UNIVERSITY FOR DEVELOPMENT STUDIES

CYBERCRIME AND ITS IMPLICATIONS ON SECONDARY EDUCATION IN THE TAMALE METROPOLIS OF THE NORTHERN REGION OF GHANA

RUHIYA ABU

2020

UNIVERSITY FOR DEVELOPMENT STUDIES

CYBERCRIME AND ITS IMPLICATIONS ON SECONDARY EDUCATION IN THE TAMALE METROPOLIS OF THE NORTHERN REGION OF GHANA

BY

RUHIYA ABU (BA INTEGRATED BUSINESS STUDIES)

UDS/MSA/0114/15

THESIS SUBMITTED TO THE DEPARTMENT OF SOCIAL, POLITICAL AND HISTORICAL STUDIES, FACULTY OF INTEGRATED DEVELOPMENT STUDIES, UNIVERSITY FOR DEVELOPMENT STUDIES IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF MASTER OF PHILOSOPHY DEGREE IN SOCIAL ADMINISTRATION

APRIL, 2020

DECLARATION

Student

I hereby declare that this thesis is the result of my own original work and that no part of it has been presented for another degree in this University or elsewhere:

Candidate's

Signature:……Date:……

Ruhiya Abu

Supervisor

I hereby declare that preparation and presentation of the thesis was supervised in accordance with the guidelines on supervision of thesis laid down by the University for Development Studies.

Supervisor's Signature:…….Date:…….

Dr. Frank K. Teng-Zeng

ABSTRACT

This research is about the study of cybercrime and its implications on secondary education in the Tamale metropolis. Cybercrime activities have several implications on the various facets of students' academic career at the Senior High School level and hence the main objective of this study was to examine the implications of cybercrime on secondary education. Differential association and general strain theories anchor the study. The 120 participants (respondents) in the study were SHS students (40 of them were involved in cybercrime activities), key informants (8) and internet café operators (4). Cross-sectional design was used for the study. This helped to triangulate both qualitative and quantitative methods. Data were analysed using SPSS version 21 to estimate the frequencies, percentages and the Kendall's coefficient of concordance. Audio files were also transcribed and analysed to achieve the objectives of the study. The simple random, purposive and snowball techniques were used to select respondents. The study reveals that the major causes and motivating factors that are responsible for the involvement of individuals in cybercrime according to respondents varies and it is determined based on different factors such as peer group influence, unemployment, easy access to internet, weak laws and corruption. From the study results, a sizeable number of cybercriminals in Ghana falls within the youthful age. None of them indicated there is a law in the statute books that addresses these types of crimes and hence its illegality and punishment by law. Some of these *Sakawa* guys cater for themselves and their siblings' education from basic to tertiary level with the aid of the cybercrime activities. In conclusion, cybercrime has a negative impact on secondary educational attainment since some of them have abandoned their education.

ACKNOWLEDGEMENTS

My sincere and deepest gratitude goes to my principal supervisor, Dr. Frank K. Teng-Zeng, for his guidance and support through the entire course. You will forever remain an inspiration to me. I am most grateful to Mr. Stephen Ameyaw for his support and useful comments. My appreciation would be incomplete without thanking my family, most especially my lovely dad for the financial support.

TABLE OF CONTENTS

DEDICATION

This thesis is dedicated to my supervisor, my family and all friends.

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE

INTRODUCTION

1.0 Background

Since the Canadian Communication theorist Marshall McLuhan (1964) coined the expression 'global village' to describe the increasing interconnectedness of societies in the world fuelled by electronic communication, the world construed as "global village" is now a cliché. The upsurge in the use of Information and Communication Technologies (ICTs) especially internet service activities has opened up and integrated most (if not all) economies across the globe. For instance, the United Nations reported that, in 2011, more than one million unique Internet Protocol (IP) addresses globally functioned as command and control servers for botnets (UNODC, 2013). This phenomenon has undoubtedly brought rapid development to many nations. Despite the positives, the upsurge of internet connectivity and access has brought with it an evolution of cybercrimes which constitutes not just a threat to the security of many nations, but also has huge implications to other sectors of their economies.

Shinder (2002) defines cybercrime as any criminal offenses committed using the internet or another computer network as a component of the crime. Cybercrimes are offences that are committed against individual or group of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly using modern telecommunication networks such as internet

and mobile phones. Such crimes may threaten a nation's security and financial health (Akogwu, 2012).

The youth in every society is of great importance and concern because they are looked upon as the leaders of tomorrow. Ghana, like many other countries across the world, constitute a ripe ground where Cybercrimes are been perpetrated. Olaide and Adewole (2011) asserted that a sizeable number of criminals in Ghana fall within the youthful age. The youths at present have discovered different ways of using the internet in doing different types of criminal activities. The incident can rightly be said to be on the increase in the country due to lack of security awareness and under reportage. Although some people's level of knowledge of the net is observably just for chatting with their friends and get information, most of them may not be in the position to protect their data or information and computer from malicious programmers (Akogwu, 2012).

A report by the International Telecommunication Union (ITU, 2012) reveals that internet users in Ghana had reached 7,958,675 as at June, 2016. The internet is the driving force for growth of e-business and e-governance. Ghana's growth potential is limited by the lack of infrastructure (connectivity) and equipment. The Government of Ghana is making concerted efforts to create a 'knowledge-based economy' thereby making Ghana an information and communication technology (ICT) – driven economy. The Government of Ghana in 2006 launched the national fibre-optic backbone project to enhance internet connectivity throughout the country. The objective of the study was to provide a reliable and cost effective access to broadband connectivity nationwide to improve the use of Information and Communication Technologies (ICTs) in the country and also enhance e-

business and e-governance. ICTs and associated applications, especially internet penetration also comes with it the growing threats of cybercrimes

However, most studies that focus on Cybercrime largely concentrates on situations in the western world, forgetting that the nature of Cybercrime is such that geographical and political boundaries are being rendered irrelevant. A person who has access to computer and connected to the internet might be participating, attempting or planning a criminal act anywhere in the world (Kumar, 2003). Awe (2009), confirmed that computer attacks can be generated by criminals from anywhere in the world, and executed in other areas, irrespective of geographical location; and often, these criminal activities can be faster, easier and more damaging with the use of the internet.

The above statement shows that cybercrime is a global issue and as such, has become an image nightmare for the Ghana government to identify the remote causes and proffer solution. Cybercrime is a relatively new phenomenon in Ghana. Its presence was first reported in Ghana between 1999 and 2000; this was primarily related to credit card fraud (Warner, 2011). Ghana has recently come to be recognised as a major hub for cyber-criminal activity. A report published in 2010 showed that Ghana gained a bad reputation of being one of the top ten cybercrime generating states worldwide along with Anglophone African neighbours Nigeria and Cameroon (Warner, 2011). Moreover, a prior report also revealed that Ghana was the second most frequently blocked location by U.S. online retailers sceptical of fake orders from Internet scammers (Kwablah, 2009 as cited in Warner, 2011 page 74). However, Warner (2011) was quick to note that the United States (followed by the U.K) is the leading state when it comes to involvement in cybercrime.

Warner (2011) has identified three major types of cybercrime in Ghana. These include false identity where criminals use social network site like Facebook and internet dating sites like Match.com to defraud their victims; fake gold dealers and estate fraud.

Cybercrimes have significant effect on economies of nations for that matter, the development of countries. In 2011, information from the Norton Cybercrime indicated that over 74 million people in the United States became victims of cybercrime activities in 2010. Consequently, $32 billion in direct financial losses occurred. Furthermore, the statistics indicate that about 69 percent of adults that are online have been victims of cybercrime resulting in 1 million cybercrime victims a day (Saini, Rao and Panda, 2012). Given the fact that many consumers have become reliant on computers, networks, and the internet, the risk of being subjected to cybercrime is high. Some of the surveys conducted in the past have indicated as many as 80% of the companies surveyed acknowledged financial losses due to computer breaches; the approximate number impacted was $450 million (Saini *et al*., 2012). Each week we hear of new attacks on the confidentiality, integrity, and availability of computer systems. This could range from the theft of personally identifiable information to denial of service attacks. As the economy increases its reliance on the internet, it is exposed to all the threats posed by cyber-criminals. Stocks are traded via internet, bank transactions are performed via internet, purchases are made using credit card via internet. All instances of fraud in such transactions impact the financial state of the affected company and hence the economy. The disruption of international financial markets could be one of the big impacts and remains a serious concern. The modern economy spans multiple countries and time zones. Such interdependence of the world's economic system means that a disruption in one

region of the world will have ripple effects in other regions. Hence any disruption of these systems would send shock waves outside of the market which is the source of the problem (Saini *et al*., 2012). Cybercrimes thus, have devastating impact on all spheres of a country's life; social, economic, political and security. The threats and crimes associated with cyber activities ought to be dealt with by all stakeholders to ensure a reliable solution to the ensuing threats posed by these activities.

1.1 Problem Statement

Cybercrime has become a threat to the efforts aimed at globalising the world economies. In Ghana, the upsurge of internet activities has certainly contributed towards the socio-economic development of the country. However, it has also brought along an emergence of new forms of criminal activities known as cybercrimes (Boateng, Longe, Mbarika, Avevor and Isabalija, 2010).

Ghana's strive to achieve greater heights in ICT development across the various levels of education, particularly the secondary educational level will be jeopardised if steps are not taken to address the issue of cybercrime (Boateng *et al*, 2010). Statistics indicate that 90% of cyber criminals in Ghana are male less than 30 years of ages who reside in or near urban centres where access to internet cafes is easy (Warner, 2011). Similarly, Okeshola and Adeta (2013) emphasised that the youth of school going age at present have discovered various ways and means of using the internet in committing various forms of cybercrime. A study by Abia *et al* (2010) found that 15% of students in Ghana were scammers, 95% of the students made friends with scammers and 65% of scammers lost focus on education

and eventually dropout of school. Government of Ghana has recognised that cybercrime is a threat to the country and is beginning to take measures to combat it (Warner, 2011). Various researchers have indicated that cybercrime is very difficult to deal with because of its nature. Boateng et al., (2010) concluded that the fact that there are limited options to address the issue of Cybercrime, there is the need for more research to be conducted in the field of this crime.

In the Northern Region of Ghana, the use of computers by the youth, especially the youth in the Senior High is on ascendency. Ennin (2015) suggests that the use of ICT in schools have helped students to improve their learning and reading skills through the use of internet. Even though the use of internet had helped students to improve their academic performance in the Northern Region of Ghana, a study by the Ministry of Gender, Children and Social Protection (2018) indicates the 25% of children have access to mobile phones and the children use the phones for various dubious purposes. Although, issues regarding to cybercrime had gained deep root in topical events, studies conducted by (Boateng *et al*, 2010) focused on cyber deception and theft. Also, ethnographic studies on cyber criminality from a Ghanaian perspective by Danquah and Longe (2011), Warner, (2011) and Barfi et al., (2018) laid emphasis on the perception of cybercrime. It is important noting that little had been done on cybercrime relating to students in the Senior High School in the Tamale Metropolis in the Northern Region of Ghana. The question is why in spite of the danger of cybercrime on the development of the Senior High School Edication, there is limited empirical studies on the subject. The study sought to examine extent of cybercrime and its implications on secondary education in the Tamale Metropolis in the Northern Region of Ghana.

1.2 Research Questions

What are the implications of cybercrime on secondary education in the Tamale Metropolis of Northern Region of Ghana?

1.3.1 Specific Research Questions

i. What is the level of awareness of SHS students with regards to cybercrime in the Tamale Metropolis of the Northern Region of Ghana?

ii. What are the causes of cybercrime among students in the Tamale Metropolis of the Northern Region of Ghana?

iii. What are the effects of cybercrime on Senior High Schools in the Tamale Metropolis of the Northern Region of Ghana?

1.4 Objectives of the Study

The main objective of this study is to examine the implications of cybercrime on secondary education in the Tamale Metropolis of Northern Ghana. The specific objectives are:

i. To assess the level of awareness of SHS students with regards to cybercrime in the Tamale Metropolis of the Northern Region of Ghana.

ii. To identify the causes of cybercrime among students in the Tamale Metropolis of the Northern Region of Ghana.

iii. To analyse the effects of cybercrime on senior high schools in the Tamale Metropolis of the Northern Region of Ghana.

1.5 Significance of the study

At present, there are inadequate empirical studies on cybercrime in Northern Ghana. The existing literature does not provide linkage between cybercrime activities and secondary education (Boateng et al., 2010; Danquah and Longe, 2011; Warner, 2011). This study therefore, will serve as a useful document for policy makers, government, ministries, and non-governmental organisations among others who are interested in preventing cybercrime in secondary schools.

The study would help the Ministry of Information to formulate polies to govern internet cafés in the northern region and the country at large to prevent children under eighteen years from using the service at midnight. The findings of the study would also help teachers and parents to monitor the activities of students on how they use the internet service for and how they are being influenced by friends indulged in such criminal activities in the Metropolis. The study would help to create awareness of students at the Senior High Schools as the consequences of the cybercrime and that will deter them from entangling themselves such criminal act. Again, the study will no doubt serve as a relevant material for further studies on the subject.

1.6 The Scope of the Study

The study was limited to the Tamale Metropolis in the Northern Region of Ghana. The study focused on the implications of cybercrime on secondary education in the Metropolis. In addition, due to the nature of the topic under investigation, the study collected detailed information from students of Senior High Schools, teachers, and internet café operators among others. The reason for this was to enable the researcher, the ability to ascertain what

actually instigate students to indulge in cyber activities. This enabled her to collect accurate data regarding the phenomenon under study.

1.6 Organisation of the study

The study is organised into five chapters. Chapter one consists of the introduction of the study, which encompasses; the background of the study which analysis the implication of cybercrimes on secondary education from the world's perspective before it was narrowed down to the study area. The problem statement also highlighted the issues from the Ghanaian perspectives and narrowed to the reality on the ground. The chapter further discusses the study questions and objectives for which the study aims at achieving it, significance of the study which indicated the importance of the study to society and to the existing knowledge, the scope of the study was considered and this indicates the reason for which the study was limited to some specific respondents and the geographical context.

Chapter two looks at a review of the available literature relevant to the work, it encapsulates the general concepts of the study and theory used to anchor the study. The literature was reviewed under the following themes: definition of concept, where important concepts such as crimes, secondary education, cybercrime, forms of cybercrime, the history of cybercrime, the upsurge of cybercrime among others were appropriately reviewed.

Again, chapter three outlined the research methodology adopted in conducting the study. This includes the study profile, the research design, target population, sample size, sampling techniques, and sources of data, data collection techniques, data collection

instrument and the data analysis. Additionally, validity and reliability of the data, limitations and delimitations were all captured under chapter three.

Chapter four focused on data presentation and analysis which deals with demographic characteristics of respondents and other four thematic areas relevant to the topic under investigation. The presentation and analysis was taking into cognisance of the rational choice theory and differential association theory and other relevant literature to anchor the study. The concluding chapter, chapter five deals with the summary of major findings from the study, conclusions drawn from the findings and recommendations made to ameliorate the situation.

CHAPTER TWO

LITERATURE REVIEW

2.0. Introduction

This chapter reviews literature on cybercrime in Ghana and across the world. The literature is reviewed on the headings as follows: definition of concepts in relation to the topic under study; causes of cybercrimes; cyber security in perspective;, activities on cyber security; cybercrimes in Ghana: history, paradigms, profiles and responses; the upsurge of cybercrime ("sakawa") in Ghana; cybercrime and local legislature; internet connectivity and cybercrimes; legal components for cybercrime prosecution; awareness of cybercrime among students; effects of cybercrime; and theoretical and conceptual perspectives of crime.

2.1 Definition of Concepts

This section takes into cognizance the various variables relevant to the study. These include education, secondary education, ICT, crime and its types, overview of cybercrime, cybercrime and its forms or types.

2.1.1 The Concept of Education

Kumar and Ahmad (2008) posits that the term "Education" was derived from two Latin words Educare (Educere) and Educatum. They explain that the educare means to train or mould or to bring up or to lead out or to draw out propulsion from inward to outward. The authors explain that the term "Educatum" means the act of teaching or training. The writer

asserts that education aims to provide a nourishing environment that would facilitate or bring out and develop the potentialities in an individual. They further continue that the term educare mainly implies the development of the latent faculties of the child. According to Frobel (1885) cited in Fernández-Oliveras and Oliveras (2015 pp. 40) views education as the process by which the learner develops its inner potential in a manner in order to participate meaningfully in the external environment. He further continues that education aims at expanding the life of the individual in order to participate in the pervading spirit which manifests and realizes itself in and through the whole universe. Redden and Ryan (1956) cited in Carmody (2011) also argue that education is the deliberate and systematic influence exerted by the mature person upon the immature through instruction, discipline and harmonious development of all the powers of the human being.

Hornby (1984) cited in Adu-Agyem (2012) states that education is the process by which the mind develops through learning at school, college, or university. He adds that it is also the knowledge and skills that one gains from being taught. Additionally, Adu-Agyem (2012) explains education as the enlightenment of an individual from darkness to light, thereby pushing away the frontiers of ignorance and discovering truth. This corroborates the findings of Adu-Gyamfi, Donkoh and Addo (2017) when he explains education as the act of transferring knowledge in the form of experiences, ideas, skills, customs, and values, from one person to another or from one generation to generations. To him, education is widely acknowledged as the foundation of civilization and development. A report by National Council of Educational Research and Training in Ghana (NCERT, 2014) views education as the process which seeks to develop the innate or the inner potentialities of humans.

Education can therefore be said to be the systematic process through which a person is transformed by equipping him/her with the requisite knowledge and skills to be able to function properly in any given society. The aim of education is to offer a training to the citizenry to make them better persons in the society and to enable them contribute meaningfully to the society. In Ghana, it is believed that the educational system is of good structures equipping the youth with relevant skills for survival. According to Graham (2013), there had been a myriad of educational system since 1592. In 1980s, the educational system at that time was geared from purely academic to more of manpower needs. The writer indicates that the 1987 educational reforms suggested first nine years from the basic education. The results of Graham show that every year, over five hundred thousand students are able to take part in the Basic Education Certificate Examination (BECE) at the end of Junior High School Form Three and those who excel are admitted into the senior high schools.

