile Communication and Society.* Massachusetts. Institute of Technology, Cambridge

Cassim, F. (2009). "Formulating Specialized Legislation to Address the Growing Spectre of Cybercrime: A Comparative Study". *P.E.R, Volume12 No.4*

Chawki, M., & Abdel-Wahab, (2009). 'Nigeria tackles Advance Fee Fraud'. *Journal of Information, Law & Technology, Vol.1 (1-16).*

Choi, K. (2008). Computer Crime Victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology, 2(1), 308-333*

Chu, B., Holt, T., & Ahn, G. (2010). *Examining the Creation, Distribution, and Function of Malware On-line.* Washington D.C, Technical Report for National Institute of Justice. NIJ Grant No. 2007IJCX0018. Available at: www.ncjrs.gov./pdffiles1/nijgrants/230112.pdf

Cohen, L., & Felson, M. (1979). *Social Change and Crime Rate Trends. A Routine Theory Approach.* America Sociological Review, 44, 588-608

Cohen, L., Kluegle, R. J., & Land, K. C. (1981). Social Inequality and predator criminal victimization: An exposition and of a formal theory. *America Sociological Review 46:505-524*

Computer Crime and Intellectual Property Section, US Department of Justice, The National Information Infrastructure Protection Act of 1996, legislative Analysis (1996). Available at www.cybercrime.gov/1030anaysis.html.

Corbin, J., & Strauss, A. (2008). *Basics of Qualitative Research: Grounded Theory Procedures and Techniques (3rd.).* Thousand Oaks, CA: Sage.

Creswell, J. W. (2009). *Research Designs: Qualitative, Quantitative, and Mixed Methods Approaches (3rd ed.).* London: Sage Publications, Inc.

Creswell, J. W. (2003). *Research Designs: Qualitative, Quantitative and Mixed Methods Approaches (2nd ed.).* Thousand Oak: Sage Publication, Inc.

Creswell, J., Plano V., Gutmann, M., & Henson, W. (2003). Advanced mixed methods research designs. In Creswell, J. W. (2009). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (3rd.).* London: Sage Publications, Inc., pp. 203-224

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

Cullen, F., & Agnew, R. (2006). *Criminological theory: past to present essential readings (3rd Ed.)*. New York: Oxford University Press, pp. 5-8.

Cukier, W., Nesselrorth, E., & Cody, S. (2007). Genre, Narrative and the "Nigeria Letter" in Electronic Mail. *In Proceedings of the 40th Annual Hawaii International Conference on System Sciences, January 03-06, HICSS*. IEEE Computer Society, Washington, DC 70

Cukier, W., & Levin, A. (2009). Internet Fraud and Cybercrime. In F. Schmalleger & M. Pittaor. (Eds.), *Crimes of the Internet* (pp. 251-279). New Jersey:Pearson Prentice Hall.

Danquah, P., & Longe, B. (2011). Cyber Deception and Theft: An Ethnographic Study on Cyber Criminality from a Ghanaian Perspective. *Journal of Information Technology Impact 11(3) 169-182.*

Danquah, P., & Longe, B. O. (2012). An Empirical Test of the Space Transition Theory of Cyber Criminality: The Case of Ghana and Beyond. *African Journal of Computing & ICTs.* 4(2), 37-48.

DiMarco, H. (2003). The electronic cloak: Secret sexual deviance in cyber society. In Y. Jewkes (ed.), Dot.cons: *Crime, Deviance, and Identity on the Internet*. Portland: Willan Publishing, pp.53-67

Doyle, C. (2014). Privacy: An Overview of the Patriot Act. *Congressional Research Service.* Accessed on December 7th 2015 from https://www.fas.org/sgp/crs/misc/R41733.pdf

Duah, F. (2013). "The Growing Global Threat of Cybercrime: Implications for International Relations". A Dissertation Submitted to the University of Ghana.

Duggal, P. (2015). *Cyber Security Law*. New Delhi: Saakshar Law Publications.

Dugle, P. (2013). *"Press Coverage of Cybercrime Issues in Ghana: A Content Analysis of the Daily Graphic and Daily Guide".* A Dissertation Submitted to the Department of Information Studies, University of Ghana, Legon.

Durkheim, E. (1984 [1893]). The Division of Labour in Society. Trans. W.D. Halls. New York: The Free Press.

Durkheim, E. (1951 [1897]). Suicide: A Study in Sociology. Trans. J.A. Spaulding & G. Simpson. New York: The Free Press.

Edelman, B. (2009). Red Light States: Who Buys Online Adult Entertainment? *Journal of Economic perspectives*, 23, 209-220

Furnell, S. (2002). Cybercrime: *Vandalizing the Information Society.* London: Addison-Wesley

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

Finn, J. (2004). A Survey of Online Harassment at a University Campus. *Journal of Interpersonal Violence, 19, 468-483*

GNA (2013). "Government Develops Cyber Security Policy". *Daily Graphic,* July 31, pp. 71.