2.1.2. The Concept of Secondary Education

According to Entwistle (2013), secondary education serves as a bridge between elementary and higher education and prepares young persons between the age group of 14-18 for entry into higher education. Jacob and Lehneh (2011) postulate that secondary education is widely believed to provide the optimum setting to prepare young people, predominantly adolescents, for healthy and productive adult lives, including participation in social, political, and economic spheres. In addition, the writers argue that for countries to compete in the global economy, a significant number of citizens needs secondary education in order to acquire the specific skills and aptitudes necessary for an increasingly technology driven market place. Adu-Gyamfi et al., (2017) espouses that secondary education in Ghana bears

the responsibility of providing a systematic introduction to knowledge including technical know-how; to train high-level workers in order to provide highly skilled future university graduates. Duflo, Dupas and Kremer (2017) contend that many people in Ghana see secondary education as having potentially transformative economic and social impacts on both boys and girls. The writers maintain that, because secondary education is very important, the United Nations have captured it in the Sustainable Development Goals (SDGs), specifically goal four, aims to ensure that all girls and boys complete free, equitable and quality primary and secondary education leading to relevant and effective learning outcomes by 2030.

2.1.3 The Concept of Information and Communication Technology

According to Sarkar (2012) information and communication technology (ICT) is used to communicate and integrate telecommunications which takes into accounts telephone lines and wireless signals. The writer adds that ICT is a necessary software that is used to store audio-visual systems which enable a person to access, transmit, store and more importantly manipulate information. The writer maintains that the term 'ICT' refers to combining audio-visual and telephone networks with computer networks through a single cabling or link system. Cocchia (2014) argues that the concept ICT does not have a definite or universal definition. He continued that the broadness of ICT covers any product that stores, retrieves, manipulates, transmits or receives information electronically in a digital form. The writer posits that the concept, the methods and application of ICT keeps evolving on almost daily basis. The writer was emphatic that ICT has helped to merge the telephone

network with the computer network system with the use of a single unified system of cabling or signal distribution and management.

Walsham (2012) espouses that ICT has witnessed a tremendous and phenomenal growth in many countries, especially in education. This has influenced the life of people, particularly students to improve on their academic performance. The author stresses that the ICT has had a strong impact on society over the last sixty years. He explains that ICT is visibly present in the use of computers, smart phones, information search, robotics and intelligent agents which has helped to boost the economy of countries, especially, in the develop countries. Also, the writer asserts that ICT has had greater impact on large number of application areas including medicine, energy production, healthcare, finance, public management, and transport logistics among others. The writer was of the view that the remarkable progress of ICT has enabled people to get prompt access to the required information they desire. He said technological advancement in modern times stimulates the interest of teachers and that of children to improve both teaching and learning skills in schools. The use of ICT has helped to enhance quality and value of education especially through integration. He continues that ICT in modern society contributes to universal access to education, equity in education, delivery of quality learning and teaching, efficient education management and administration and teachers' professional development. This implies that ICT has played a pivotal role in promoting and enhancing education worldwide.

Additionally, Rouse (2005) cited by Ekwonwune, Egwuonwu, Elebri and Uka (2016) affirms that ICT is any communication device or application that encompasses radio,

television, cellular phones, computer software and hardware network and satellite systems. This takes into account the video conferencing and distance learning in both tertiary and second cycle institutions. A report by the UNESCO (2009) refers ICT to all technologies used to communicate, create, manage, access, gather, and distribute information. Malekani (2018) views ICT as the main driver of the Fourth Industrial Revolution and state. He continues that ICT has also been introduced in the Secondary schools and examinable by WAEC in Ghana. It is to prepare the youth to develop relevant knowledge and skills for the future drive towards information and knowledge-based economy. Even though, ICT has contributed tremendously to the education, it exposes the youth to potential cyber-threats and engagement in cybercrime activities. The writer attributes the cause to the inadequate acquisition of knowledge in the use of internet by the teachers. To the writer, inadequate knowledge in the area caused the youth to abuse the use of ICT or internet to enrich themselves.

2.1.3. The Concept of Crime

According to Morrison (2013), crime is any action or omission that causes harm in a situation that the person or group responsible ought to be held accountable and punished, irrespective of what the law books of a state say. He continues that crime can be seen as an action against the law of God, whether as revealed in the holy books, such as The Bible, Koran, or Torah, or that we instinctively recognize as against God's will, irrespective of what the law books of a State say. To him, if the laws of the state allow something that we know to be against God's will it does not change its status as crime. He explains that crime is an act or omission that is defined by different nations in which it occurred so that

punishment should follow from the behaviour. He lays emphasis that if there is no public authority capable or ready to police social activity and punish offenders, then there is no crime. The writer's position is that crimes and criminals only exist when a public body has judged them such according to accepted procedures. Therefore, it is worth noting that without the state and the criminal law there is no crime and without criminal justice systems, there are no criminals. The author posits that crime is tied to the formal social control mechanism of the State.

Similarly, Reid (2015) views crimes as acts or omissions forbidden by law that can be punished by imprisonment and/or fine. He cited murder, robbery, burglary, rape, drunken driving, child neglect, and failure to pay your taxes as common examples of crime. Cooley (2017) argues that crime involves the idea of a public as opposed to a private wrong with the consequent intervention between the criminal and injured party by an agency representing the community as whole. Crime is thus the intentional commission of an act deemed socially harmful; or dangerous and the reason for making any given act a crime is the public injury that would result from its frequent participation. The society therefore takes steps for its prevention by prescribing specific punishments for each crime.

The Criminal Code of Ghana 1960 (Act 29) clause …defines crime as both the act, or action and the intent to commit the act. The code continues to define it as the breaking of rule(s) or regulation(s) for which a governing authority via mechanisms such as legal systems can ultimately prescribe a conviction (Adinkrah, 2011).

Contrary, Downes and McLaughlin (2016) opines that the assertion by Durkheim that crime is both normal and functional was criticized. The authors explain that to the realist point of view crime is a very real problem for victims and for society and that the sociology of crime and deviance should inform policy-makers in terms of how to prevent crime. According to them the Marxists argue that Durkheim fails to consider where the consensus comes from and in whose interests it exists. They indicated that the laws are made by the state, usually working in the interests of the ruling class. Instead of there being a value consensus in the interests of society, there is ideology or hegemony in the interests of capitalism.

2.1.4 Types of Crime

A report by NIBRS (2015) categorizes crimes into three types. These are; Crimes Against Persons, Crimes Against Property and Crimes Against Society. These crimes have been aggravated by the invention and upsurge in internet activities. Therefore, they are closely linked with cybercrimes.

2.1.4.1 Crime Against Persons

Crime committed by a human being against another is defined as crime against persons (NIBRS, 2015). The NIBRS (2015) considered among others crime such as aggravated assault, forcible sex offenses, non-forcible sex offenses, and kidnapping/abduction. They explain murder as the willful killing of one human being by another. The stress that any death due to injuries received in a fight, argument, quarrel, assault, or commission of a crime is counted as a murder.

Aggravated assault was indicated that as one of the crimes against persons. They describe aggravated assault as the unlawful attack by one person upon another for the purpose of inflicting severe or aggravated bodily injury. The said that aggravated assault is usually accompanied by the use of a weapon or by other means likely to produce death or great bodily harm. To them, an attempted aggravated assault involves the display of or threat to use a gun, knife, or other weapon which include serious personal injury.

Forcible sex offense is any sexual act directed against another person, forcibly and/or against that person's will; or not forcibly or against the person's will where the victim is incapable of giving consent because of his/her temporary or permanent mental or physical incapacity.

2.1.4.2 Crime against property

Any act that elicits harm or destroys assets and valuable belongings of people (properties) is considered to be a crime against property (NIBRS, 2015). There are several crimes under this type of crime. These include arson, bribery, and criminal mischief/damaged property, fraud, larceny, motor theft, Counterfeiting/Forgery among others. NIBRS (2015) alludes that arson is the willful or malicious burning or attempting to burn, with or without intent to defraud, a house, public building, motor vehicle or aircraft, personal property of another. Afari-Boateng (2014) argues that larceny is the unlawful taking of property from possession of another. He cites an example like thefts of bicycles or automobile accessories, shoplifting, pocket-picking, or the stealing of any property or article which is not taken by force and violence or by fraud. Puzzanchera (2010) emphasizes that larceny is the unlawful taking, carrying, leading, or riding away of property from the possession or constructive possession of another; attempts to do these acts are included in the definition.

This crime category includes shoplifting, pocket-picking, purse-snatching, bicycle thefts, and so forth, in which no use of force, violence, or fraud occurs. In addition, fraud is the intentional perversion of the truth for the purpose of inducing another person or other entity in reliance upon it to part with something of value or to surrender a legal right. This offense includes the fraudulent conversion and obtaining of money or property by false pretenses. Confidence games and bad checks, except forgeries and counterfeiting, are included. Gilbert (1997) cited in Vaisu, Warren and Mackay (2003 pp. 66) also defines fraud as an act using deceit such as intentional distortion of the truth of misrepresentation or concealment of a material fact to gain an unfair advantage over another in order to secure something of value or deprive another of a right. To him fraud is grounds for setting aside a transaction at the option of the party prejudiced by it or for recovery of damages.

2.1.4.3 Crime against society

NIBRS (2015) also indicates that some crimes affect not just one person, but has effect on group of persons, a community, a village, or a town. Examples of such crimes include drug abuse, animal cruelty and pornography.

Pornography is the portrayal of sexual subject matter for the exlusive purpose of sexual arousal. (Park, Wilson, Berger, Christman, Reina, Bishop, & Doan, 2016). Pornography is usually depicted in many media including film, video and so on. The expansion of internet activities has contributed significantly to the increase in the access to pornographic materials by just a click of a button (Seltzer, 2011).

2.1.5 Overview of Cybercrime

Online crime has grown more prevalent with consumer confidence in online transactions declining steadily. In the olden days, hackers created viruses to be mischievous; modern-day malware authors create threats primarily to make profit. These scams are amazingly lucrative, with profits totalling in the millions per year. Many perpetrators hail from Eastern Europe where cybercrime is rampant and considered 'business as usual' (Mohsin, 2006).

According to the 2017 Internet Crime Report, published by the Internet Crime Complaint Centre (IC3), from January 1, 2017 through December 31, 2017, about 301,580 complaints were filed online with IC3. This figure represents a 9 percent increase compared to 2008 when 275, 284 complaints were received.

The Norton Cyber Security Insights Report (NCSIR) (2016) gives a very glaring picture of cybercrime across the globe. The NCSIR (2016) states that across the globe, cybercrime victims have spent $126 billion and lost 19.7 hours dealing with cybercrime activities. The number of devices connected to Wi-Fi has seen exponential growth in 2016 and there is constant need for connections (NCSIR, 2016).

The internet has evolved from being scientific to a platform that is enabling a new generation of businesses. E-business is a relatively new and fast paced approach to meeting consumer needs, introducing new products, and across geographic boundaries. E-business growth worldwide reached US$2.5 trillion in 2009 being that years' total value of e-business transactions worldwide (Mohsin, 2009).

While there are many positive aspects of this new e- business model, e-crime has become a serious concern for all e-businesses, with a significant impact on the bottom line. Cybercrime entails criminal activities or crimes in which computing devices or other forms of ICTs are the target (Pati, 2003). From the perspective of ICT for development, it is not misplaced to say that cyber is a double edge sword, with both the potential of speeding up the development of a nation as well as possibly stalling its development. The internet, by its very design, is an inherently vulnerable network which has enabled cybercrime to flourish in a new virtual environment.

Cybercrime has a potential to widen the digital divide, crumble the information infrastructure and affect consumer confidence in online transactions (Longe et al, 2009; Salifu, 2008; Oumarou, 2007). E-businesses face many challenges, especially in today's turbulent economy, and the effects of cybercrime make it even harder for the business to survive.

2.1.6 The Concept of Cybercrime

A primary problem for the analysis of cybercrime is the lack of a consistent and statutory definition for the activities that may constitute cybercrime (Yar, 2005). According to Smith et al. (2004), defining cybercrime raises conceptual complexities. Varied definitions of cybercrime do exist. In addition to the difficult of definition, it is also called by variety of terms such as computer crime, computer-related crime, digital crime, information technology crime (Maat, 2004), Internet crime (Wall, 2001), virtual crime (Lastowka and Hunter, 2004; Grabosky, 2001), e-crime (AIC, 2006) and net crime (Mann and Sutton,

1998). Gurjar et al., (2015) postulates that cybercrime could reasonably include a wide variety of criminal offenses and activities. Cybercrime is the latest and perhaps the most complicated problem in the cyber world. They continue that cybercrime may be said to be those species, of which, genus is the conventional crime, and where either the computer is an object or subject of the conduct constituting crime. It worth noting that any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cybercrime.

In the Council of Europe's (2001) Convention on Cybercrime, cybercrime is used as an umbrella term to refer to an array of criminal activities including offenses against computer data and systems, computer-related offenses, content offenses, and copy-right offenses (AIC, 2006). The Convention covers cybercrime in four main categories under substantive criminal law including:

1. Offenses against the confidentiality, integrity, and availability of computer data and systems such as illegal access, illegal interception, data or system interference, and illegal devices.

2. Computer related offenses like computer-related forgery and computer-related fraud

3. Content-related offenses (e.g. child pornography).

4. Offenses related to infringements of copyright and related rights.

Thomas and Loader (2000) cited in Wall (2015) define cybercrime as those who are computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks. The working definition for cybercrime by the Canadian Police College has increasingly been accepted by Canadian law enforcement agencies; as a criminal offence involving a computer as the object of the crime, or the tool used to commit a material component of the offence (Statistics Canada, 2002). Maat (2004) proposed a definition for cybercrime which encompasses all illegal activities where the computer, computer systems, information network or data is the target of the crime and those known illegal activities or crime that are actively committed through or with the aid of computer, computer systems, information network or data. It is significant to note that there is no consistent and statutory definition for cybercrime.

'Definitions' of cybercrime mostly depend upon the purpose of using the term. A limited number of acts against the confidentiality, integrity and availability of computer data or systems represent the core of cybercrime. Beyond this, however, computer-related acts for personal or financial gain or harm, including forms of identity-related crime and computer content-related acts (all of which fall within a wider meaning of the term 'cybercrime') do not lend themselves easily to efforts to arrive at legal definitions of the aggregate term. Certain definitions are required for the core of cybercrime acts. However, a 'definition' of cybercrime is not as relevant for other purposes, such as defining the scope of specialized investigative and international cooperation powers, which are better focused on electronic evidence for any crime, rather than a broad, artificial 'cybercrime' construct.

2.1.7 Forms of Cybercrimes

Cybercrimes are categorised by Yar (2005) as:

Cyber-Trespass; which involves crossing boundaries into other people's property and/or causing damage. An example of this is this type of cybercrime is hacking, defacement and viruses. Yar, (2006) explains that hacking is one of the most widely analyzed and debated forms of cyber-criminal activity, and serves as an intense focus for public concerns about the threat that such activity poses to society. He notes that hacking is an unauthorized access and subsequent use of other people's computer systems. He continues that early hackers had a love of technology and a compelling need to know how it all worked, and their goal was to push programs beyond what they were designed to do. Yar (2013) argues that the word hacker did not have the negative connotation as expressed by some authors today. It was revealed in the writings of Jewkes and Yar (2013) that the hacker attackers take place in several phases such as information gathering or reconnaissance, scanning and finally entering into the target system. The authors argue that the Information gathering involves obtaining information or to open security holes. They explain that the robber will find out the whole information about the place that wants to rob before making attempt. The computer attacker tries to find out information about the target.

Yar (2013) identified ***Cyber-Deceptions and Theft*** as one of the forms of cybercrime. This involves stealing such as stealing money and property, credit card fraud, intellectual property violation and piracy. He opines that the different types of acquisitive harm that can take place within cyberspace. He maintains that this level lie on more traditional patterns of theft, such as the fraudulent use of credit cards and cash, but there is also a

particular current concern regarding the increasing potential for the raiding of online bank accounts as e-banking become more popular.

Yar (2006) cited in Morelli, Bianchi, Baiocco, Pezzuti and Chirumbolo (2017 pp. 115) identifies ***cyber-pornography*** as one of the forms of cybercrimes. This represents activities that breach laws on obscenity and decency. According to Gurjar, Baggili, Breitinger, and Fischer (2015), cyber-pornographic include pornographic magazines produced using computers to publish and print the material and the Internet to download and transmit pornographic pictures, photos, and writings. The writers further indicated that Indian recent incidents revolving around cyber pornography in many schools include the Air Force Bal bharati School. The explain that a student of the Air Force Bal bharati School, Delhi, was teased by all his classmates for having a pockmarked face. They allude when the student was tired of the cruel jokes; he decided to get back at history mentors. He scanned photographs of his classmates and teachers, morphed them with nude photographs and put them up on a website that he uploaded on to a free web hosting service. This was only discovered after a parent of one of the class girls featured on the website objected and lodged a complaint with the police that any action was taken.

Yar (2012) identifies ***cyber violence*** as one of the forms of cybercrime which involves causing psychological harm to a person or inciting physical harm against others. Yar (2012) argues that the violent impact of the cyber activities of others upon individual, social or political grouping. He explains that these activities do not have a direct manifestation on the victims, they nevertheless feel the violence of the act and can bear long-term psychological scars as a consequence. According to him, these activities range from cyber-

stalking and hate-speech, to tech-talk. The writer explains to include cyber-harassment or bullying and adds that it is the use of electronic information and communication devices such as e-mail, instant messaging, text messages, blogs, mobile phones, pagers, instant messages and defamatory websites to bully or otherwise harass an individual or group through personal attacks or other means. Comparatively, Mishna, Cook, Gadalla, Daciuk and Solomon (2010) argues that cyber-bulling is more serious even than physical fight, because at least in a physical fight, there's a start and an end, but cyber-bullying, taunts, insults and harassment over the internet or text messages sent from mobile phones mostly have tragic consequences on the individual.

2.1.8. Aspects of Cybercrimes

a) Credit Card Fraud Schemes

Credit Card Fraud Scheme is a cybercrime which occurs when a person uses the credit card of another person to transact business fraudulently without any permission or authorisation from the owner of the credit card (Pittaro and Schmalleger, 2009). This represents the most challenging crime to business transactions in the 21st century where online transactions have become so common. Pittaro and Schmalleger (2009) further explain that credit card frauds occur usually through an act of deception, illegitimate use of people's account for personal advantage and misrepresentation of account information to purchase goods and services. The European Commission Press Release (2013) which published the Eurobarometer Survey conducted in 2013 in which over 27000 people in all European countries were covered indicated that 76% of the respondents agreed that the risk of becoming victims of credit card fraud has increased over the years. Many online markets

have emerged in Ghana over the past years such as Jumia, Alibaba, OLX and tonanton.com among others. The emergence of these online markets in Ghana presents risks similar to the findings of Pittaro and Schmalleger (2009).

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 occurs when a person takes the personal identifiable details (such as name, picture, passwords, social security, residential address and date of birth among others) of another person (Pittaro and Schmalleger (2009). Cybercriminals use different types of schemes in fraudulently getting the personal identity of their victims, technical and social engineering strategies. The social engineering scheme involves the use of telephone or computer (internet) by cybercriminals on their victims to get sensitive personal information of their victims. These criminals usually know some details of their preys either directly or through third parties which they use to deceive the victims to think they know them very well. Example for such incidence in Ghana is the mobile money fraud where criminals call victims and deceive them to take their passwords or to transfer money to them (Akomea-Frimpong & Dwomoh-Okudzeto, 2019). Technical engineering on the other hand involves the use of computer by ICT inclined criminals who can scam the internet and re-rout people's electronic mail accounts without their consent. Due to the prevalence of the social network sites and platforms such as facebook, instagram, whatsapp, and so on, identity theft has become common. People create fake accounts using the profile pictures of people to commit crimes.

c) Merchandise and Auctions Fraud

The International Cybercrime Centre (IC3) Annual Report (2013) states that 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 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

Cyber pornography and obscenity involve activities that are affront to 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 (Döring, 2009). 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 and Bossler, 2012). 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 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 have originated 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 and Cukier and Levin, 2009). 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 shrivelled. 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 the 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, Cukier and Levin, (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 and Bossler, 2012). Though hackers engage in and develop cyber security tools, individuals view hacking in its malicious context because of the economic and personal harm (Furnell, Emm, and Papadaki, 2015). In fact, malicious hacking is often tied to the creation and distribution of pirated softwares that can automate attack against computer system (Shakarian, Gunn and Shakarian, 2016). These programs can disrupt e-mail operations, and at times damaged private files in the computer.

h) 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 infection. This enables 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.

2.2. Causes of Cybercrime

In this section, an attempt was made to identify the causes and motivating factors that are responsible for the involvement of individuals in cybercrime. The motivating factors that encourage or drive individuals into cybercrime varies and it is determined based on a number of different factors such as money/ financial gain, recognition/fame, low rate of conviction, easy to perpetrate, intellectual pursuit, frustration, revenge, display of wealth by corrupt politicians and yahoo boys, laziness, un-satisfaction from what they earn, lack of good moral upbringing from parents and guardians (Das and Nayak, 2013).

2.3. Cyber Security in Perspective

Cyber security is concerned with making cyberspace safe from threats. The notion of "cyber-threat" is rather vague and implies the malicious use of information and communication technology (ICT) either as a target or as a tool by a wide range of malevolent actors. Cyber security is often confused with national security while national security, according to Udotai (2002) in Odumesi (2006 page 45) may often be implicated in some cases of cyber security. Cyber security as a term refers only to security of networks and systems- computers, electronics and auxiliary devices. Typical cyber security issues, according to Udotai (2002) in Odumesi (2006 page 45) include: confidentiality of information; and integrity of systems and survivability of networks. The major objectives

of cyber security include: protection of system/networks against unauthorised access and data alteration from within; and defence against intrusion from without.

As commonly used, the term "cyber security" refers to three things:

1. A set of activities and other measures, technical and non-technical, intended to protect computers, computer networks related hardware and software devices, and the information they contain and communicate, including software and data, as well as other elements of cyberspace, from all threats, including threats to national security;

2. The degree of protection resulting from the application of these activities and measures;

3. The associate field of professional endeavour, including research and analysis, aimed at implementing and those activities and improving their quality.

Cyber security is thus more than just information security or data security, but is closely related to those two fields, because information security lies at the heart of the matter. Information security refers to all aspects of protecting information. Most often, these aspects are classified in three categories: confidentiality, integrity, and availability of information. Confidentiality" refers to the protection of information from disclosure to unauthenticated parties, while "integrity" refers to the protection of information from unauthorised changes. "Availability" means the information should be available to authorised parties when requested. Sometimes, "accountability" the requirement that the actions of an entity be uniquely traceable to that entity is added to the list.

The first goal of a modern information security has, in effect, become to ensure that systems are predictably dependable in the face of all sorts of malice and particularly in the face of denial-of-service attacks. The dominance of network topologies has implications for the shape of the protection policies and, subsequently, in determining appropriate protection efforts, goals, strategies, and instruments for problem solution:

1. *Cyber security as an Information Technology issue*: Cyber security can be approached as an IT security or information assurance issue, with a strong focus on Internet security. Policies are thus aimed at countering threats to the information infrastructure by technical means such as firewalls, anti-virus software, or intrusion detection software. The main threats perceived range from accident, system failures, bad programming, and human failures to hacker attacks.

2. *Cyber security as an economic issue*: Cyber security is relevant to the business continuity, and especially to e- business, which requires permanent access to ICT infrastructures and permanently available business processes to ensure satisfactory business performance. The main actors are representatives of the private sector. The main threats are viruses and worms, human failures, but also hacker attacks of all sorts, and acts of cybercrime.

3. *Cyber security as a law enforcement issue*: Cyber security is seen as relevant to cybercrime. Cybercrime is a very broad term with various meanings, and definition can include everything from technology-enabled crimes to crimes committed against

individual computers. The main actors are law enforcers. The main threats are acts of computer criminality, but also cyber terrorism.

4. *Cyber security is a national security issue*: Society as a whole and its core values are endangered, due to their dependence on ICT. Action against the threat is aimed at several levels (the technical, legislative, organisational, or international levels). The main actors are security specialists. The main threats are terrorists, but also information warfare threats from other states (Taylor, Fritsch & Liederbach, 2014).

2.4. Activities on Cyber Security

Various activities have been taking place across the globe in an effort to address cyber issues especially crimes relating to cyber. Most of the countries in the developed nations have advanced initiatives in combating cybercrime, whilst the developing nations lag behind in terms of adequate regulations, institutionalisation and the fight against cybercrimes. The ensuing discussions present the global, regional (Africa) and the local (Ghana) activities on cyber security.

2.4.1 Global Activities on Cyber Security

Globally, statistics on cybercrime remain very limited largely due to the fact that victims seldom report to the appropriate authorities. Technology has integrated nations and the world has become a global village. The economy of most nations in the world is accessible through the aid of electronic via the internet. Since the electronic market is opened to everybody (which also includes eavesdroppers and criminals), false pretence finds a fertile ground in this situation (Duah and Kwabena, 2015).

The Ghana National Cyber Security Policy and Strategy (GNCSPS) states that cyber security is central to the Information and knowledge economy. Countries which have high levels of networked computers and automat ion stand greater risks than countries with the least developed networked computer infrastructure (MoC, 2014). As many countries with leased developed network infrastructure strive to become a knowledge society, many network infrastructures will be rolled out with automation. This is evidenced in many African countries where over the last few years, we have seen massive submarine fibre optic cable Internet transit land on the shores and the massive in-country fibre optic back bones being rollout. An increase in network computer infrastructure will bring a proportionate risk to critical information infrastructure. Since the year 2000, several countries with high levels of networked computers infrastructure been working around securing their critical information infrastructure and have developed cyber security policies and strategies to mitigate cyber incidences and crimes (MoC, 2014).

The United States of America for instance recently revised its policy and strategy to meet high incidences of cyber-attacks and increasing threats of cyber war. Every cyber citizen (people in cyberspace) has a right to lawfully access to information from around the globe irrespective of the location of the information. However, many criminally-minded cyber citizens tend to misuse the grant of access to information and commit cybercrimes. Since no one country can control cyber space and everyone can have access to information anywhere it is important for countries to put in place a very robust security around critical national infrastructure, setup very swift response systems as risk of attacks cannot be eliminated, and use an international approach of cooperation to secure cyber space and mitigate cybercrimes (MoC, 2014).

Many countries have formed Computer Emergency Response Teams (CERTs) empowered with the responsibility of taking reports of incidences of cybercrime and taking all necessary actions to mitigate its effects. However, CERTs are rarely formed in developing countries; in countries where they are setup, they lack the technical knowhow and capacity to function, although there is much talk about the subject in many developing countries as networked computers infrastructure expands (MoC, 2014). The International Telecommunication Union (ITU) through the International Multilateral Partnership against Cyber Threat (IMPACT) program has been playing a leadership role is providing early warning systems and training cyber security experts around the world (Choucri, Madnick and Ferwerda, 2014). Today, IMPACT has over 142 countries as members. The IMPACT program has been used to prosecute a global cyber security agenda. ITU has indeed developed frame work for developing countries to help them kick start a process of developing policies and strategy around cyber security. Forum of Incident Response and Security Teams (FIRS T) has also been a global platform of Computer Emergency Response teams in the world. Membership to FIRST is by recommendation and through testing of operational environment of country CERTs. The Budapest Convention on Cyber Security which has been in force since 2004 was elaborated by the Council of Europe with the participation of Canada, Japan, South Africa and the USA. The convention is open to any country which wants to participate. The convention is used as a guideline, reference standard or model law in more than 100 countries (MoC, 2014).

2.4.2. Regional Initiatives

Governments in Africa today have moved ICT discussion form infrastructure to cyber security. A decade ago, infrastructure was a major challenge to many African countries.

Many countries have invested in massive in-country infrastructure and the access challenge is waning. The networked computer infrastructure coming up in many African countries has open up cyber space to many more citizens and accompanying this, the risk of using the internet. A few countries like Tunisia, South Africa, Ghana, Nigeria and Kenya have CERTs, whilst many other countries are in the process of developing cyber security policy and strategy (Quarshie and Martin-Odoom, 2012). In an attempt to harmonising cyber security policy and strategy, the African Union, and the UN Economic Commission for Africa (UNECA) have developed a draft cyber security convention that has been reviewed and adopted by African Heads of State and Government in Malabo, Equatorial Guinea in June 2014. When harmonised with national policies, the document will create a platform for a regional co-operation in the fight against cybercrimes in the African sub-region.

2.4.3. Initiatives in Ghana

Today's society thrives virtually on using the Internet for communication and business. As networked computer infrastructure expands in the country, there is an increasing threat to business and communication. Recent several cyber-attacks on government websites in Ghana is a wake-up call for the development of a cyber-security policy and strategy (MoC, 2014). Resolutions of cyber incidences have been uncoordinated and, in many cases, there were no reporting structure put in place to guide us in dealing with future attacks. NITA's concern of ensuring security of the network has forced it to initiate discussion amongst stakeholder in the Ministries, Departments and Agencies (MDAs) to setup a NITA Computer Emergency Response team (nitaCERT) to coordinate cyber incidences and assist in resolving future incidences within the government network. The Ministry of Communication in collaboration with the Commonwealth Cyber-security Initiative (CCI)

have initiated an on-going process towards creating a national Computer Security Incident Response Team (CSIRT) in Ghana. The National Security Council as well as other institutions such as the Ghanaian Academic and Research Network (GARNET) are working on different projects, all geared towards securing Ghana's cyberspace (MoC, 2014).

The Ministry of Communication (MoC) has been championing the drive towards addressing the issues of cyber security in Ghana (MoC, 2014). The ministry has since its inception, initiated various measures to ensure crime free cyber environment in Ghana. Among other measures include the SIM card registration exercise, the issuance of Ghana Card, among others. The SIM registration exercise enforced by the Ministry of Communication on the various mobile telecommunication networks is yet another initiative in Ghana to combat cybercrimes relating to the use of mobile phones. Recently, the National Identification Authority (NIA) launched the Ghana Card which seeks to provide a single most efficient national biometric identification system for all those living in Ghana. This initiative which was launched in November, 2017 will contribute significantly towards the fight against crimes in general and cybercrimes in particular.

Other efforts aimed at ensuring cyber security by government agencies cannot be left out. The Ghana Police Service for instance has also put in place the Anti-Fraud Unit to alleviate cyber and other crimes. The Economic and Organised Crimes Office (EOCO) of the Attorney General's Department and the Financial Intelligence Centre for the finance, the government had directed all initiatives towards mitigating crimes in general and cybercrimes in particular (MoC, 2014).

2.5. 1. Cybercrime in Ghana: History, Paradigms, Profiles, and Responses

In 2010, Ghana, long viewed as Africa's flawless gem, had its sparkling reputation tarnished. In a report published that year, Ghana gained the unsavoury distinction – along with the West African neighbours Nigeria and Cameroon – as one of the top ten cybercrime generating states worldwide (Warner, 2011). In addition to its embarrassing addition to this list, a prior report also revealed that Ghana was the second most frequently blocked location by U.S. online retailers sceptical of fake orders from Internet scammers (Warner, 2011).

To better understand just how one of the continent's superlative states fell victim to the practice, this section offers a broad sketch of cybercrime in Ghana. Beginning with a brief history of cybercrime in Ghana, Warner (2011) notes that the Nigerian complicity in underwriting Ghanaian cyber-fraud are true or not, one commonality between the two countries that no doubt contributes to their statuses as the numbers one and two cyber-criminal states that: English, as many have noted, is the contemporary language of the Internet. Thus unlike citizens of Francophone or Lusophone African countries whose target audience for these crimes is much smaller, one sees that a far broader market of wealthy victims exists in the Anglophone world (from the United States, Canada, the U.K, but also from the billions of English bilinguals in the world (Anderson et al., 2013).

Warner (2011) found out that the common cybercrime in Ghana 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 (Ennin, 2015).

2.5.2. The Upsurge of Cybercrime 'Sakawa' In Ghana

The use of the Internet in Ghana has seen a significant increase since the liberalisation of the telecommunication industry in the 1990's. The country had 43 Internet users per 1,000 people in 2008 as compared to 1 Internet user in 1999 (ITU, 2009). The number of PC ownership doubled to 52 owners per 1,000 people between 1999 and 2005 (ITU, 2007). As at 2015 Ghana's mobile broadband penetration rate was estimated to be 62 percent (Duah and Kwabena, 2015). With these developments also comes negative effects and unintended consequences of ICT, particularly, cyber-crime.

"Sakawa" is a Hausa term that consists of the root 'saka-' [to put it in] and 'wa' (a simultaneously past and plural affix). Combined, these affixes literally mean 'to [have] put something in. 'Sakawa' is a coinage by youth fraudsters from deprived communities in Accra such as Nima, Mamobi and Lagos Town (Duah and Kwabena, 2015). The word indexes an 'azaa' (fraudulent) activity where cyber fraudsters' alleged involvement in ritual occultism is aimed to compel their victims to accede to their demands. These alleged rituals include taking an oath not to divulge 'sakawa' secrets and to fully abide by 'sakawa' rules;

inflicting wounds that never heals; sleeping in coffins for specified days at cemeteries (maximum being a week); carrying coffins in the dead of the night at road-intersections while being semi-naked; drinking human blood obtained either from murdering someone or from discarded female menstrual pads; eating contents from rubbish dumps for a required number of days; abstaining from bath before and after making a hit (in sakawa lingua culture, a 'hit' principally refers to a successful receipt of funds transferred through money transfer process like Western Union or Money Gram as well as other material items); spiritually sacrificing one's manhood (which manifests either as impotence or not being able to have children (Warner, 2011).

In terms of the strategies that these fraudsters allegedly use, therefore, a plethora of these two will be discussed for illustrative purposes. In this type, the perpetrator manages to contact the victims either through mass-mailing or through a lead. The victim is promised an incredibly profitable return on his investment (usually shady and dubious) (Duah and Kwabena, 2015). The popular baits include gold, diamond, lottery and some abandoned money that the client can help recover. Whatever, the bait, the true bait is the promise of instant wealth for the victim. These are well crafted plans with alibis that those who use fake documents sometimes originate from genuine sources such as the Office of the President, Attorney General's Department and respectable banks. At times, a duplicate website is designed which may look similar to a legitimate one or will redirect to a legitimate one when visited. Whatever be the case, the success of this is basically ignorance or greed on the part of the victim. In the worst-case scenario, the victim is lured to a location and physically attacked and robbed or even killed. It is believed that this type of cybercrime

was carried over with the influx of Nigerians into Ghana. The returns from this activity can range from 1,000 to 1,000,000 dollars (Warner, 2009).

After creating an online profile, a 'sakawa' person will send baiting emails which establish the basis for an initial friendship if the 'mugu' (client or the targeted person) responds. The fraudsters use this stage to profile and assess the generosity or seriousness of the client. Testing this characteristic involves requesting items like cologne, lingerie, explicit or near explicit pictures of the client. If this is accomplished, then the stage is set to demand bigger sums of money (Duah and Kwabena, 2015).

Duah and Kwabena (2015) further state that in the other type, the perpetrator is usually a young man posing as a woman (90%) or a young woman posing as a grown woman (7%). The remaining 3% are gay. Often, these perpetrators are poor and hungry with no real options for making ends meet or a real career path. Here, these fraudsters scout dating sites and examine profiles of males/females who are interested in relationships. They would then create profiles that match those of their potential 'mugu' (client). Here, they use photographs either taken from the web or that of a female accomplice. The victim is usually a bored rich old man or someone in the mid-forties. The perpetrators present themselves as a fabulously luscious young lady (using pictures from pornographic or fashion websites). The promise of overseas love is found so attractive and irresistible that the victim (who at times is a dissatisfied husband or wife or attention deprived) will do anything to get this kind of attention. The victim commits to love over the internet with the hope that they will meet their lovers eventually (Warner, 2011).

2.5.3. Cybercrime and Local Legislation

Cyber specific laws fall into three categories; enabling, prohibition and investigation. Enabling typically gives legal effect to electronic documents and storage. For example, digital signatures can legally work as real signatures only when legislation provides such judicial capability. Evidence for tax or other purposes can be effective when a specific law defines electronic exchange and storage to be sufficient as evidence (Ennin, 2015).

Prohibition typically barns and punishes computer related crimes. In Ghana, electronic data destruction cannot be criminalised under the general law because it does not destroy any physical matter. Similarly, intrusion itself does not constitute a crime as it does no physical harm. Thus, a specific law is required; Unauthorised Access Prohibition act is therefore required in Ghana to cater for this (Ennin, 2015).

For investigation purposes, Internet Service Providers (ISPs) are typically required to reserve communication logs for a certain period of time and submit such records to national investigative agencies. As communication service providers are prohibited from divulging communication secrets, specific legislation is required to give exemption. Eavesdropping and network monitoring for specific communication should also be allowed under a jury court's order judged in line with a law allowing special investigation. These types of laws are prepared to indirectly fight against threats (MoC, 2014).

In Boateng *et al* (2010), respondents (consisting of legal practitioners) were asked to indicate the type of law in the criminal code of the Republic of Ghana under which the

suspects or internet fraud are charged and whether or not it is appropriate to charge them under these laws. All the respondents indicated there is no law in the statute books that address these types of crime. Crime prosecution in Ghana is still reliant on primitive crime laws espoused in the Criminal Code 1960 (Act 29) and other statutes. However, in these provisions, cybercrime is subject to bail and punishments spelt out are not deterrent enough to regulate this dastardly criminal activity. The respondents also indicated that it is not wholly appropriate to use this law because the facts of some of the cases do not support the charges made against the suspects under that law hence most lawyers capitalise on such technicalities and have their clients acquitted.