Ghana Statistical Service (2014), 2010 Population and Housing Census. District Analytical Report: Accra Metropolitan. Ghana Statistical Service, Accra

Ghana Statistical Service (2012), 2010 Population and Housing Census: *National Analytical Report.* Ghana Statistical Service, Accra.

Ghana Narcotics Drugs Law *(P. N. D. C. L 236)*

Ghana Police Service: *2013 Annual Report.*

Giddens, A. (1994). *Sociology (2nd ed.).* Cambridge: Polity Press, pp. 709

Glickman, H. (2005). 'The Nigerian '419' Advanced Fee Scams: Prank or Peril'. *Canadian Journal of African Studies. Vol. 39. Nos. 3. Pp 460-489.*

Harvey, D. (1990). *The Condition of Postmodernity*. Oxford: Blackwell Publishing Ltd.

Henderson, J. (1989). The Globalization of High Technology Production: Society, Space and Semiconductors in the Restructuring of the Modern World, London: Routledge.

Hennink, M., Hutter, I., & Baily, A. (2011). *Qualitative Research Methods*. Los Angeles: Sage Publications Inc.

Higgins, E. G. (2005). Can low self-control help with the understanding of the software piracy problem? *Deviant Behavior, 26, 1-24*

Hilbert, A. R. (1989). 'Durkheim and Merton on Anomie: An Unexplored Contrast and Its Derivatives'. *Social Problems* 36(3):242-250

Hinduja, S. (2003). Trends and patterns among Software pirates. *Ethics and Information Technology*, 5, 49-61

Holt, T., & Blevins, K. (2007). Examining sex work from the client's perspectives: Assessing johns using online data. *Deviant Behavior,* 28, 178-198

Holt, T., & Blossler (2009). "Examining the applicability of lifestyle-routine activities theory for cybercrime victimization". *Deviant Behavior, 30, 1-35*

International Communication Union (ITU) (2014). Understanding Cybercrime: Phenomena, Challenges and Legal Response. Available at: www.int/ITU-D/cyb/cybersecuirty/legislation.htm

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

International Communication Union (ITU) (2012). *Key Statistics Highlights:* ITU Data Release June 2012. ITU World Telecommunication/ICT Indicators Database. Retrieved August 2014 from http//www.itu.int/ITU/statistics/pdf

International Communication Union (ITU) (2009). *Understanding Cybercrime: A Guide for Developing Countries:* Exploratory Report to the Council of Europe Cybercrime Convention, ETS No. 185

Internet Crime Complaint Centre (IC3) 2013 Annual Report. http://www.ic3.gov/media/annualreports.aspx). Accessed on 10th November, 2014

Internet Crime Complaint Centre (IC3) 2012 Annual Report. http://www.ic3.gov/crimesschemes. Accessed on 5th January, 2015.

Jaishankar, K. (2008). Space Transition Theory of Cyber Crimes. In F. Schmallager, & M. Pittaro (Eds.), *Crimes of the Internet*. Upper Saddle River, NJ: Prentice Hall, pp. 283-301

Jones, D. (1993) "Banks move to cut currency dealing costs", *Financial Technology International Bulletin*, 10(6): 1-3

Keith, F., & Brinkman R. (2009). *A Crime Without Borders in Postmodern World*. JSTOR International journal

Kigerl, A. (2012). Routine Activity Theory and the Determinants of High Cybercrime Countries. *Social Science Review, 30*(4),470-486

Koops, B. J. (2010). The Internet and its Opportunities for Crime. In Herzog-Evans, M (ed). *Transnational Criminology Manuel.* Nijmgen, Ntherlands: WLP, pp. 735-754

Kwablah, E. (2009, February 17). Cyber crime: Giving a bad name to Ghana. *Business and Financial Times.* Retrieved September 12, 2014 from http://ghanabusinessnews.com/2009/02/17/cyber-crime-giving-a-bad-name-to-ghana

Kabay, E. M. (2008). *Computer Security Handbook,* (5th ed.), New York: John and Wiley

Kumekpor, B. K. (2002). *Research Methods and Techniques of Social Research.* Accra: SonLife Press & Service.

Kwesie, J. K. (2010). *Test Your Knowledge (IQ) in Information and Telecommunication Technology (2nd ed.).* Accra: Vestel Publication.

Ling, R., & Haddon, L (2001). *Mobile Telephony, Mobility and Coordination of Everyday Life.* Machine that Becomes Us Conference, Rutgers University, New Brunswick, New Jersey, United States of America

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

Ling, R. (2004). *The Mobile Connection: The Cell Phone Impact on Society*. Elsevier: San Francisco, United States of America.

Maccoby, E., & Levin, H., (1957). "Learning theory and the acquisition of value". *Psychological Review 1960, 67*(5), 317-331.

Marcus, C. D. (2008). Identifying potential factors of adolescent online victimization for high school seniors. *International Journal of Cyber Criminology 2(2), 346-348*

Mendell, L. R. (1998). *Investigating Computer Crime: A Primer for Security Managers.* Illinois: Charles C. Thomas Publisher Ltd.

Mensah, M. (2013). "Government to develop cyber security strategy for country". *Daily Graphic*, January 30th, pp. 32

Mensah, M. (2014). "Gvt Sets Up Data Processing Commission". *Daily Graphic, November 14, pp. 32*

Mensah M. (2015). "Data Protection Board Inaugurated". *Daily Graphic, April 25th, pp. 3*

Mensah, M. (2015). "Australian duped $2m: 9 in police grip". *Daily Graphic, February 6 pp 3.*

Middleton, B. J. (2002). *Cyber Crime Investigator's Field Guide*. New York: Auerbach Publications.

Ministry of Communications (2014). Ghana National Cyber Security Policy and Strategy: *Final Draft.*

Morse, J. (1991). "Approaches to qualitative-quantitative methodological triangulation". *Nursing Research, 40* (1), 120-123

Murphy, T. (2010). Security Challenges in the 21st Century Global Commons; *Yale Journal of International Affairs, volume 5, Issues 2: Spring/Summer 2010.*

National Development Planning Commission (2012). *2011 GSGDA Annual Progress Report*. Government of Ghana, Accra

Neuman, L.W. (2003). *Social Research Methods: Qualitative and Quantitative Approached (4th ed.).* Boston: Pearson Education, Inc.

Nukunya, G. K. (1992). *Traditional and Change in Ghana: An Introduction to Sociology*. Accra: Ghana Universities Press.

Nuknunya, G. K. (2003). *Traditional and Change in Ghana: An Introduction to Sociology (2nd ed.).* Accra: Ghana Universities Press.

Newman, G., & Clarke, R. (2003). *Superhighway Robbery: preventing E-Commerce Crime*. Cullomptom, UK: Willan Press.

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

Nyarko, N., & Addae-Madzi, J. (2015). "6 busted over Sim box fraud". *The Ghanaian Times, January 27, pp. 3*

Obiri-Yeboah, C. (2013). *How to Deliver Yourself from Criminals.* Accra: Tommi's Media

Ofori-Amankwah, E. H. (2012). *Outline of Criminal Law Lecture*. Accra: 2WENTY 3THIRD SOLUTION

Olayemi, J. (2014). "Combating the Menace of Cybercrime". *International Journal of Computer Science and Mobile Computing, Vol.3, Issues 6, pp.980-991*

Olayemi, J. O. (2014). "A socio-technological analysis of cybercrime and cyber security in Nigeria". *International Journal of Sociology and Anthropology, Vol. 6(3), pp. 116-125.*

Olowu, D. (2009). "On the Origins of Advanced Fee Fraud Electronic Mails: A Technical Investigation Using Internet Protocol Address Tracers. *The African Journal of Information System, Volume 3/ Issue 1*

Osei Darkwa, K. (2012). "Contemporary trends in cybercrime in Africa". *Ghanaian Times*, June 8, pp. 19

Pocar, F. (2004). New Challenges for International Rules against Cyber-crime. *European Journal on Criminal Policy and Research, 10(1):27-37*

Quanson, D. J. (2013). *"The Use of Information Communication Technology to Combat Financial Crime in Ghana: A Case Study of the Ghana Police Service Commercial Unit"*. A Dissertation Submitted to the Department of Information Studies, University of Ghana, Legon.

Quinn, J., & Forsyth, C. (2005). Describing sexual behavior in the era of the internet: *A typology for empirical research. Deviant Behavior, 26, 191-207*

Regoli, M., & Hewitt, D. (1997).*Delinquency in Society (3rd ed.).* New York: McGraw-Hill Companies, Inc.