Since 2008, the Parliament of Ghana and the Government of Ghana passed legislations and launched the Electronic Transaction Act, 2008 (ACT 772); the Electronic Communications Act, 2008 (Act 775), and the Data Protection Act, 2012, Act (843) to regulate electronic communication and transactions. Article 141 of the Electronic Transaction Act 2008 (ACT 772) mandates the security agencies to confiscate assets of cyber fraudsters.

In addition, the Economic and Organised Crime Office (EOCO) was set up by Act 804 of 2010 in line with Article 190 (1((d) of the 1992 constitution to supplement and augment government's effort in the fight against corruption and fraud in the State. The Office was established as a specialised agency of government to monitor, investigate and on the authority of the Attorney-General, prosecute any offence involving serious financial and economic loss to the state and to make provision for connected and incidental purposes. The mandate of the Office is clearly set out by the EOCO Act. The relevant provisions, at Sections 3(1) (a), (b), (c), (d) and (2) S. 12, and S. 13 indicate clearly that the mandate to

investigate any suspected fraud is inherent in the Office and can be activated by the Executive Director without reference to any other authority or agency of state.

Ghana has also passed a Mutual Legal Assistance Act, 2010 (Act 807) which among others requires persons to submit reports of suspicious transactions to the newly established Financial Intelligence Centre (FIC). Government has also set up an emergency Cybercrime Response Team (CRT), to review existing legislature governing the Information Communication and Technology (ICT) activities and strengthen the country's cyber security.

2.5.4. Legal Components for Cybercrime Prosecution

Despite the numerous laws and regulations in Ghana on crime, legal practitioners are of the strong conviction that cybercrimes cannot be prosecuted under the criminal codes due to the fact that not enough strict punishments are prescribed for this modern criminal activity (Boateng et al., 2010).

One major challenge with treatment and apprehension of cyber criminals is the issue of jurisdiction and the ability of existing legal frameworks to prosecute cybercriminals. In Ghana, the government passed the Electronic Transactions Act (Act 772) which addresses Cybercrime issues but as indicated in Boateng *et al* (2010) the police still rely on conventional crime laws on false pretence in the criminal Code Act 29/60 Section 131 and its associate statutes. Crimes committed under these laws are bailable offences and carry lesser punishments which cannot therefore deter the fraudsters from committing cyber

offences. Obviously these laws provide a vent for the criminal as the weight of judgment is not in any commensurate to the depth of cyber-criminal activities. It is therefore not wholly appropriate to use this law because the facts of some of the cases do not support the charges made against the suspects under that law. Most lawyers capitalise on such technicalities and have their clients acquitted (Boateng *et al*, 2011). The laws under which the suspects are charged are the existing laws on fraud established in 1960 which gives room for defence lawyers to often win when the prosecution presents poor evidence. Premised on these issues are the fact also that cyber criminality is not well understood. As the internet expands, opportunities for unethical use will continue to increase if nothing is done in terms of understanding the modus operandi of the cyber-criminal and the methods of victimization. This is reflected in the routine activity theory which posited that crime can be motivated by opportunities provided in routine activities. Incidentally, the use of the web falls perfectly into the domain of routine activities howbeit on a global scale (Cohen and Felson, 1979).

2.6. Awareness of Cybercrimes among Students

It is evident that countries all over the world have realised the importance of cyber education. Currently, there is a lot of cyber education related material available online. These are all initiatives of the countries in response to the recent rise in cyber-attacks. It has been widely recognised as a vital requirement by most countries and has led to a large number of initiatives in making cyber safety material available online (Saluja, Bansal, and Saluja, 2012). Essentially, they all work on a voluntary basis and so are not very viable to ensure measurable mass adoption.

Cyber education needs to be institutionalised across the various segments of users. The best way for this is to do it through schools especially, the Senior High School level where the students are been introduced to the internet use through varied sources. Since everyone goes to school, this much needed education can reach a larger number of kids ensuring a wider coverage. Children are starting to use technology at a younger age and hence expose themselves to the online dangers earlier too. Schools and houses are increasingly becoming more IT enabled so it is important that the children remain safe (Saluja et al., 2012).

New generation is growing up with computers and most important is that all the monetary transactions are moving on to the internet. So, it has become very important for us to be aware of the various cybercrimes being committed with the help of computers. People's perception and attitude towards computer ethics and information security significantly affect the way they use information technology (Saluja et al., 2012). This phenomenon is evident among SHS students and extends to disturbing levels among the tertiary students who are generally regarded as major violators of computer ethics and computer security (Saluja et al., 2012).

Statistics from a recent study on internet studies conducted in 2011 showed the rapid adoption of the internet by the youth and some of the dangers caused by it. Out of the surveyed youth in urban Indian schools, 84% had an internet connection at their homes. Internet use at home was highest among students between 13 and 14 years of age, with some spending as much as 8 hours online daily (Saluja, Bansal, and Saluja, 2012). Another survey by Associated Chambers of Commerce and Industry of India (ASSOCHAM) survey in 2010 as cited in Salaju, Bansal and Salaju (2013), revealed that about 52% of children

in the 8-11 age group daily spent over five hours online - chatting and playing games. In the same age group, 30% spent between 1-5 hours a day on the net while 18% said they didn't surf daily. The usage was higher among 12-15-year olds, 58% of whom fell into the "excessive use" category. Only 10% of these children didn't surf daily and 32% spent up to five hours a day on Internet (Saluja, Bansal, and Saluja, 2012).

Colfer (2007; Li, 2006) state that there are dissimilar perceptions and awareness between men and women. According to Titi (2003) women are more aware of cyber regulations and have superior ethical values compared to men. Women are less likely to become victims as compared to men. Lifestyle Theory states that sex is an often-mentioned demographic characteristic that is associated with difference in lifestyle (Ngo and Paternoster, 2011; Reyns, 2010; Choi, 2008; Wolak et al., 2006). Neiss et al. (2009) state that perception and awareness of young people are dissimilar between age groups. It is because young people and older people have different perspectives. Young people give more negative emotional perception than older adults. Lifestyle Theory suggests that individual of different ages participate in different kinds of lifestyle. These lifestyle differences, therefore, expose individuals of different ages to varying levels of risk of victimisation (Hasan et al., 2015; Reyns, 2010; Choi, 2008; Wolak et al., 2006). It has been persistently reported that younger people are more likely to be victimised than older people.

A report on cybercrimes by the Australian Youth Affairs Coalition submitted the office of Privacy Commissioner in which they state that the students in the age group of 18-24 are in high risk environments when exposed to online activities (Hasan et al., 2015). Knowledge is very important for young people to prevent cybercrime (Curtis and Colwell,

2000; Wang et al., 2008). Chawki (2005) states that educating young people would help decrease the risk of students in cyberspace. Asokhia (2010) finds that the level of education contributes significant differences to the students' perceptions of cybercrime. Knowledge helps people to be more aware on cybercrime (Levin et al., 2008). The number of cybercrime victims could be reduced by introducing proper awareness activities such as training programs, sufficient resource for compliance, develop policies and regulations and sufficient protection of personal information (Bougaardt and Kyobe, 2011; Choi, 2008; Levin et al., 2008; Chawki, 2005). Choi (2008) emphasises on the effectiveness of university programs in promoting knowledge and values about cybercrime as these programs could improve future behaviour of students towards cybercrime in terms of safety and security. This would establish norms and adjust prospects for illegal or delinquent behaviours. Based on the review of above literatures it is anticipated that gender, age and knowledge have significant influences on cybercrime.

2.7. Effects of Cybercrime

Lunda Wright (as cited in Saini et al. 2012 page 204), a legal researcher specialising in digital forensic law at Rhodes University, has an interesting research finding on a blog posted in October 2005. It states that there has been an increased rate of prosecutions of cyber-criminals. There has been an increased clamping down on cyber-piracy related to the film and music works. There are novel lawsuits and strategies for litigation. There is a greater dependence on the skills of computer forensic experts in corporations and government. Finally, there is an increase in inter-government cooperative efforts (Aseef et al., 2005). There are trends indicating organised crime involvement in white-collar

crime. As criminals move away from traditional methods, internet based crime is becoming more prevalent. Internet-based stock fraud has earned criminals millions per year leading to loss to investors, making it a lucrative area for such crime. Police departments across the nation validate that they have received an increasing number of such crimes reported in recent years. This is in sync with the national trend resulting from increased computer use, online business, and geeky sophisticated criminals. In the year 2004, cyber-crime generated a higher payback than drug trafficking, and it is set to grow further as the use of technology expands in developing countries. Scott Borg, director of the U.S. Cyber Consequences Unit, an agency supported by the U.S. Department of Homeland Security, recently indicated that denial-of-service attacks won‘t be the new wave of future. The worms, viruses are considered not quite mature as compared to the potential of attacks in future.

2.7.1. The Necessity of Cyber Education in High Schools

Over the last few years, cybercrime has seen a meteoric rise. The recently released report by RSA brings out that every minute, 232 computers are infected by malware. The lightning speed at which cybercriminals develop attacks and new malware code is making it harder for global organisations to manage cyber security risk. Saluja, Bansal, and Saluja (2012) revealed that criminal attacks using social networking sites increased by 500% between 2008 and 2009. As we see development of new technology, there is an increase in the threats and vulnerabilities. Now the development cannot be stopped but our preparation to cope with these threats can improve. These threats pose serious risks to children since most of them are ill-informed regarding this issue. By educating kids, we are ensuring that

the future generations will be safer online. There is a thin line between using the internet and abusing it and some people unknowingly cross that line. The Internet is there for use for both adults and kids so it must be seen that no matter who uses it, it shouldn't bring anyone any harm. The internet is misused by some people that indulgence in activities such as cyber bullying and the creation of fake IDs (Saluja et al., 2012). Moreover, children are unaware about all of these risks and hence don't realize when they might be committing a crime by, most often, infringing the copyright law. Although illegal, this isn't considered a crime by the teenagers today. It was also revealed that children were often harassed online but did not know what to do. These children put up their personal information and pictures in public forms without realizing that they are putting themselves in danger (Saluja et al., 2012).

2.8.1. Theoretical and Conceptual Perspectives of Crime

Many Social researchers specifically, criminologist have made frantic efforts over the years to model and predict reasons for crime in societies. Felson and Clarke (1998) established the 10 principles of opportunity, which can be considered as a criminal behaviour. Technically, opportunities are vital in understanding crime. These opportunities are highly specific and focused in time, space and dependent on everyday movement.

Four theories have often been used by criminologists and sociologists to model the behaviour of criminals, namely, Crime Pattern Theory, Routine Activity Approach, Rational Choice Perspective and Differential Association Theory. The Crime Pattern Theory (CPT) theory propounded by (Brantingham and Brantingham, 1993) asserts that,

crime is not randomly committed but has a specified pattern. The theory explains that human life is not random and thus crimes are committed along the human routine life pattern. Human being move from home to work, or home to places of leisure. Perpetrators of crime fully understand this pattern and attack their victims at times and places where they can commit their heinous activities successfully. Rossomo stated that this is "similar to the concept of a comfort zone" (Rossomo, Laverty, and Moore, 2005. P.106). Technically, an individual's awareness space is not driven from the individual activity space. An activity space is a measure of individual spatial behaviours which captures individual and environmental differences and offers an alternative approach to studying the spatial reaction of travellers.

The Rational Choice Theory emanate from the classical school of thought that believes that criminals are guided by hedonism. This means offenders try to maximise their pleasure and reduce pain. Thus; weighing the benefits of their actions against its consequences. In other words, risk plays a critical role in a criminal decision to commit a certain crime at a particular place at a given time. Cornish and Clarke (2003) in their work assert offenders weigh the effort require and the associated benefit compared with likelihood of being apprehended and the severity of the punishment.

According to the Routine Activities Theory, it is not only offenders who play a critical role in crime, but also victims play a vital role. The theory emphasises that the everyday routine activities of humans is as well essential in studying crime. Thus, people who have very busy movement schedules are more likely to be victims than those with less movement schedules. The routine activities theory postulates that crime operates easily in the presence

of three criteria. These criteria as propounded by Cohen and Felson (1979) are: suitable target, motivated offender, absence of capable guardian. It again stresses that rather than planning to strike a victim over a time, offender's usual strike at a given opportunity. This opportunity is assessed on the set criteria above. For instance, in a working-class neighbourhood, where both parents of homes within the vicinity leave home for work, offenders find burglary within such vicinity easy.

2.8.2. Differential Association Theory

The Differential Association Theory (DAT) was first propounded by Sutherland (1924). The most widely used theory in criminology. According to the author, the rational rallying behind this theory suggests that criminal behaviours are learned by interacting with friends, family and close associates who have criminal behaviours or deviant tendencies, thereby resulting to acceptance and practice of such criminal activities. Sutherland, Williams, McShane (2015) underscore why normal law-abiding citizens end up as criminals through peer influence. The authors view social environment as a tool that interacts to model the behaviour of individuals. This is common in poor socio-economic settings which encourage to facilitate the defiance of law and order. The basis of this theory is that criminal behaviours are usually acquired through interactions between criminals and non-criminals (Sutherland, 1924). It worth to mention that some these interactions are created through social networking sites such as Facebook, WhatsApp, Twitter etc. These social networks usually have norms and values for which its operators must abide in order for them to stay connected. The established norms by the social network groups on the social networking may deviate from the socially accepted norms of the society. The unpalatable values and

norms of the groups on the social networks could coerce its participants not to abide by norms of the larger society.

Sutherland (1939) cited in Akers and Jennings (2015) suggests that the process of learning includes two vital elements, thus the requisite skills and techniques for committing crime. The writer maintains that people commit crime on the basis of specialized skills of computer fraud, trading and readily available skills to them. Cloward and Ohlin, (2013) believes that crime is feasible if the following conditions prevail: (1) if the person has the requisite skills to commit a crime; (2) if the person has a definition of his actions favourable to justify his actions; (3) if the person has the opportunity to commit that crime.

In addition, the theory looks at crime transmission among peer groups is used for this study because cybercrime is largely committed via peer group influence with the youth in our Senior High Schools being the most vulnerable.

The theory of Differential Association can be applied to Cybercrimes. The main premise behind this theory is that criminal behaviour is learned through social interactions with others. The profile of cyber criminals is one who is very smart, highly knowledgeable and who are computer savvy. Their social interactions may come through electronic communications with other individuals who share similar technological interests. If they do not currently have any desire to commit malicious acts through electronic means, such as an act in violation of the computer fraud and abuse act, then they may become influenced through another individual with whom they share electronic communications. This theory which was developed to help explain white collar crime fits in well with those who violate

or commit Cybercrime. Imhof (2010) contends that a lot of systems hacking occur in schools and colleges. Many of these individuals spend time with people who share similar interests. Differential association is a theory with a number of postulations which help to explain the causes behind why Cybercrimes are increasing so quickly in the society and how an individual learns to become a cybercriminal. There are a wide spectrum of the different kind of offenders and motivations.

In sociological analysis, theories are indispensable. They form an integral part of sociological research as it is a general principle that explains or predict facts, observation or events. The theory of differential association was adopted for this study. This theory was propounded by Edwin Sutherland an American Sociologist. Differential association theory proposed that through interaction with others, individuals learn the values, attitudes, techniques and motives for criminal behaviour. According to this theory, the environment plays a major role in deciding which norms people learn to violate (Sutherland, 1939).

The principle of differential association asserts that a person becomes delinquents because of an "excess" of definitions favourable to violation of law over definitions unfavourable to violation of law. What this means is that an individual will become a criminal because they are exposed to more favourable criminal behaviour. That is when one is exposed to more criminal influences rather than more favourable legal influences. In other word, criminal behaviour emerges when one is exposed to more social message favouring misconduct than pro – social messages. This can be seen in environments with poor socio-economic conditions which may encourage negative views towards the law and authority.

2.8.3. Space Transition Theory of Cyber Crime

The study employed space transition theory of cybercrime. This theory was initiated by Jaishankar (2008). The theory explains the causation of crimes in cyberspace. The theory brings to bear individuals who exhibit unacceptable behaviour by the use of physical space and cyberspace. According to Jaishankar (2011), cyberspace in most cases influence individuals, particularly the youth to become social non-conformist as indicated by Durkheirm (2015). Jaishankar (2011) argues that the movement of individuals from one place to another space either positive or negative impact on their activities. The theory suggests the following as the causal factors that coerce individuals to commit cybercrime.

First and foremost, the theory suggests that individual with repressed behaviour commit cybercrime, because of their social situations or statuses. Jaishankar (2011) alludes that such individual would not have committed cybercrime if they are not suppressed in the society. To him, the repressed situation causes persons to move in search for solutions to their problems and this influence them to use cyberspace to exploit or dupe other people for survival. He argues that individuals are more concern about their social status and this makes them feel various degree of self-reproach in the society. The author emphasizes that the degree of inferiority one feels in the society causes them to embark on cybercrime activities. The theory suggests that individuals weigh the magnitude of social and material risks of being criminal as against the comfort of being law-abiding citizens in the society before deciding on committing cybercrime. He posits that if the profit that would be earned from the cyber activity outweighs punishments, they prefer committing cybercrime than being social conformist as indicated by Durkheirm (2015). He further argues that people

who are more sensitive are not willing to endorse cybercriminal styles. Comparatively, those who are insensitive to guilt commit cybercrime without guilt in societies.

According to Jaishankar (2011), one of the factors that influence individuals to commit cybercrime is when the person disassociates him or herself from the societal norms. He continues that crimes defenders like the security services who are expected to mete out appropriate punishment to the perpetrators to serve as deterrent to others give little or no punishment and ginger the perpetrators to commit more cybercrimes. The writer maintains that millions of people are into cybercrime where the computer is used to perform forensic analysis to crime. Recently, the computer is used to commit sophisticated financial fraud, malware, theft among others (Stephen & Gilbert, 2013). The writers were of the view that, some youth in recent times view cybercrime as an instrument of getting what they want from the rich in the society. Jaishankar (2011) indicates that cyber is an imported crime which is more prevalence among young people. He argues that perpetrators of cybercrime are always seen in groups with a unifying goal or agenda. The author asserts that persons with more close societies are more likely to commit cybercrime than those from the open societies. The theory suggests disjuncture between social norms and the value of physical space and the value surrounding the cyberspace breeds cybercrime in societies. The writer sees the emergence of cyberspace in society as a new locus of criminality.