Ritzer, G. (1996). *Postmodern Social Theory*. New York: McGraw-Hill Publishing

Rollins, J., & Wyler, S. (2013). Terrorism and Transnational Crime: Foreign Policy Issues for Congress. *Congressional Research Service,* retrieved December 27, 2014. http://www.fas.org/spg/crs/terro/R41004.pdf

Reyns, W., Henson, B., & Fisher, B. (2011). "Being pursued online: applying cyberlifestyle-routine activities theory to cyber stalking victimization". *Criminal Justice and Behavior, 38, 1149-1169*

Saha, T. (2014). "Indian Women at Risk in the Cyber Space: A Conceptual Model of Reasons of Victimization". *International Journal of Cyber Criminology, 8 (1), 57-67.*

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

Salifu, A. (2008). "The Impact of internet Crime on Development". *Journal of Financial Crime, 15,* 432-443

Schmalleger, F., & Pittaro, M. (2009). *Crimes of the Internet.* Saddle River, NJ: Pearson Prentice Hall

Schaefer, R. T. (2005). *Sociology (9th ed.).* Boston: McGraw-Hill, pp.182

Siegel, L., & Senna J. (1994). Juvenile Delinquency: Theory, Practice and Law (5th ed.). New York: West Publishing Company, pp195-196.

Smith, R., Grabosky P., & Urbas G (2004). *Cyber Criminals on Trial. Cambridge* (UK): Cambridge UP.

Smith, B. (2011). *"Cybercrime and the Youth in Ghana: A Study of the Sakawa Conundrum in Accra and Agona Swedru Communities"*. A Thesis presented to the Department of Sociology, University of Ghana, Legon.

Snail, S. (2009). 'Cyber Crime In South Africa-Hacking, cracking, and other unlawful online Activities'. *Journal of Information, Law & Technology (JILT)*

Snyder, F. (2001). "Sites of criminality and sites of governance". *Social and Legal Studies 10, 251-256*

Strauss, A. L. (1987). *Qualitative Analysis for Social Scientist.* Cambridge: Cambridge University Press

Suman, S., Srivastava, N., & Pandit, R. (2014). Cyber Crimes and Phishing Attacks. *International Journal on Recent Innovation Trends in Computing and Communication, 2 (2), 334-337*

Sutherland, E. H. (1939). *Principle of Criminology*. Philadelphia: Lippincott

Sutherland, E., & Cressey, D. (1978). *Principles of Criminology (10th ed.).* Philadelphia: Lippincott

Thomas, D., & Loader, B. (2000). Cybercrime: Law Enforcement, Security and Surveillance in the Information Age. London: Routledge.

Thomas, J. (2013). *Cybercrime and Criminological Theory*. San Diego: Cognella academic publishing

Tive, C. (2006). *419 Scam: Exploits of the Nigerian Con Man*. Bloomington:iUniverse

Tuffour, A. F. (2013). "CID equips investigators to fight cybercrime". *The Ghanaian Times, April 22, pp. 3*

United Nations (2005). *UN recommendations on fighting cybercrime*. http://www.crime-research.org/news/13.05.2005/1225/ . Accessed 29 December, 2014.

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

UNODC (2013). *Comprehensive Study on Cybercrime.* New York: UN

Van Der Merwe, D. (2008). *Information and Communication Technology Law*. Durban: LexisNexis

Vold, G., & Bernard, T. (1986). *Theoretical Criminology (3rd. ed.).* New York: Oxford University Press, pp 205-213.

Wall, D. S. (2001). *Crime and the Internet.* London: Routledge.

Wall, D. S. (2004). Digital realism and the governance of spam as cybercrime. *European Journal on Criminal Policy Research, 10, 309-335*

Wall, D. S. (2007). Cybercrime: *The Transformation of Crime in the Information Age*. Cambridge: Polity Press.

Warner, J. (2011). Understanding Cybercrime: A View from Below. *International Journal of Cyber Criminology*, *5*(1),736-749

Weber, A. (2003). The Council of Europe's Convention on Cybercrime. *Berkeley Technology Law Journal, 18(28): 426-446*

Wright, K., & Wright, K. (1994). Family Life, Delinquency, and Crime: A Policymakers Guide. *Research Summary. Washington DC: OJJDP. 4-21.*

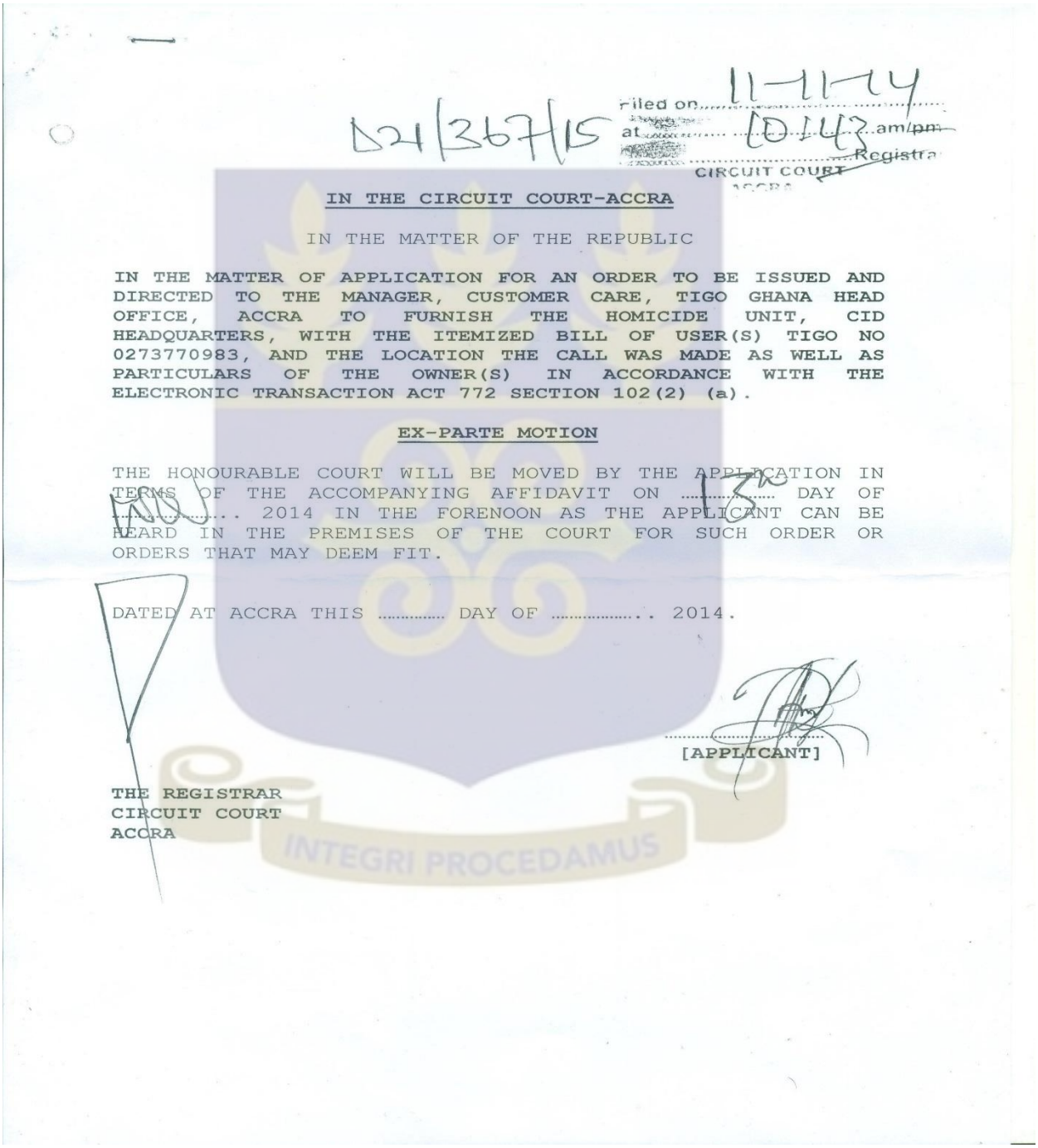
Yar, M. (2005). The Novelty of 'Cybercrime': An Assessment in light of routine activity theory. *European Journal of Criminology, 2(4), 407-427*

Yar, M. (2013). *Cybercrime and Society (2nd ed.).* London: Sage Publication, pp 6-9.

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

APPENDICES

Appendix I: The Process of Disclosing Customer's Information by Telecom Operator's in Ghana



D21/367/15

filed on 11-11-14
at 10:43 am/pm
Registra
CIRCUIT COURT

IN THE CIRCUIT COURT-ACCRA

IN THE MATTER OF THE REPUBLIC

IN THE MATTER OF APPLICATION FOR AN ORDER TO BE ISSUED AND DIRECTED TO THE MANAGER, CUSTOMER CARE, TIGO GHANA HEAD OFFICE, ACCRA TO FURNISH THE HOMICIDE UNIT, CID HEADQUARTERS, WITH THE ITEMIZED BILL OF USER(S) TIGO NO 0273770983, AND THE LOCATION THE CALL WAS MADE AS WELL AS PARTICULARS OF THE OWNER(S) IN ACCORDANCE WITH THE ELECTRONIC TRANSACTION ACT 772 SECTION 102(2) (a).

EX-PARTE MOTION

THE HONOURABLE COURT WILL BE MOVED BY THE APPLICATION IN TERMS OF THE ACCOMPANYING AFFIDAVIT ON ..... DAY OF ..... 2014 IN THE FORENOON AS THE APPLICANT CAN BE HEARD IN THE PREMISES OF THE COURT FOR SUCH ORDER OR ORDERS THAT MAY DEEM FIT.

DATED AT ACCRA THIS ..... DAY OF ..... 2014.