Again, the author argues that one of the main factors that causes individual to engage in cybercrime is anonymity. To him, anonymity is the single most important factor that causes de-individualization. De-individualization is one of the main reasons for deviant behaviour of people in cyberspace. He explains that de-individualization is a psychological state in

which one loses his sense of individuality and personal responsibility. This disorder in society influence people to behave less altruistically. The people especially the youngsters become more selfish and more aggressive in getting what want.

2.8.4 General Strain Theory

The general strain theory was created by Robert Agnew (2010). Strain theory by Robert Merton informed Agnew to create the general strain theory. The theorist argues that group of strains; thus, conditions and events of people influenced individual to commit crime, or leads individual to deviance. The theory suggests three major types of strains. These strains include:

- the presence of aversive or negative stimuli, example of these are sexual or physical abuse
- the incapacity to obtain positively-cherished aims which takes into account the wealth, and prestige of the person and
- the absence of positively-cherished stimuli. This considers the loss of wealth and loved parents.

It is important pointing out that the three general kinds of strains cover a number of minor strains. The outlined strains by the theory lead individuals to bad feelings and the individuals may deal with them by deviance. The writings of Agnew (2014) indicates that the strains can lead a group of people to have bad feelings towards a particular goal. He argues that an individual who is exposed to the outlined strains can be coerced to take an action against them to overcome the bad feelings and this can resort to deviancy. The writer

expressed the view that negative emotions can diminish worry for the criminal costs and reduces the ability to deal with problems in legitimate way. This, according to the writer incites the perpetrators to commit crime and helped to develop justification for the deviance and the motives that rally behind the illegitimate action. It is argued that these psychological feelings which lead to deviance are mostly fueled by anger. He indicated the strains are mostly escalated by anger and some cases emotions like frustration, jealousy, fear, hopelessness, shame, and malicious envy play mediating roles which are more likely to play mediating roles.

He said the individual respond to deviance or not depends on how on the outcome of three cardinal strains namely; (1) tendency for deviance, (2) criminal costs, and (3) the capability of involvement in legitimate and illegitimate coping. The writer was of the view that factors such as weak traditional coping abilities and resources self-efficacy, deviant skills and sources, weak conventional social supports, weak social control, definitions in favor of crime and criminal peers, and exposure to conditions in which the criminal costs are none or small and the gains are great lead an increase in criminal coping. In addition, it is argued that there is a positive correlation between the strains the individual is exposed to and crime. Lanier (2018) and Zweig, Yahner, Visher and Lattimore (2015) tested the theory and examined this and observed that an increase in strain leads to a great increase deviancy.

2.9 Conclusion

It is emphatic that noting that cybercrime has deleterious effect on students' education, since, a number of youths pursue quick money instead of pursuing knowledge which would

gradually lead them to riches. In recent times, cybercrimes had marred the security of many countries in the world where the youth had devised dubious ways in duping innocent individuals. The activities of cybercrime among students (youth) had impelled many to become school drop-outs and they have abandoned the laid down societal norms by resorting to illegitimate means of achieving the societal goals as posited by Agnew's general strain theory. This comes a result of environmental anonymity which at times causes de-individualization in societies.

CHAPTER THREE

METHODOLOGY

3.0. Introduction

This chapter provides information on the study area, research design, study population and sampling procedures used for the study. Information about the sample size, instrumentation and data collection as well as the data analyses procedures are addressed.

3.1. Study Area

Tamale Metropolis

The Tamale Metropolis is one of the six metropolises in the country. It lies between latitude 9.16° and 9.34° North and longitudes 00.36°and 00.57. The metropolis has a total estimated land size of 646.901 sq. km Ghana Statistical Service (GSS, 2013). The metropolis is located at the heart of the Northern Region of Ghana (as shown in the map below) and shares boundaries with six other districts namely the Savelugu- Nanton to the North, Mion to the East, Tolon and Kumbungu districts to the West, Central Gonja to the South West and East Ganja to the South. The total population of the Tamale Metropolis is 223,252 representing 9.0 percent of the total population of the northern Region (GSS 2013). This is made up of 111,109 males and 112,143 females constituting 49.8 percent and 50.2 percent respectively (GSS, 2013). The Metropolis has a predominantly urban population (80.8%). About 63.3 percent of the population aged 15 years and older in the metropolis are

economically active. For those who are economically inactive, a larger percentage of them are students (56.0%). Figure 3.1 below shows the map of Tamale Metropolis

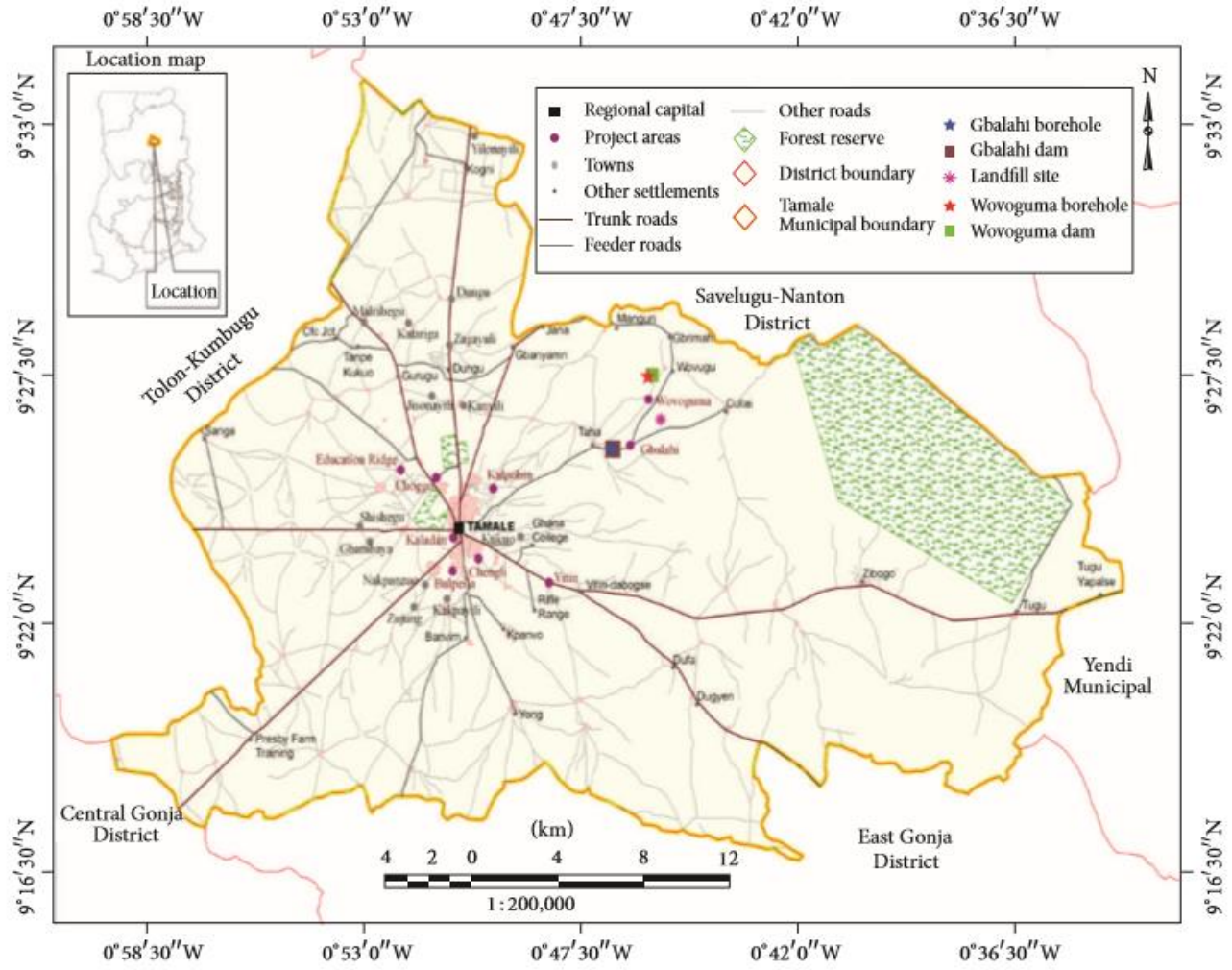

Figure 3.1 Map of the Tamale Metropolis

Source: Ghana Statistical Service (2014)

3.1.2 Social and Cultural Structure

The Northern Region of the country has vast land cover with smaller population sizes and the Metropolis is of no exception. This area begun experiencing high population growth after many people with different ethnic backgrounds started migrating from other areas to settle there; thus, making it a cosmopolitan area. The Dagombas are the majority and other ethnic groups such as Gonjas, Mamprusis, Akan, Dagaaba and other groups from the Upper East Region are also residing in the Metropolis. Also found in the Metropolis are other nationals from Africa such as Nigeria, Togo, Burkina Faso and other countries across the globe. The area has deep rooted cultural practices reflected in activities such as annual festivals, naming and marriage ceremonies. Some of the festivals that are celebrated annually in the Metropolis are Damba, Bugum (fire festival) and the two Muslim Eid festivals (Eid-Fitr and Eid-Adha). The Metropolis is dominated by Muslims and followed by Christians, spiritualists and traditionalists (Ghana Statistical Srvice, 2014).

3.1.1 Markets and Financial Institutions

There are four major markets in the Metropolis namely: Central Market, Aboabo, Kukuo and Lamashegu Markets. In addition to these, there are satellite markets in other communities. The Central market comprises of mini shops and stalls. Plans are underway, to upgrade the market with modern facilities. The Central Business District (CBD) is also fast developing with new business ventures. The uncompleted modern super market block that was started during the 1970s but was abandoned due to lack of financial resources and perhaps political instability is now under construction. This facility when completed would provide space for offices, stores and shopping for businesses. When completed it would

offer permanent accommodation for a lot of traders roaming the streets and those occupying open spaces in the CBD of the metropolis.

There are sanitation facilities ranging from one 24-seater water closet (WC), one 10-seater KVIP and aqua privy in some of the markets but these are inadequate. The Lamashegu and Kukuo markets are yet to be provided with sanitation facilities. These facilities are however inadequate for the rapidly growing population of the Metropolis.

The Assembly has an abattoir located at Shishiegu in the Tamale South-Sub Metro. This abattoir has the capacity of generating waste for bio-gas production. Aside this facility is the landfill site that receives 250 tons of waste daily (GSS, 2014). The procurement of a digester and establishment of a recycling plant could be a good investment opportunity worth exploring since it could bring economic gains to the Metropolis and other neighboring districts. The landfill site is a huge potential for the generation of not only bio-gas but also for generation of fertilizer which could be very useful to farmers. The landfill as at now is poorly developed, and could in the near future have serious consequences on the health of the people.

There are many international, national and local financial institutions in the metropolis. Prominent among these are the Bank of Ghana (the national Regulator), Barclays Bank, Standard Charted Bank, Stanbic Bank, Ghana Commercial Bank, Agricultural Development Bank, Zenith Bank, National Investment Bank, and Unibank amongst others (GSS, 2014).

3.1.2 Utilities and Services

Utility services are available in the metropolis. Electricity, water, roads, markets and communication services are available in urban communities in the Metropolis. However; more need to be done in the rural communities. The roads in the Metropolis are fairly good especially those that link the Metropolis to other adjoining district capitals. The tarred roads in the area facilitate easy commuting from one place to the other. There is no traffic congestion. Most of the farming and the peri-urban communities are linked to the marketing centers by feeder roads. The availability of access roads linking farming communities to marketing centres enables farmers to transport their produce to the urban marketing centres with ease. Consequently, their postharvest losses are likely to be less or reduced.

The Metropolis enjoys frequent water supply from the Dalun and the Nawuni Water Treatment Plants. The main source of water in the Metropolis is pipe borne water which is rationed and managed by the Ghana Water Company Limited in urban Tamale. The Ghana Water Company Limited supplies 45,000 cubic meters daily. Reports from the company indicate that there is a surplus in treated water supply in the Metropolis. This implies water bottling companies could take this opportunity to establish bottling plants to utilize this resource in the area. This would also create employment opportunities in the area for the youth. Other water sources include; Town water systems, mechanized bore holes, wells, dams and dugouts.

The Metropolis enjoys electricity supply from the National Grid and about 70 percent of the communities are connected. Electricity supply has been fairly stable. With the

expansion of electricity in the Metropolis, there is also an expansion of Small and Medium-Scale Enterprises in the area.

3.1.3 Transport

The major transport services in the area are taxi cabs with a main taxi station at the Central Business District (CBD). State Transport Company, Metro Mass Transit, O. A. Travel and Tours and other private bus services link the Metropolis with other cities and towns in the country. Most of the people also use motorbikes as their means of transport within the Metropolis. For easy transport of goods and services, EMS, FEDEX, DHL and others offer fast and reliable express services from the Metropolis to other places (GSS, 2014).

3.1.4 Communication

The Tamale Metropolis also enjoys telecommunication services. New mobile communication service providers such as Airtel, Expresso and Glo are now operating alongside the major networks (MTN and Vodafone). Broad band service has been introduced in the Metropolis, which is encouraging as it links the Assembly to the worldwide web. It has also proved very useful in business transactions for both public and the private sector. The Metropolis has lately witnessed an increase in media activities. For instance, FM radio stations have increased from 3 to 8; TV stations from 1 to 5 with a considerable jump in newspaper supply vendors. The Media houses are avenues for organizing educative programmes especially on government policies to the illiterate population in the local languages. The major problem with the newspapers is that, they arrive from Accra and Kumasi in the Metropolis very late in the day. With technological

advancement there would be the need for a newspaper printing press to be located in the Metropolis to serve the three Northern regions of the country (GSS, 2014).

3.1.5 Sports

There is an Ultra-Modern Sports Stadium in the Metropolis which is being managed by the Ghana Sports Council. The Sports Stadium has contributed in boosting sporting activities in the Metropolis. Real Tamale United is the biggest football club in the Metropolis with other smaller clubs. There are other facilities such as conference rooms, restaurants and shops within the sports stadium for public use. The inner perimeter of the stadium could also be used for entertainment related activities such as musical displays and other major events.

3.1.6 Tourism and Hospitality

The Metropolis is a transit point to many tourist sites in other districts and regions in the northern part of the Country. For instance, many tourists moving to the Mole National Park do make a stopover in Tamale before embarking on their trip to the West Gonja District. There are also a few tourist sites in the Metropolis namely: Tugu Crocodile Pond, the Python Sanctuary, the German Cemetery as well as a Cultural Centre. The Centre for National Culture is located right in the Central Business District of Tamale; a place many tourists would cherish visiting to have a look at many items of local Arts and Craft exhibitions.

There is also a vibrant hospitality industry. More hotels, guest houses, restaurants are springing up. Some of the prominent ones are Mariam Hotel, Picorna, Gariba Lodge,

Modern City Hotel, Radach Memorial Centre and Hamdallah Guest house among many others.

3.1.7 Education

The Ghana Statistical Service (2014) reported that 60.1% of the population gamut from 11 years and above are literates and 39.9% are non-literates. The report further indicate that the proportion of literate males are 69.2% higher than that of females who are 51.1%. Five out of ten people representing 54.8% can speak and write both English and Ghanaian languages. The population amongst the aged 3 years and older (84,897) currently attending school in the metropolis, 52.9% are males and the remaining 45.1% are females. Among those who have attended school in the past, males constitute 58.6% and the females represent 41.4%. This shows that both among those who attended school in the past and those who are currently, males have higher proportions. Among those currently attending school, 15.1% are in nursery, 18.2% in JSS/JHS, 12.5% in SSS/SHS and the largest proportion (40.0%) is in primary. Only 5.7% of the population 3 years and older in the metropolis are currently attending tertiary institutions.

3.2 Research Philosophy

The study employed pragmatist philosophy to underpin the study. According to Creswell (2014), pragmatist philosophies do not see the world as an absolute unity. He argues that pragmatic is not based on a strict dualism between the mind and reality as suggested by the positivists that reality is out there and it is structured by norms and values of society or the constructivist view which seek to understand reality. He stresses that pragmatics on the

other hand view reality and mind as independent and hence eliciting information from individuals require separate methods to give individuals freedom of choice. Based on this assumption by Creswell, the study though cross-sectional design, triangulated both quantitative and qualitative data, because they work to provide the best understanding of the phenomena understudy. This helped the researcher to ask question like "what is the level of awareness of SHS students with regards to cybercrime? This provided deeper meaning to the various concepts and questions as indicated by Creswell (2014).

3.2. Research Design

Cross sectional design was used to solicit information from the respondents, this helped the research to triangulate both quantitative and qualitative data as asserted by De Vaus and De Vaus (2013). The triangulations of methods in this design helped the researcher to develop interview guide and questionnaire to seek an in-depth information about the topic under study (Crano, Brewer and Lac, 2014; Paluck and Cialdini, 2014). Studying and understanding any social phenomena is a complex process as it requires the researcher to think through all the process of the research problem and then try to situate it in a proper and relevant perspective. This guided the data collection and analyses process which provides the bases as to how research questions were answered to in connection with the study objectives. This was done in a single point in time with which the researcher did not go back to the schools again, after the data had been collected. This was appropriate to determine the effects of cybercrime on secondary education in the Tamale Metropolis of the Northern Region of Ghana.

3.3. Target Population

The study targets SHS students in the Tamale Metropolis. Café managers or operators, opinion leaders, the police and teachers, especially ICT teachers in the metropolis were also part of the study. Also, sakawa guys who were willing to participate on condition of anonymity and confidentiality were also part of the study.

3.4. Sampling Techniques and Sample size

It is important noting that the sample size determination table by (Krejcie and Morgan, 1970 as cited in Alhassan, Odame and Ameyaw, 2017) was used to determine sample size of 120 respondents out of the total population of 887. The table has already calculated almost all the sampled population suitable for this study. In lieu of this, there is no need for the researcher to calculate for any the sample size again since everything is calculated and tabulated.

Both probability and non-probability sampling techniques were employed. With the probability sampling, the multistage sampling procedure which involves taking of samples in stages using smaller and smaller sampling units at each stage was used. Multistage sampling involves dividing the population into groups or clusters and then one or more group(s) or cluster(s) are chosen at random and everyone within the chosen cluster is sampled. This technique is frequently used when a complete list of all members of the population does not exist or is inappropriate. Although cluster sampling and stratified sampling bear some great similarities with multistage sampling, they are substantially

different. In stratified sampling, a random sample is drawn from all the strata, where as in cluster sampling only the selected clusters are studied, either in single or multi stage. The simple random sampling technique where respondents have equal chance of being selected was used.

Conversely, with the non-probability sampling technique, purposive and snowball sampling techniques were employed. The purposive sampling technique was used to select the internet café managers and school masters and the police officers whereas the snowball sampling technique was used for the purpose of identifying students who were sakawa guys for interviews.