.....
[APPLICANT]

THE REGISTRAR
CIRCUIT COURT
ACCRA

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

Filed on 11-11-14
at 1043 hrs/pm
Registrar
CIRCUIT COURT
ACCRA

IN THE CIRCUIT COURT-ACCRA

IN THE MATTER OF APPLICATION FOR AN ORDER TO BE ISSUED AND DIRECTED TO THE MANAGER, CUSTOMER CARE, TIGO GHANA HEAD OFFICE, ACCRA TO FURNISH THE HOMICIDE UNIT, CID HEADQUARTERS, WITH THE ITEMIZED BILL OF USER(S) OF TIGO NO. 0273770983 AND THE LOCATION THE CALL WAS MADE AS WELL AS PARTICULARS OF THE OWNER(S) IN ACCORDANCE WITH THE ELECTRONIC TRANSACTION ACT 772 SECTION 102(2) (a).

IN THE MATTER OF AFFIDAVIT IN SUPPORT OF THE MOTION THEREOF

1. D/SGT. GODSWAY AMEGEE OF GHANA POLICE SERVICE STATIONED AT CID/HEADQUARTERS; ACCRA MAKES OATH AND SAY AS FOLLOWS:

2. THAT I AM THE DEPONENT HEREIN

3. THAT I HAVE THE AUTHORITY AND PERMISSION OF THE INSPECTOR GENERAL OF POLICE [IGP] TO TAKE THIS ACTION.

4. THAT THE POLICE ARE INVESTIGATING A CASE OF THREAT OF DEATH IN WHICH A SUSPECT USED HIS CELL PHONE NO. 0273770983 TO SEND THREATENING MESSAGES TO MAJOR GENERAL RTD, GHANA'S AMBASSADOR TO THE REPUBLIC OF SIERRA LEONE.

5. THAT INVESTIGATION HAS REACHED A STAGE WHERE THE ITEMIZED BILL AND THE PARTICULARS OF THE USER(S) AS WELL AS THEIR LOCATION HAS BECOME NECESSARY TO ASSIST IN THE INVESTIGATION.

6. THAT I SWEAR TO THIS AFFIDAVIT IN THE INTEREST OF JUSTICE FOR AN ORDER TO BE ISSUED AND TO BE DIRECTED TO MANAGING DIRECTOR OF TIGO GHANA LIMITED TO PROVIDE POLICE WITH THE ITEMISED BILL OF THE OWNER(S) OF TIGO NO. **0273770983** FROM 1ST APRIL TO 31ST MAY, 2014 AND ALL INFORMATION REQUESTED FOR IN PARAGRAPH 5 OF THIS AFFIDAVIT.

SWORN AT ACCRA THIS 11th DAY OF NOV 2014

BEFORE ME:

REGISTRAR
CIRCUIT COURT
28TH FEBRUARY ROAD
ACCRA

DEPONENT

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

IN THE CIRCUIT COURT OF GHANA
28TH FEBRUARY ROAD COURTS
ACCRA – A.D. 2014

COURT CASE NO. D21/367/15

IN THE MATTER OF AN APPLICATION FOR DISCLOSURE OF INFORMATION ON TIGO SIM CARD NO. 0273770983

ORDER FOR DISCLOSURE OF INFORMATION

(SGD)
H/H PATRICIA QUANSAH
CIRCUIT JUDGE

UPON READING the affidavit of **D/SGT.GODSWAY AMEGEE** of Ghana Police Service stationed at C.I.D Headquarters, Accra filed on the 11th day of November, 2014 in support of Motion Ex-parte for an Order for Disclosure of Information on the holder of **TIGO NO. 0273770983.**

AND UPON HEARING A.S.P. AMEGAH for Prosecution:

IT IS HEREBY ORDERED that **MANAGEMENT OF TIGO GHANA LIMITED** furnishes the Police with the following:

1. Particulars of the owner/user of TIGO cell phone number 0273770983.
2. Itemized bills in connection with above-mentioned cell phone number from 1st April, 2014 to 31St May, 2014.
3. Call location and information relevant and necessary for the purpose of investigations.

GIVEN UNDER MY HAND AND THE SEAL OF THE CIRCUIT COURT, ACCRA THIS 19TH DAY OF NOVEMBER, 2014.

(SGD)
SEIDU YUSIF
(R E G I S T R A R)

V.M.O.

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

Appendix II: Internet Fraudsters

The Ghanaian Times

Ghana's most authoritative newspaper

No. 17,407 ISSN: 0855-1503 Website: www.ghanaiantimes.com.gh TUESDAY, JANUARY 27, 2015 PRICE: GH¢ 2.50

6 BUSTED OVER SIM BOX FRAUD

...Through SUBAH, CID collaboration

Page 3

Dr. Alexander Tweneboah (fourth fromleft) among the suspects. In front are the equipment they used

Photo: Hannah Nkrumah

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

Appendix III: Questionnaire for Offenders

SOCIOECONOMIC BACKGROUND

1. Age of respondent: (a) <18yrs☐(a) 18-25☐ (c) 26-30☐ (d) 31& above ☐

2. Religion: (a) Islam ☐ (b) Christianity ☐ (c) Tradition ☐ (d) Others ☐

3. Educational background:(a) J.S.H ☐ (b) S.H.S ☐ Tertiary☐ Other ☐

4. Occupation: (a) Employed☐ (b) unemployed ☐

5. Please, if you are employed state the average monthly income: Gh¢700 below ☐

Gh¢700-1000☐ Gh¢1100 & above ☐

6. Is your income adequate for all needs? (a) Yes☐ (b) No ☐

7. Marital status: Married ☐ Single ☐

9. Number of Years Spent in "Sakawa" 1-2yrs☐ 3-4yrs ☐ 5yrs & above ☐

10. Who do you live with? Both Parents ☐ Single/other parents ☐

11. Number of Siblings: <4☐ 4-6☐ 7 & above ☐

12. Parents' Education: No formal edu.☐ Primary ☐ Secondary☐Tertiary ☐

13 Parents' employment backgrounds: (a) Employed☐ (a) Unemployed ☐

14. Types of Occupation; Civil Servant ☐ Self employed ☐

15. Range of parents' income if known: 100- 600☐ 700-1800☐ 1900 &

above ☐

16. Were parental incomes adequate for all needs? Yes ☐ No ☐

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

Appendix IV: Interview Guide for Offenders

EXPLORING THE MEANING AND VARIOUS FORMS OF "SAKAWA"

What is cybercrime/Sakawa
Please, state the various forms of cybercrime you know/ which of these were you involved in? (probe)
Is your family aware of your indulgence? Yes ☐ No ☐
Why Yes or No

MOTIVATIONAL DRIVES

Why did you get involve in Sakawa business? (Probe)
Can you justify your reason for indulgence?
How much, on the average, do you realize from each operation and how often do you gain from your potential client (Victims)

OPPORTUNITIES /PROCESS OF BECOMING SAKAWA

What category of persons do you normally targeted?

What criteria do you use in selecting your clients (potential victims?) i.e romance, business, and social relationships?

How do you go about this business?

Please explain some of the strategies you used to entice your client

Is the same procedure applicable to all potential victims? Yes ☐ No ☐

If you had to physically interact with your client, would you still indulge in the business? Yes ☐ No ☐

What are your perceptions of the legal consequences?

Do you have a partner who engaged in Sakawa activities inside or outside the country? Yes ☐ ☐ No

Explain your relationship with him

Is there any secret to your success Yes ☐ No ☐

Some of your colleague believes their success in this job depends on supernatural powers; do you share the same view?

If you hit the scam how do you receive the money from the financial institutions?

What do you use the money for?

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

Appendix V: Questionnaire for Victims

SOCIOECONOMIC BACKGROUND

1. Age of respondent: (a) 18-23☐ (a) 24-30 ☐ (c) 31-40☐ (d) above 40 ☐

2. Ethnicity: Akan☐ Ewe ☐ Ga ☐ Hausa☐ Other ☐

3. Religion: (a) Islam ☐ (b) Christianity☐ (c) Tradition☐(d) Others☐

4. Highest education: Primary☐ (b) Secondary☐ Tertiary ☐

5. Marital status: Married ☐ Single☐ Divorced ☐

6. What work do you do……

7. Approximately how much do you earn in every month:

Gh¢300-600 ☐ Gh¢700-2000☐ Gh¢2100 and above ☐

Appendix VI: Interview Guide for Cybercrime Victims

EXPLORING THE EXPERIENCES OF THE CYBERCRIME VICTIMS

How did you become a victim of cybercrime?

Can you explain in details how the perpetrators successfully defrauded you?

What motivated you to stay in touch with the perpetrator?

Why did you remit money to the culprit?

How much money did you remit?

How many social networks do you subscribe to? 1☐ 2☐ 3 and above☐

Do you update your social network accounts regularly? Yes☐ No☐

Do you allow strangers to access your social network including personal information? Yes☐ No☐

Have you utilized online service in acquiring friends? Yes☐ No☐

Do you think that you were hypnotized by the culprit in anyway?

Did you at any point have doubts about the credibility of the culprit?

Did you report the incidence to the police? (Explain further; ie police reactions and the outcome)

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

Appendix VII: Interview Schedule (Police)

My name is Daniel Ennin, a graduate student from the University of Ghana. As a requirement for Mphil programme in Sociology, I am conducting a study on cybercrime activities in Ghana with the aim of gaining an in-depth knowledge on the phenomenon. I humbly request you to grant me an interview. Your participation is very crucial towards the success of this research. The primary goal for this interaction is to explore the responses and challenges of the Ghana Police Service towards cybercrime. Information gathered will be used purposely for this research and you are also assured of strict confidentiality.