The study used the survey design and employed multistage sampling procedure to select 120 SHS students in the Tamale metropolis of Northern Ghana (40 of them were students involved in sakawa activities). The Tamale Metropolis was stratified into four zones (North, South, East and West) with a total number of 120 students from which four schools (Tamale Girls SHS, Vittin SHTS, Business SHS, and Presbyterian SHS) were selected from each stratum using the simple random sampling by the lottery method.

The lottery method is the most widely used random sampling procedure and the simplest. It involves writing all possible samples on a like-shaped pieces of papers. Which is then folded in similar manner and the sample size is picked from the folded pieces of papers mixed up in a container. In this case, the papers folded were 887 (representing the sample frame) and after folding the papers, the 80 (20 from each school) randomly selected students were picked.

A total number of 30 respondents were selected from the four schools and questionnaires were then administered at each school across all the three forms (F1 to F3). At least two questionnaires were administered at each class in the selected schools.

In addition, purposive and snowball sampling techniques were employed to select key informants for interviews on the subject. These methods ensured in-depth responses on the subject matter and enable all objectives set by this study to be achieved. To this end, ICT masters, internet café operators and some students involved in sakawa activities were targeted for the interviews. Table 3.1 shows the sample size distribution for the study.

S/N	CATEGORY	SIZE	TOOL USED	METHOD OF DATA COLLECTION
1	Students (40 of them involved in Sakawa)	120	Questionnaire	Interviews
2	ICT Teachers	8	Interview schedule	Focus Group discussions
3	Internet café operators	4	Interview schedule	Interview
4	Police Officers	2	Interview scheduled	Interview

Table 3.1. Distribution of the Sample Size for the study

Source: Fieldwork, (2017).

3.5 Data Sources

Data for the study were derived from both primary and secondary sources. The primary data were obtained directly from the respondents through the questionnaires and the interview guides while Secondary data was obtained from Ghana Education service, articles, published and unpublished thesis, government documents, journals and other existing literature.

3.6. Data Collection Techniques and Tools

The reliability and validity of every research depends largely on the appropriateness of the instruments (Godfred, 2015). The instruments used in the data collection were interviews with the help of questionnaires and supplemented by focus group discussion and observations. The data were collected from students, teachers, sakawa guys and internet café operators in the Tamale Metropolis with the aid of interview guide using structured and semi-structured questionnaires. The structured questionnaires provided predetermined closed-ended questions with options for respondents to choose from, whilst the semi-structured questionnaires provided both open-ended and closed-ended questions for respondents to answer (Kamara, 1999; Twumasi, 2001). The questionnaire used is presented in appendix A.

In order to reduce the ambiguities and avoid unanswered questions, the questionnaire for this study was pre-tested (Ahuja, 2007). The questionnaire was pre-tested in the Tamale Islamic Senior High School in the Sagnarigu District.

3.7. Data Analysis and Presentation

This section shows how the analysis and presentation of data were carried out. Descriptive statistics such as frequencies, percentages, mode and median were used for the purpose of analysing the data collected. Frequency distribution tables, bar charts and pie charts were employed as tools for data presentation. This method is easy to understand and gives a vivid picture of the data analysed. In addition, the respondents were asked to rank some predetermined causes identified from the literature from which Kendall's W was used to determine the extent of agreement in the ranks.

Kendall's Coefficient of Concordance (W)

Kendall's W extends the analysis of Spearman's correlation coefficient to calculate the level of agreement among three (3) or more rankers as they rank a number of subjects according to particular characteristic. What this means is that a number of subjects, n, are ranked (1 to n) by each of the respondents and the statistic (Kendall's W) indicates how much the respondents agree with one another. For the purpose of this study, the number of rankers was the number of respondents (120) whereas the number of subjects to be ranked was the number of predetermined causes of cybercrime. The mean ranks were also used to identify the major cause to the least cause of cybercrime in the Tamale Metropolis. The analysis was carried out using the Statistical Package for Social Scientists (SPSS).

According to Legendre (2005), the Kendall's coefficient of concordance *(W)* is represented by the equation (1)

$$w = \frac{12s}{P^2\left(n^3 - n\right)} - p^t \quad \text{.....(1)}$$

Where: W represents the Kendall's coefficient of concordance; P denotes the 120 students ranking the challenges, n denotes the number of challenges ranked and t denotes correction factor for tied ranks, while *s* denotes the sum of squares statistics over the row sum of ranks (Ri). The sum of square statistics (*S)* is given as:

$$S = \sum_{i-1}^{n} (R_i - R)^2 \text{.....(2)}$$

Where $R_i$is row sums of rank and R is the mean of R_i. The correction factor for tied ranks (T) is also given as:

$$\text{T}= \sum_{k-1}^{m} \left(t^3 - t_k\right) \text{.....(3)}$$

Where $t^3$is the number of ranks in each of *m* group of ties

The test of significance of the Kendall's coefficient of concordance was done using the chi-square statistics which is computed using the formulae:

$$X^2 = P(n-1)W \text{.....(8)}$$

3.8 Ethical Consideration

The respondents' anonymity and confidentiality were assured because of the sensitivity of subject under study. Prior notices were given to the respondents before the interview dates were slated. An introductory letter was collected from the department to assist the

researcher to collect data from the respondents. Permission was obtained from the Ghana Education Service to the four selected schools. This permitted the researcher to conduct a study under this topic without any intimidation. The methods and techniques were meticulously selected to prevent the study from hurting or harming its respondents and the respondents were informed about the purpose of the study. This helped the researcher to collect accurate and relevant data from the respondents under all circumstances as asserted by Creswell (2013).

3.8 Validity and Reliability

In order to ensure the validity of information gathered from the field and the analysis of the data, each of the data collection instrument was pretested. This was done to know whether respondents have fore knowledge of the phenomenon before later the questionnaires were administered. This was done to check for the accuracy of the findings by employing certain procedures. With this the transcripts were appropriately checked to ensure that they contain the necessary information to the study. After which the codes were constantly compared to the data with which the codes have been assigned to. The codes were cross-checked by different researchers who have requisite knowledge about the phenomenon by comparing results that are independently derived as asserted by Creswell (2009). This was possible, because the supervisor in tandem with other colleagues made relevant suggestions to refine the study. In subsequent, triangulation of different sources of data were examined. This helped the researcher to test the accuracy of the research tools used against the expected outcomes. This aided the researcher an opportunity to eschew errors and repetition of similar studies or ideas from the field. Also, it helped the researcher

to clarify ambiguous interpretation of the data by following up to confirm from the respondents who responded to certain specific questions.

3.9 Limitations of the study

The study was saddled with some challenges. To some point the researcher finds it difficult to schedule interview meeting with the respondents, particularly the ICT teachers and the café operators due to their busy schedules. At times when appointments were made, they were cancelled for lashing with co-curricular activities and emergency (unexpected) schedules of the respondents. In consequence, some respondents failed to corporate with the researcher and since the topic is very sensitive others became annoyed of involving them in the study, though they were pre-informed before the inception of the interviews. Students' respondents were running away from the researcher and were not ready to disclose certain relevant information regarding the study. Some of the students had the feeling that the researcher was from the security service who wanted to sort sensitive information to arrest them. Internet café operators were unwilling to disclose certain information for the fear that the researcher wanted to collapse their businesses which aid them income for living and were much hostile to the researcher.

On the part of the schools, even though the researcher sought permission from the Ghana Education Service in the Metropolis, some head teachers blatantly refused the researcher the opportunity to conduct the research in their schools. The reason provided was that the researcher could be a journalist by name Anas Aremeyaw Anas (a world-renowned investigative journalist) who wants to interrogate them and publically broadcast the information of school which could tarnish the image of the schools. To some point, some

head teachers, café operators and even students were playing hide and seek with the researcher. Some schools were far apart which needless to say was a bit difficult for researcher and this impel her to work for distance before reaching the destination for information.

Although the researcher faced the outlined challenges, it is worth to note that the challenges could not prevent her from obtaining important information from the willing respondents for the work to be completed. To combat these challenges, first of all, the researcher explained to the respondents and other stakeholders the rationale for the research, which is purely for an academic exercise for the award of a Master of Philosophy degree. This was followed up on other occasions by producing the school identity card of the researcher and an introductory letter from the university. This made those who were unwilling to respond to the questions to provided adequate time for the study.

Again, the research assistants helped to explain certain things to the respondents for the information to be gathered.

The researcher was determined to eliminate all bottlenecks that are likely to affect findings of the study. The purpose of the study was painstakingly explained to the respondents and in other occasions, meetings with respondents were rescheduled several times in order to get the necessary inputs and to ensure the accuracy of the data gathered. Internet café operators closed late at night and therefore time was made by the researcher to meet them during Sundays when they do not operate.

Students were also educated on the fact that the responses they provide will be anonymous and will not seek to victimise them now or the future. They were encouraged to feel at home and provide accurate responses to the questions asked. They were also given the questions to fill on their own (self-administered) after taking them through the questionnaires. This gave them some privacy and allowed them enough time to be able to respond appropriately without hesitation.

All these efforts while being put in place to offset the challenges also came along with a common challenge, time. It was time consuming to put these measures in place towards combating the challenges confronting the research. To address the time challenge, the research employed competent research assistants to speed up questionnaire administration, interviews and data entry. The researcher worked tirelessly to conduct analyses and the write-up of the results.

CHAPTER FOUR

DATA PRESENTATION AND ANALYSIS

4.0 Introduction

This chapter presents detailed presentation and analyses of the data obtained from the study field. These findings are categorised into three (3) broad sections. The various objectives are treated under these broad sections. The first section deals with the demographic characteristics of the respondents whilst the other two sections extensively discuss the awareness level, causes and effects of cybercrime in the Metropolis.

4.1 Demographic Characteristics of the Respondents

This section analyses the social and demographic characteristics of the respondents. The sex, age, and religious denomination of the respondents are analysed under this section. The respondents selected were 120 for the study and these are students within the selected schools within the metropolis

4.1.1 Sex of Respondents

Figure 4.1 illustrates the sex distribution of the 120 respondents. Of these respondents, 64.2% of them were male whereas 35.8% were female. This emphasised that there were more males in the selected schools than females. This is in congruent with an assertion by the ICT teacher when he expressed the view that:

"in this school male students are more than the females and besides that the male students have much interest in ICT than the females, so to me it is not surprising that the

males in this part of the country are mainly involve in the sakawa business than females (Interview, February 10, 2018).

It could be deduced from the narration that male students are likely to enter cybercrime activities than their female counterparts. During the data collection it was observed that respondents who were sincere to disclose their identity for being involved in the sakawa business are mainly male students. This supports an interview conducted with one of the perpetrators that the male child has been indoctrinated since infancy to be the bread winners of the family. This makes them to be more aggressive to be look for means to survive in terms of difficulties. Therefore, if parents are unable to provide for them, they had no other alternative than to involve in delinquency to enable them achieve their aims. This supports the strain theory or theory of anomie that when the individuals perceived the means of achieving the societal goals to be too long, they innovate illegitimate ways of achieving their goals rather than to follow the lay down procedure. This is illustrated in the figure.4.1 below.

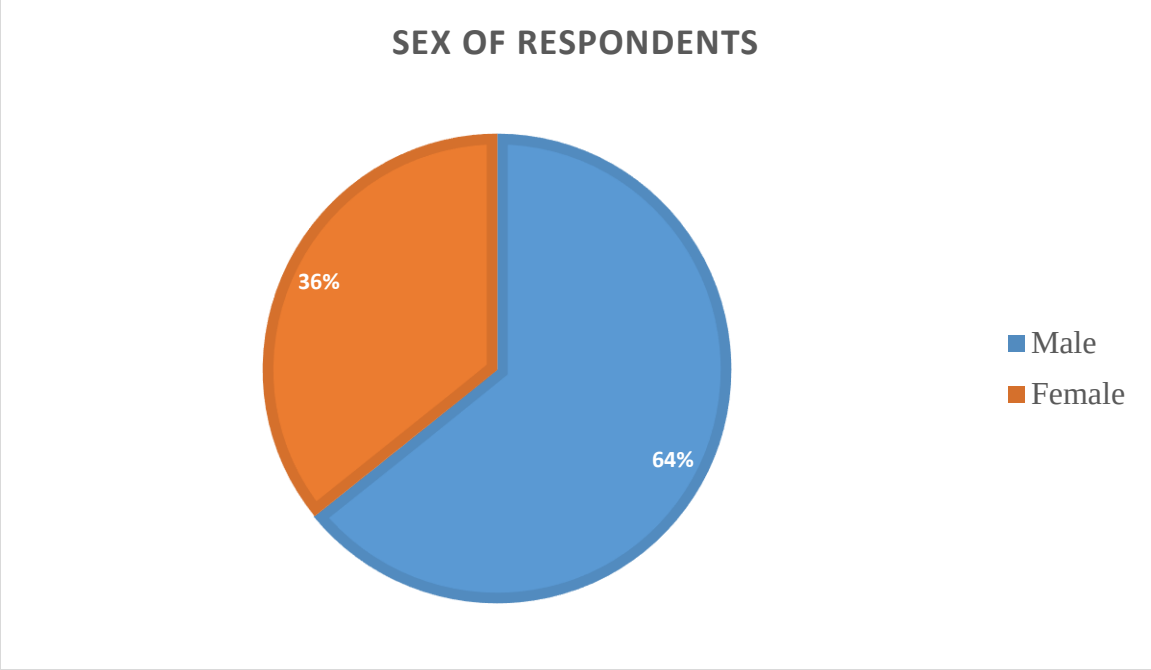

Figure 4.1. Sex of Respondents

Source: field survey, March, 2017

4.1.2 Age of Respondents

The age distribution of the respondents is illustrated in Figure 4.2. The results show that majority of the respondents are in the age 18-22 years category representing 53.3% of the respondents. This confirms the Ghana Statistical report (2014), majority of the youth are within the ages 18-24. It further affirms the findings of Assaad and Roudi-Fahimi (2007) that youth represent a period in life when one makes the transition from the dependence of childhood to the independence of adulthood. This implies that the youth at this period are filled with enthusiasms, dreams and ambitions. The age of the respondents is followed by those within 15-17 years representing 20% of the respondents; whilst few of the respondents are in the age 28 and above year's category. The results give an indication of

youthful respondents and thus, representative of the category who have greater inter interaction with the computer and on the internet via social media and other means. The results further points to the fact that at that age, they enjoy company of friends and seen hanging up with them during schools and holidays. Parents also allow their children space to interact with their colleagues with the intention that they share knowledge and exchange ideas from what they learn in school.

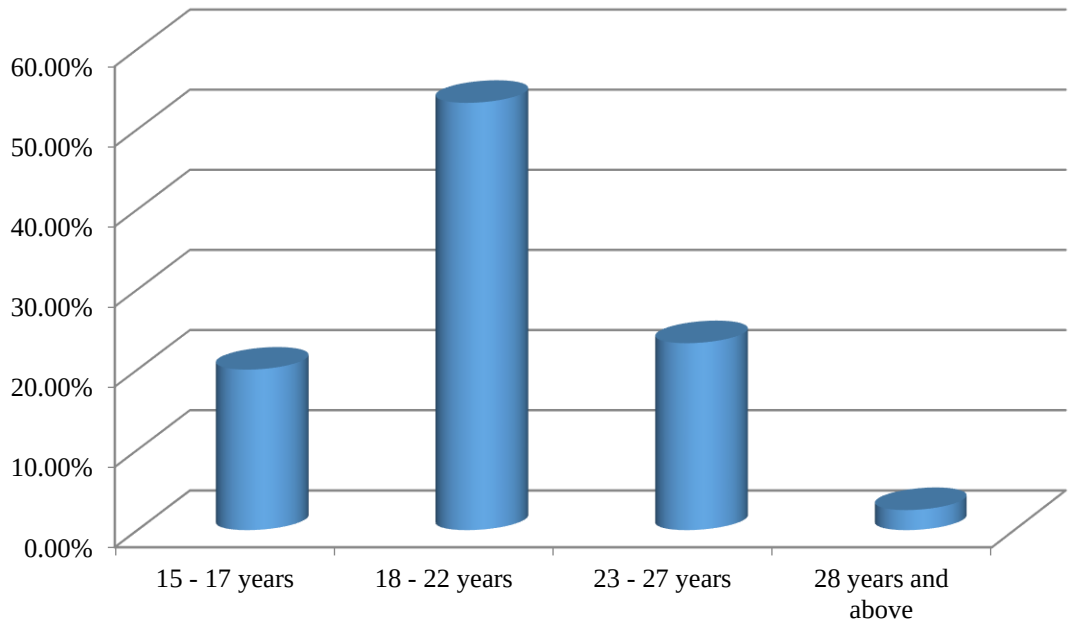

Figure 4.2. Age of respondents

Source: Field Survey, March, 2017.

4.1.3 Religious Denomination of Respondents

The religious denominations of the respondents are captured in Table 4.1. The results show that majority of the respondents (85%) belong to the Islamic faith whilst the remaining

15% are Christians This result is in line with the general religious distribution in the Tamale Metropolis where Muslims are the majority (Ghana Statistical Service, 2014). The religious affiliation of respondents was much imperative since the religion frowns upon crime and considers members who involve in crime as sinners and, or violators of the Holy Bible, Quran and the Tora. Therefore, the religion of a person can influence him or her to refrain from committing cybercrime since members mostly adhere to the directives of their leaders and view them as the eye of God.

Table 4.1. Religious Denomination of Respondents

Religion	Frequency	Percentage
Islam	102	85.00%
Christianity	18	15.00%
Total	**120**	**100.00%**

Source: Field Survey, April, 2017

4.2 Respondents Awareness of Cybercrime (Sakawa)

4.2.1 Knowledge of Cybercrime

The knowledge of cybercrime by the respondents is represented in Figure 4.3. The result shows that almost all (92.5%) of the respondents indicated they know what cybercrime (sakawa) entails. However, 7.5% of the respondents indicated that they do not know what cybercrime entails. The respondents who indicated that they know what cybercrime entails

said a lot about the activities of cybercrime. Most of their definitions revolve around the use of ICT tools and 'juju' in stealing. For example, these are what two students said about cybercrime '*the youth faking their identities (using pictures and information about others) on social media to steal money*'. Another student wrote: *'fraudsters pick up new identities and trick other people into believing in them and then dupe them of their money, sometimes using spiritual help'*. The views of the ICT masters (teachers) as well as the internet café operators were in agreement with what most of the students expressed.