Thank you.

RESPONSES AND CHALLENGES

Rank……

Number of years in the Service……..

What is the primary function of your department?

What is cybercrime/Sakawa

Does the Ghana Police Service have a working definition for cybercrime/Sakawa

Who are involved? (i.e. Offenders &Victims)

What in your opinion are predisposing factors of "Sakawa" activities in Ghana?

What legal provisions or instruments are available in Ghana to address cybercrime?

Why many cybercrime cases are pending for investigation?

What challenges do police encountered in its efforts to combat cybercrime?

How can the challenges be overcome, in your view?

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

Appendix VIII: Interview Schedule (Legal Practitioners)

My name is Daniel Ennin, a graduate student of the University of Ghana. As a requirement for Mphil programme in Sociology, I am conducting a study on cybercrime activities in Ghana with the aim at gaining an in-depth knowledge on the phenomenon. I humbly request you to grant me an interview. Your participation is very crucial towards the success of this research. The primary goal for this interaction is to explore the efficacy and limitations of the ***Electronic Transaction Act (Act 772)****, as an instrument for promoting legal certainty in the cyber space of Ghana. The synopses for the discussion are; the criminalization of the cyber offences; admissibility of electronic in the cybercrime proceedings, and the jurisdictional issues. Information gathered will be used purposely for this research and you are also assured of strict confidentiality.*

Thank you.

SOME LEAD QUESTIONS

What is the main purpose of the Act?

Can a cyber-offender who is outside the country be tried under this Act (probe)

Do the Courts accept intangible evidence in relation to cybercrime cases?

What in your opinion are the limitations of the Act if any

Why is punishment not clearly stated as in the drug trafficking law (imprisonment without fine & confiscated of assets)

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

Appendix IX States the Article 2 to 10 of the CoE Convention on cybercrime in detail

Offences against the confidentiality, integrity and availability of computer data and system.

Article 2- Illegal access

Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or nay part of a computer system without right. A party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 3- Illegal interception

Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer carrying such computer data. A party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 4- Data interference

1 Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

2 A party may reserve the right to acquire that the conduct described in paragraph 1 result in serious harm.

Article 5- Systems interference

Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting deteriorating, altering or suppressing data

Article 6- Misuse of devices

1 Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

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

a. the production, sale, procurement for use, import, distribution or otherwise making available of:

i. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Article 2 through 5;

ii. a computer password, access code, or similar data by which the whole or nay part of a computer system is capable of being accessed, with the intent that it be used for the purpose of committing any of the offences established in Article 2 through 5

b. the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A party may require by law that a number of such items be possessed before criminal liability attaches.

2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Article 2 through 5 of the Convention, such as for the authorized testing or protecting of a computer system.

3. Each party may reserve the right not to apply paragraph I of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a, ii of this article.

Computer-related offences

Article 7-Computer –related forgery

Each party shall adopt such legislative and other measures as may necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it may be considered or acted upon for legal purposes as if were authentic, regardless whether or not the data is directly readable and intelligible. A party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Article 8- Computer-related fraud

Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

a. any input, alteration, deletion or suppression of computer data,

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

b. any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

Content-related offences

Article 9- Offences related to child pornography

1. Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right the following conduct:

a. producing child pornography for the purpose its distribution through a computer system

b. offering or making available child pornography through computer system

c. distributing or transmitting child pornography through a computer system

d. procuring child pornography through a computer system for oneself or for another person.

e. possessing child pornography in a computer system or on a computer-data storage medium.

2. For the purpose of paragraph 1 above, the term 'child pornography' shall include pornographic material that visually depicts:

a. a person engaged in sexually explicit conduct;

b a person appearing to be a minor engaged in sexually explicit conduct realistic images representing a minor engaged in explicit conduct

3. For the purpose of paragraph 2 above, the term 'minor' shall include all person under 18 years of age. A party may, however, require a lower age-limit, which shall be not less than 16 years.

4. Each party may reserve the right not to apply, in whole or in part, paragraph 1, sub-paragraph d, and e, and 2, sub-paragraph b and c.

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

Offences related infringements of copyright and related rights

Article 10- Offences related to infringements of copyright and related rights

1 Each part shall adopts such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that party, pursuant to the obligations it has undertaken the Paris Act of 24 July revising the Bern Convention for the protection of Literature and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed willfully, on a commercial scale and by means of a computer system.

2 Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Originations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual property rights and the WIPO performances and phonograms treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed willfully, on a commercial scale and by means of a computer system.

3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and such reservation does not derogate from the party's international obligations set forth in the international instruments referred to in paragraph 1 and 2 of this article