One ICT Master added that,

"The students show so much interest in the ICT subject. They want to learn more, especially about internet surfing and social media handles. Some of them use the knowledge they acquire to commit crimes"

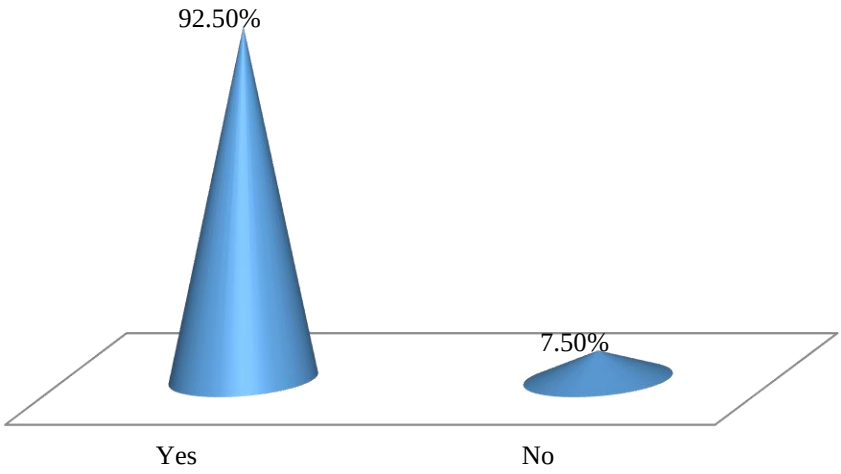

Figure 4.3. Knowledge of Cybercrimes

Source: Field Survey, April, 2017

4.2.2 The Frequency of Cybercrime (Sakawa) Activities

Table 4.2 shows the frequency of cybercrime. One half of the respondents indicated that they have heard or seen friends involved in cybercrime (or sakawa) activities very often. Whilst 31.7% of the respondents indicated that they often hear/see people involved in cybercrime (or sakawa) activities, 14.2% indicated that they seldom hear of or see people involve in cybercrime (or sakawa) activities. However, respondents who said they have never heard of or seen someone involved in cybercrime (or sakawa) activities constitute 4.2%. One of the internet cafe operators interviewed said everyday young boys come to access the net trying to get their 'friends' send money to them by deceiving them. He stressed 'it is regular for many of them'. He maintained that most of the youth are influenced into the activities by their peers. Also, the study observed that the young males are mostly involved in the cybercrimes than females. This correspond to an interview with a police officer when he alluded that:

"All cybercrime perpetrators in this region are young males who want to get rich overnight. Cybercrime cases reported to since 2015 involved young men who have just completed either SHS and are tertiary students" (interview, January 17th, 2019).

Table 4.2. Frequency of Cyber Fraud Activities

Frequency of Cybercrime	Frequency	Percentage
Very often	60	50.0%
Often	38	31.7%
Seldom	17	14.2%
Never	5	4.2%
TOTAL	**120**	**100%**

Source: Field Survey, June, 2017

4.2.3 Places where Cybercrime (Sakawa) Activities are perpetrated

Table 4.3 shows the findings of the study as regards the places where cybercrime (or sakawa) activities are usually perpetrated. Most (79.2%) of the respondents indicated that cybercrime (or sakawa) activities are usually carried out at the internet cafes. A few others, constituting 13.8%, indicated that these activities are usually carried out at homes. However, very few respondents indicated that cybercrime is usually committed at computer labs, hotels, and government and private offices. During the interview of key informants (internet café operators), the respondents indicated that most of the sakawa guys (some of them in school uniforms) are always found in the cafés, especially during weekends when school is not in session. They search for their victims (mostly white ladies and men) and entice them. One of the respondents said 'at night the links are very good and fast, so they usually spend all the night there [the internet cafe]. Aside the speed of the internet at night, the night time in Ghana corresponds to the time some people in other parts of the world (Example in North America) might have closed from work or are free to chat

with friends. This statement is in congruent with the assertion by Okeshola and Adeta (2013) when they emphasised that cybercrime is mostly committed at internet cafes and at night where they would be no destruction to obstruct the perpetrators from duping the victims.

Table 4.3 Places of Cybercrime Activities

Place	Frequency	Percentage
Internet café	95	79.20%
Home	16	13.80%
Computer lab	3	2.50%
Hotel	2	1.70%
Government office	1	1.70%
Private office	2	1.70%
Total	**120**	**100.00%**

Source: Field Survey, June, 2017

4.2.4 Activities Respondents Accessed on the Internet

A multiple response set was created for the activities the respondents ever accessed using the internet including social media (Facebook and WhatsApp), Google Search, E-mail, academic research, internet phoning, pornography, spamming, and piracy. Respondents were asked to tick all that apply. A multiple response analysis was performed and the result is shown in the Table 4.4. A total of 297 ticks were obtained. Whereas many of the

respondents indicated they have ever accessed social media, Google search, E-mail and academic research which constitute 70.7%, 80.2%, 57.8% and 35.3% of the respondents respectively, few of them reported that they have ever performed internet phoning, pornography and spamming which constitutes 6.0%, 3.6% and 2.4% of the respondents respectively. No respondent indicated that he or she has ever performed piracy. The internet café operators also indicated that the sakawa guys usually reach out their victims by sending unsolicited emails. It is evident from table 4.4 that majority (80.2%) of the total respondents accessed cybercrime activities on the Google search. The ICT teachers in the selected schools confirmed that in most instances when the students go to the schools' computer laboratory, instead of surfing the internet for academic purposes, there will be using the internet to search for irrelevant materials that relate to how to dupe a person for get rich. The teachers revealed that students who were caught in that act were advised and stringent measures had been provided to regulate the internet activities of the students in the schools' laboratories. Even though, the teachers had revealed that the schools had provided stringent measures, it was observed that there were some instances where the students were left alone in the computer lab without any teacher facilitating their movements or activities.

Table 4.4. Activities Respondents Accessed on the Internet

Item	Frequency	Percentage	Percentage of cases
Social media	82	27.60%	70.00%
Google search	93	31.30%	80.20%
E-mail	67	22.60%	57.80%
Academic research	41	13.80%	35.30%
Internet Phoning	7	2.40%	6.00%
Pornography	4	1.30%	3.40%
Spamming	3	1.00%	2.60%
Piracy		0.00%	0.00%
Total	**297**	**100.00%**	

Source: Field Survey, July, 2017

4.3 Social Attributes of Cyber Criminals or Sakawa Guys

This section gives an idea of the characteristics of the cyber fraudsters. The social attributes of Sakawa guys such as age, sex, level of education and religious denomination were assessed.

4.3.1 Age of most Sakawa Guys

The age distribution of sakawa guys is presented in Table 4.5. The results show that most half of the students who are involved in cybercrime activities (50%) are within the age category of 18 – 22 years. Similarly, the police officers also indicated majority of cybercrime perpetrators are within the ages of 20 and 25. Again, a cafe operator said:

"I hardly see people older than me [he said he was 35 years] involved in this business. When you see someone like that [someone older than 35yeas] maybe he is coming to apply for something online or update his app. They don't spend much time here" (interview, January 13, 2019).

The above narration suggests that sakawa guys are mostly young guys who spend a lot of time in the cafes and they fall the age category of the youth. Therefore, this agrees with the report by the Australian Youth Affairs Coalition (2005) cited in Hasan et al., (2015) that the students in the age group of 18-24 are in high risk environments when exposed to online activities like cybercrime. Moreover, 40% and 10% of the sakawa guys indicated they are within the age brackets of 15 – 17 years and 23 – 27 years respectively. However, none of the respondents sakawa guys have ages 28 years and above. This concurs with most of the definitions the respondents give to cybercrime as most of it has the words 'young boys' or 'the youth'. The cafe operators also said it is mostly the youth that are involved in these activities.

Table 4.5. Ages Distribution of Sakawa Guys

Age category (in years)	Frequency	Percentage
15 – 17	16	40.0%
18 – 22	20	50.00%
23 – 27	4	10. 00%
28 and above	0	0.00%
Total	**40**	**100.00%**

Source: Field Survey, May, 2017

4.3.2 Sex and Religious Denomination of Most Sakawa Guys

As shown in Table 4.6, majority of the sakawa guys (75%) are boys while the remaining 25% are girls. The girls involved are normally used by the boys to lure their prey as potential brides. The above analyses reveal that females are not usually involve in cybercriminal activities. However, one of the internet operators interviewed said sometimes young beautiful ladies are used by cyber criminals to lure their victims.

To this end, a girl remarked that "I work with my boyfriend who has a client (white man). He used my picture to propose to him and agree to marry him" (interview, May 21, 2017).

This result is in sync with the findings of Warner (2011) that 90% of cyber criminals in Ghana are male less than 30 years of ages who reside in or near urban centres where access to internet cafes is easy.

Table 4.6 further illustrates the religious distribution of the sakawa guys in the Senior High Schools. The results show that majority of the respondents (67.5%) are Muslims while the remaining 32.5% are Christians. This result is in line with the religious distribution in the Tamale Metropolis as well as the sample used for this study.

Table 4.6. Sex and Religious Denomination of Sakawa Guys

Sex	**Frequency**	**Percentage**
Male	30	75.00%
Female	10	25.00%
Religion		
Islam	27	67.50%
Christianity	13	32.50%

Source: Field Survey, June, 2017

4.4 Causes of Cybercrime (Sakawa)

The causes of cybercrime are determined using the Kendall's Coefficient of Concordance. The Kendall's W ranks the scores in each row of the data file independently of every other row.

4.4.1. Mean Ranks of the causes of Cybercrime (Sakawa) and the Kendall's W

The mean ranks of the causes of sakawa and the Kendall's W are represented in Table 4.7. Kendall's coefficient of concordance (Kendall's W) was used to calculate agreements in the ranks among the respondents. In a circumstance where there is perfect agreement among the ranks, Kendall's W is one (1). Where maximum disagreement exists, Kendall's W is zero (0). Hence, Kendall's W neither takes negative values nor values greater than one (1).

Kendall's W, as can be seen in Table 4.7, was 0.520. This means that there was moderately strong agreement among the respondents in their ranking. The chi-square tests the null hypothesis that ranks of the variable does not differ from their expected value. For a constant sample size, the higher the value of the chi-square statistic the larger the difference between each variable rank sum and its expected value. From table 4.7, the chi-square value is 374.5 with 6 degrees of freedom. The p-value (0.000) is the approximate probability of obtaining a chi-square statistic as extreme as 374.5 with six (6) degrees of freedom in repeated samples if the rankings of each cause are not different. Because a chi-square of 374.5 with six (6) degrees of freedom is unlikely to have arisen by chance, it is

concluded that there is agreement among the ranks of the respondents for all seven (7) causes.

The ranking of the causes of cybercrime was carried out by each respondent who participated. The ranks for each cause was summed and then divided by the number of rankers (respondents) to yield a mean rank for that particular cause. It can be seen that Peer Group Influence has the lowest mean rank of 2.32. This means that the 120 respondents tended to rank Peer Group Influence more highly than the other six (6) causes. Hence, the study identified Peer Group Influence as the major cause of cybercrime (sakawa) in the Tamale Metropolitan Assembly. This is consonance with the differential association theory which argues the environment of persons influence them to commit crime.

This was followed by Poverty and Youth Unemployment with mean ranks of 2.52 and 2.79 respectively. Easy Access to Internet is the fourth most severe cause of cybercrime in the metropolis. In summary, the mean of ranks gives the causes from the most severe to the least cause of cybercrime in the Tamale Metropolitan Assembly as: Peer Group Influence, Poverty, Youth Unemployment, Easy Access to Internet, Weak Laws, Defective Socialisation and Corruption. In relation to this study, the perpetrators had easy access to the internet and that impel them to commit crime. Similarly, the study supports relative deprivation theory by Ted Gur (2015) cited in Alonso and Andrews, (2019) that when the individual expectations are denied, they resort to committing crime in order to achieve their societal needs. Therefore, in the quests of some youth seeking to be employed without getting job resort to cybercrime in order to earn money for living as indicated by Warner (2011).

Table 4.7. Causes of Cybercrime

Cause	Mean Rank	Position
Easy access to internet	3.71	4th
Weak laws	5.18	5th
Peer group influence	2.32	1st
Poverty	2.52	2nd
Youth Unemployment	2.79	3rd
Defective socialisation	5.24	6th
Corruption	6.25	7th
Number of rankers		120
Kendall's coefficient of concordance		0.520
Chi-square (χ^2)		374.500
Degrees of freedom6		6
p-Value		0.000

Source: Field Survey, August, 2017

4.5. Effects of Cybercrime on Academic Performance of Students

The effects of cybercrime on academic performance of SHS students especially those involved in the internet fraud (Sakawa Guys) are analysed by examining the effects of the cybercrime on attendance, performance and retention of the Sakawa guys.

4.5.1. Effect of Cybercrime on Attendance of SHS Students

On a Likert scale of 1 – 5, the effects of cybercrime (sakawa) on the performance of Senior High School students was measured by assigning weights to the extent of agreement or disagreement of the respondents to each item. The respondents strongly agree, agree, remain neutral (neither agree nor disagree), disagree, or strongly disagree to each of the statements made.

Table 4.8 illustrates the extent of agreement of the respondents with regards to whether the sakawa guys come to school early. Whereas 8.3% of the respondents agree or strongly agree that sakawa guys come to school early, most (87.5%) of them (the respondents) disagree or strongly disagree that sakawa guys come to school early. However, 7.5% of the respondents indicated that they have no opinion regarding the lateness of sakawa guys to school. Some of these respondents said they have not taken notice of that while others said sakawa guys they know are not in their classes or are not in the school at all. The ICT teachers revealed in an interview indicated that "though the sakawa guys do not come early to school, they are punctual in ICT lessons". This is as a result of their interest in that subject as a necessary tool towards enhancing their cyber activities.

Table 4.8. Sakawa guys come to school early.

Come Early to School	Frequency	Percentage
Strongly agree	1	2.50%
Agree	1	2.50%
Neither agree nor disagree	3	7.50%
Disagree	10	25.00%
Strongly disagree	25	62.50%
Total	**40**	**100.00%**

Source: Field Survey, August, 2017

4.5.2. Punctuality of Sakawa Guys at School

As it can be seen in Table 4.9, only 5% of the respondents agree or strongly agree that sakawa guys are punctual at school. Most of the respondents (85%) disagree or strongly disagree that sakawa guys are punctual at school. The remaining 10% of the respondents neither agree nor disagree that sakawa guys are punctual at school.

Table 4.9 Sakawa guys are punctual at school.

Rate	Frequency	Percentage
Strongly agree	1	2.5%
Agree	1	2.50%
Neither agree nor disagree	4	10.00%
Disagree	12	30.00%
Strongly disagree	22	55.00%
Total	**40**	**100.00%**

Source: Field Survey, September, 2017

4.5.3. Performance of Sakawa Guys

Table 4.10 illustrates the performance of Sakawa guys in examination. The results show that many (87.5%) of the respondents agree or strongly agree that sakawa guys perform poorly in examinations. A few (7.5%), however, disagree or strongly disagree that sakawa guys perform poorly in examinations. However, 5.0% of them neither agree nor disagree that sakawa guys perform poorly in examinations. A visual inspection of their exercises revealed that Sakawa guys do not perform well as compared to their counterparts. This means that most of the sakawa guys perform poorly in examinations. This is to be expected as they spend most of their time surfing through the internet and interacting court their prey. The trade-off of academic work for courting prey implies loss of valuable reading time in favour of cyber activities. The ICT teachers also corroborated this finding

indicating that "the sakawa guys perform poorly in most of the subjects especially the core subjects due to their absenteeism and lateness to school." These indications were further confirmed by the sampled terminal report cards of some of the sakawa guys in the various schools. The observation of the terminal report cards indicated that the sakawa guys perform poorly in Mathematics and Integrated Science.

Table 4.10. Sakawa guys perform poorly in examinations.

Rate	Frequency	Percentage
Strongly agree	23	57.5%
Agree	12	30.00%
Neither agree nor disagree	2	5.00%
Disagree	2	5.00%
Strongly disagree	1	2.50%
Total	40	100.00%

Source: Fieldwork, 2017

4.5.4. Retention of Sakawa Guys

The retention of Sakawa guys in school is represented in Table 4.11. The results show that most of the respondents strongly agree (45%) and agree (45%) that the sakawa guys have

high tendency of dropping out of school. On the other hand, only 5% of the respondents strongly disagree and disagree. This shows that the majority of the respondents agree that the sakawa guys easily drop out of school. This phenomenon is due to the fact that "for most of them who 'hit', they are overwhelmed by the large amounts they receive and therefore do not find the need to continue with their education, since for them, the purpose of education is to gain employment, make money and become successful in life." As remarked by one of the ICT masters. Another ICT master stated that "some of the pupils drop out of school due to poor performance in the examinations. One boy in my class stopped schooling because he said he felt embarrassed that his name appeared on the notice board for poor performance in the examination."

Table 4.11. Sakawa guys are more likely to stop coming to school.

Rate	Frequency	Percentage
Strongly agree	18	45.00%
Agree	18	45.00%
Neither agree nor disagree	2	5.00%
Disagree	1	2.50%
Strongly disagree	1	2.50%
Total	**40**	**100.00%**

Source: Field Survey, September, 2017

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.0. Introduction

This chapter entails the summary, conclusions and recommendations of the study based on the outcomes of the analyses. The summary provides a snapshot of the salient issues emerging out of the study. The conclusion states the position regarding the objectives set; whilst the recommendations provide suggestions on the way forward.

5.1. Summary

The study sort to examine the implications of cybercrime on secondary education in the Tamale Metropolis of Northern Ghana. The study administered structured questionnaire on 120 respondents selected using multistage sampling technique, which involved the simple random sampling technique where respondents have equal chance of being selected. The purposive sampling technique was used to select key informants (café managers) for the interviews; whereas the snowball sampling technique was used for the purpose of identifying 40 students who were sakawa guys for interviews. Structured questionnaire was administered on the respondents.

The analysis of the data shows that almost all (92.5%) of the respondents indicated they know what cybercrime (sakawa) entails. On the frequency of cybercrimes, 31.7% of the respondents indicated that they often hear of or see people involved in cybercrime (or sakawa) activities whilst 14.2% indicated that they seldom hear of or see people involved

in cybercrime (or sakawa) activities. The study further indicated that most cybercrimes (79.2%) are committed at the internet cafes; few others constituting 13.8% indicated that these activities are usually carried out at homes. The age distribution of the Sakawa guys show that most (50.0%) of the sakawa guys have ages ranging from 18 to 22 years. A few (12.5% and 10.8%) of the respondents indicated that most sakawa guys they know have ages which falls from 13 – 17 years and 23 – 27 years.

The Kendall's W was used to estimate the level of agreement among respondents as to the causes of cybercrimes in the Tamale Metropolis. The Kendall's coefficient of concordance (0.520) means that there was about 52% (moderately strong) agreement among the respondents in their ranking of the causes of cybercrimes. The ranking of the causes of cybercrime indicates that Peer Group Influence has the lowest mean rank of 2.32, followed by Poverty and Youth Unemployment with mean ranks of 2.52 and 2.79 respectively. On the other hand, Corruption and defective socialisation are ranked the least with a mean rank of 6.25 and 5.24 respectively.

The study also revealed significant effect of cybercrimes or sakawa on the educational attainment of the sakawa guys. The study revealed that only 5.0% of the respondents agree or strongly agree that sakawa guys come to school early, whilst most (87.5%) of the respondents disagree or strongly disagree that sakawa guys come to school early. Moreover, only 5.0% of the respondents agree or strongly agree that sakawa guys are punctual at school, but most of the respondents (85%) disagree or strongly disagree that sakawa guys are punctual at school. The performance of the sakawa guys in school is also affected by the cybercrime activities as many of the respondents (87.5%) agree or strongly

agree that sakawa guys perform poorly in examinations. A few (7.5%), however, disagree or strongly disagree that sakawa guys perform poorly in examinations. However, 5.0% of the respondents neither agree nor disagree that sakawa guys perform poorly in examinations. Finally, retention of Sakawa guys in school is poor, as most of the respondents agree (90%) and strongly agree (5%) that the sakawa guys have higher probability of dropping out of school.

5.2. Conclusion

The study achieved the set objective of examining the implications of cybercrime on secondary education in the Tamale Metropolis of Northern Ghana. The analyses of the results reveal that the sakawa menace is in the fibre of some Senior High School Pupils, and msut be dealt with to avoid its widespread to the majority of the students through peer group influence, which is the most common path to the menace. The study also implies that the most important causes of the sakawa or cybercrime are peer group influence, unemployment, easy access to internet and weak laws governing cyber activities. TheA sakawa phenomenon is said to affect all walks of life of the perpetrators, especially, their educational development; it affects attendance, punctuality, performance and retention in school.

5.3. Recommendations

The findings of this study calls for intervention by all stakeholders (parents, tutors, government, and non-governmental organisations) to help address the upsurge of the cybercrimes in schools in particular and the country in general. Therefore the following recommendation are made for consideration:

- Promotion of responsible use of the internet: School authorities and non-governmental organisations need to sensitise students on the responsible use of the internet and to educate the public on the menace of cybercrime in the metropolis. Parents have the enormous responsibility on the guidance and enforcement towards the responsible use of the internet. This will further deepen the awareness level of SHS students in ICT and also promote their responsible use of the internet.

- The government should ensure effective implementation of existing legislations and polices on cyber activities to regulate the use of internet and guide internet cafés to operate in accordance with the law to eschew student from committing cybercrime.

- Enforcement of school regulations: The school authorities should endeavour to enforce school regulations to restrict students from using sophisticated phones. The rules and regulations restricting students from using such phones at school will prevent students' sakawa perpetrators from committing cybercrime and concentrate fully on their academic works. This will help to optimize the academic performance of the secondary schools in the Metropolis and the country at large.

- Parents should endeavour to monitor the movement of their children and questioning students who spend more time outside the house and return home at late hours. They help to provide some basic needs for their wards to school and should also refrain from buying sophisticated phones for their children. This will reduce the rate of cybercrime in the Metropolis since the children needs are catered for, they may not try to use illegitimate ways of committing cybercrime.

- Community Members should try as much as possible to report cybercrime perpetrators to the police and assist the police to identify and arrest perpetrators of cybercrime in the Metropolis. In addition, since most members of the communities perceive the priest, fetish priest, Imams and the traditional leaders as God's eyes, they should endeavour to inculcate the moral values into the youth and educate them on the necessity to start life from one step to the other. In addition, since there is a belief that those who flouted the directives of God who not make to heaven, many who want to go to heaven as believed will desist from committing cybercrime.

The above suggested recommendations when followed will ensure reduction and possible eradication of the sakawa or cybercrime menace at the senior high schools in the Tamale Metropolis.

REFERENCES

Abia, W., Jato, D., Agejo, P., Abia, E., Njuacha, G., Amana, D., & Ekuri, D. (2010). Cameroonian youths, their attractions to scamming and strategies to divert attention. *International NGO Journal*, *5*(5), 110-116.

Adinkrah, M. (2011). Epidemiologic characteristics of suicidal behavior in contemporary sGhana. Crisis.

Adu-Agyem, J., and Osei-Poku, P. (2012). Quality education in Ghana: The way forward. *International Journal of Innovative Research and Development*, *1*(9), 164- 177.

Adu-Gyamfi, S., Donkoh, W. J., and Addo, A. (2017). Educational reforms in Ghana: past and present. *Journal of Education and Human Development*, *5*(3), 158-172.

Afari-Boateng S. (2014). Time Series Analysis (Autoregressive Integrated Moving Average Model) of the Major Crimes in Ghana. The Case Study of Eastern Region.

Agnew, R. (2014). General strain theory. *Encyclopedia of criminology and criminal justice*, 1892-1900.

Agnew, R. (2010). A general strain theory of terrorism. *Theoretical Criminology*, *14*(2), 131-153.

Ahuja, R. (2007). *Research Methods.Rawat Publishers*, New Delhi, India.

Akers, R. L., & Jennings, W. G. (2015). Social learning theory. *The Handbook of Criminological Theory*, *4*, 230.

Akogwu, S. (2012), *An Assessment of the Level of Awareness on Cybercrime among Internet Users in Ahmadu Bello University, Zaria (Unpublished B.Sc project)*.Department of Sociology, Ahmadu Bello University, Zaria.

Alhassan, E., Felicia, O. S., & Ameyaw, S. Idling of the youth without jobs and its implications in the Wa municipality of the upper west region of Ghana.

Alonso, J. M., & Andrews, R. (2019). Fiscal decentralisation and local government efficiency: Does relative deprivation matter?.cial and personality psychology, 81-97.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., ... and Savage, S. (2013). Measuring the cost of cybercrime. In *The economics of information security and privacy* (pp. 265-300). Springer, Berlin, Heidelberg.

Aseef,N.,Davis, P., Mittal, M., Sedky, K., and Tolba, A. (2005).*Cyber-Criminal Activity and Analysis*, White Paper, Group 2.

Asokhia, M., (2010). *Enhancing national development and growth through combating cybercrime internet fraud: A comparative approach*. Journal of Social Science, 23: 13-19.

Awe, J. (2009).*Fighting Cybercrime in Nigeria. R*etrieved on 23/03/17 from: http://www.jidaw.com/itsolutions/security3.html

Barfi, K. A., Nyagorme, P., & Yeboah, N. (2018). The Internet Users and Cybercrime in Ghana: Evidence from Senior High School in Brong Ahafo Region. *Library Philosophy and Practice*, 1-16.

Boateng, R., Longe O., Mbarika V., Avevor I., Isabalija S. R., (2010), *"Cybercrime and Criminality in Ghana: Its Forms and Implications"*, Americas Conference on Information Systems. (AMCIS) 2010 Proceedings, Available online http://aisel.aisnet.org/amcis2010/507

Bougaardt, G. and M. Kyobe, (2011).*Investigating the factors inhibiting SMEs from recognising and measuring losses from cybercrime in South Africa*.Electr. Journal of Inform. Syst. Evaluat., 14: 167-178.

Brantingham, P.L. and P.J. Brantingham (1993)."*Environment, Routine, and Situation: Toward a Pattern Theory of Crime."* In: R.V. Clarke and M. Felson (eds.), *Routine Activityand Rational Choice.* Advances in Criminological Theory, Vol. 5. New Brunswick, NJ: Transaction Publications.

Carmody, B. (2011). Towards a contemporary Catholic philosophy of education. *International Studies in Catholic Education*, *3*(2), 106-119.

Chawki, M., (2005).*A critical look at the regulation of cybercrime*.ICFAI J. Cyberlaw, 3: 1-55.

Choi, K.(2008). *Structural equation modelling assessment of key causal factors in computer crime victimisation*.Ph.D Dissertation, Indiana University of Pennsylvania, USA.

Choucri, N., Madnick, S., & Ferwerda, J. (2014). Institutions for cyber security: International responses and global imperatives. Information Technology for Development, 20(2), 96-121.

Cloward, R. A., & Ohlin, L. E. (2013). Delinquency and opportunity: A study of delinquent gangs. Routledge.

Cocchia, A. (2014). Smart and digital city: A systematic literature review. In *Smart city* (pp. 13-43). Springer, Cham.

Cohen, L.A., and Felson, M.(1979). *Social change and crime rate trends: A routine activities approach.* American Sociological Review, 44, 588-608.

Cooley, C. H. (2017). *Human nature and the social order*. Routledge.

Cornish, D. B., and Clarke, R. V. (2003). *Opportunities, precipitators, and criminal decisions: A reply to Wortley's critique of situational crime prevention*. In M. J. Smith and D. B Cornish (Eds.), *Theory for practice in situational crime prevention* (pp.41-96). Monsey, NY: `Criminal Justice Press.

Council of Europe's Convention on Cybercrime. (2001). *Budapest*, 23.XI.2001 Accessed http://www.europarl.europa.eu/meetdocs/20142019/documents/libe/dv/7convbudapest/7convbudapesten.pdf

Cukier, W., & Levin, A. (2009). Internet fraud and cybercrime. Crimes of the Internet, 251-279.

Crano, W. D., Brewer, M. B., & Lac, A. (2014). Principles and methods of social research. Routledge.

Creswell, J. W. (2014). *A concise introduction to mixed methods research*. Sage Publications.

Creswell, J. W. (2009). Mapping the field of mixed methods research.

Curtis, P.A. and L. Colwell, (2000). *Cybercrime: The next challenge: An overview of the challenges faced by law enforcement while investigating computer crimes in the year 2000 and beyond.*School of Law.

Danquah, P., & Longe, O. 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.

Das, S., & Nayak, T. (2013). Impact of cybercrime: Issues and challenges. International journal of engineering sciences & Emerging technologies, 6(2), 142-153.

Data Protection Act. (2012). Data Protection Act, Act 843 2012. Parliament House, Ghana. Available at https://www.dataprotection.org.gh/sites/default/files/Data%20Protection%20Act%20%2C%202012%20%28Act%20843%29.pdf

De Vaus, D., & de Vaus, D. (2013). Surveys in social research. Routledge.

Döring, N. M. (2009). The Internet's impact on sexuality: A critical review of 15 years of research. Computers in Human Behavior, 25(5), 1089-1101.

Downes, D., Rock, P. E., and McLaughlin, E. (2016). Understanding deviance: a guide to the sociology of crime and rule-breaking. Oxford University Press.

Duah, F. A. and Kwabena, A. M. (2015). The Impact of Cyber Crime on the Development of Electronic Business in Ghana. *European Journal of Business and Social Sciences*, 4(1): 22 – 34.

Duflo, E., Dupas, P., and Kremer, M. (2017). The impact of free secondary education: Experimental evidence from Ghana. *Massachusetts Institute of Technology Working Paper Cambridge, MA*.

Duah, F. A., and Kwabena, A. M. (2015). The impact of cybercrime on the development of electronic business in ghana. *European Journal of Business and Social Sciences*, *4*(01), 22-34.

Economic and Organised Crime Office, EOCO. (2010). Economic and Organised Crime Act, Act 804 2010. Parliament House, Ghana.

Edelman, L. (2009). Unbecoming: Pornography and the queer event. In *Post, porn, politics: Queer-feminist perspective on the politics of porn performance and sex-work as culture production [symposium, reader]* (pp. 33-46).

Ekwonwune, E. N., Egwuonwu, D. U., Elebri, L. C., & Uka, K. K. (2016). ICT as an instrument of enhanced banking system. *Journal of Computer and Communications*, *5*(1), 53-60.

Electronic Communications Act. (2008). Electronic Communication Act, Act 775. Ministry of Communication, Ghana. Available at https://www.moc.gov.gh/sites/default/files/downloads/Electronic%20Communications%20Act-775.pdf

Electronic Transactions Act. (2008). Electronic Transactions Act, Act 772. Parliament House, Ghana. Available at https://www.researchictafrica.net/countries/ghana/Electronic_Transactions_Act_no_772:2008.pdf

Ennin, D. (2015). *Cybercrime in Ghana: A Study Of Offenders, Victims and the Law*. Thesis: University of Ghana.

Entwistle, N. J. (2013). Styles of learning and teaching: An integrated outline of educational psychology for students, teachers and lecturers. David Fulton Publishers.

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

Felson, M., and Clarke, R. V. (1998).*Opportunity makes the thief: Practical theory for crime prevention*. London: Home Office and Reducing Crime Unit.

Fernández-Oliveras, A., and Oliveras, M. L. (2015). Conceptions of science, mathematics, and education of prospective kindergarten teachers in a play-based training. *International Journal on Advances in Education Research*, *2*(1), 37-48.

Furnell, S., Emm, D., & Papadaki, M. (2015). The challenge of measuring cyber-dependent crimes. Computer Fraud & Security, 2015(10), 5-12.

Ghana. Statistical Service. (2014). 2010 population and housing census report. Ghana Statistical Service.

Ghana. Statistical Service. (2013). 2010 Population & Housing Census: Brong-Ahafo Region (Vol. 2). Ghana Statistical Service.

Graham, C. K. (2013). *The History of Education in Ghana: From the Earliest Times to the Declaration of Independance*. Routledge.

Godfred, A. (2015). *Research Instruments for Data Collection.*Kwame Nkrumah University of Science and Technology, Ghana.Retrieved from: http://campus.educadium.com/newmediart/file.php/1/giilmadstore/UgradResearch/TheWrit4all/files/notes/resInstr.pdf. (13th September, 2015).

Grabosky. PN (2001). *Virtual criminality: Old wine in new bottles.* Social and Legal Studies 10(2):243-249.

Gurjar, S., Baggili, I., Breitinger, F., and Fischer, A. (2015). An Empirical Comparison of Widely Adopted Hash Functions in Digital Forensics: Does the Programming Language and Operating System Make a Difference?.

Hasan, S., Abdul Rahman, R., Farah, S., Abdillah, H. B. T., and Omar, N. (2015).*Perception and Awareness of Young Internet Users towards Cybercrime:*

Evidence from Malaysia. Journal of Social Sciences, 11 (4): 395.404 DOI: 10.3844/jssp.2015.395.404.

Holt, T. J., & Bossler, A. M. (2012). Police perceptions of computer crimes in two southeastern cities: An examination from the viewpoint of patrol officers. American Journal of Criminal Justice, 37(3), 396-412.

Humphrey, J. A., and Palmer, S. (2013). Deviant behavior: Patterns, sources, and control. Springer Science and Business Media.

IC3, Internet Crime Complaints Centre. (2017). *Internet Crime Report*. Federal Bureau of Investigations

ITU (International Telecommunication Union) (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

Jacob, J. W., and Lehner, S. (2011). EQUIP2 State-of-the-Art Knowledge in Education: Secondary Education. *Guide to Education Project Design Based on a Comprehensive Literature and Project Review. USAID.*

Jaishankar, K. (Ed.). (2011). *Cyber criminology: exploring internet crimes and criminal behavior*. CRC Press.

Jewkes, Y., and Yar, M. (Eds.). (2013). Handbook of Internet crime. Routledge.

Kabay, M.E. (2008). *A brief history of computer crime.An introduction for students.*School of Graduate Studies Norwich University SA.Available from http://www.mekabay.com/overviews/history.pdf [Accessed 10-03-2014].

Kamara, A, Van, K. B, Magingxa, L. (2001).*Economic viability of small scale irrigation systems in the context of state withdrawal: the Arabie Scheme in the Northern Province of South Africa*. In: Proceedings of the 2nd WARSFA /Waternet Symposium: Integrated water resources management: theory, practices, cases; 2001 October, 30 – 31 October, Cape Town.

Kumar, S., and Ahmad, S. (2008). Meaning, aims and process of education. *School of Open Learning*.

Kumar, K. (2003). *Cyber Laws, International Property and e-commerce Security*. Dominant Publishers and Distributors, New Delhi.

Kwablah, E. (2009). Cybercrime: 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

Lanier, M. M. (2018). *Essential criminology*. Routledge.

Lastowka, F. G., Hunter, D. (2004). *Virtual Crimes.*New York Law School Law Rev. 49:293-316.

Levin, A., Foster, M., West, B., Nicholson, M. J., and Hermandez, T. (2008).*The next digital divide: Online social network privacy.*Privacy and Cybercrime Institute, Ryerson University, Canada.

Longe, O., Ngwa, O., Wada, F., Mbarika, V. and Kvasny, L. (2009).*Criminal Use of Information and Communication Technologies in Sub-Saharan Africa: Trends,*

Concerns and Perspectives, *Journal of Information Technology Impact*, 9, 3, 155-165.

Maat, S. (2004).*Cybercrime: A Comparative Law Analysis (Doctoral thesis)*, University of South Africa, Pretoria, South Africa p.239.

Malekani, A. A. (2018). Access to, use and challenges of ICTs in secondary schools in Tanzania: a study of selected secondary schools in Morogoro Municipality. *Information Impact: Journal of Information and Knowledge Management*, *9*(2), 44-57.

Mann, D. and Sutton, M. (1998).*NETCRIME:More Change in the Organization of Thieving*. Br. J. Criminol. 38(2):201-229.

Ministry of Gender, Children and Social Protection (2018) Children's online safety concerns in Ghana: A position paper on legislative and policy gaps. Retrieved on 24/08/19 from: https://www.unicef.org/ghana/media/1806/file/Child%20Online%20Safety%20Legislation%20and%20Policy%20Gaps.pdf.

Mishna, F., Cook, C., Gadalla, T., Daciuk, J., and Solomon, S. (2010). Cyber bullying behaviors among middle and high school students. *American Journal of Orthopsychiatry*, *80*(3), 362-374.

MoC, [Ministry of Communication]. (2014). *Ghana National Cyber Security Policy and Strategy*. *Ministry of Communication*, Accra; March 2014.

Mohsin, A. (2006). Cyber Crimes and Solutions, Retrieved from http://ezinearticles.com/?Cyber-Crimes-AndSolutions&id=204167

Morelli, M., Bianchi, D., Baiocco, R., Pezzuti, L., and Chirumbolo, A. (2017). Sexting behaviors and cyber pornography addiction among adolescents: The moderating role of alcohol consumption. *Sexuality Research and Social Policy*, *14*(2), 113-121.

Morrison, W. (2013). What is crime? Contrasting definitions and perspectives. *Criminology*, 3-22.

National Council of Educational Research and Training. (2014). Basics in Education; Textbook for B. Ed. Course.

NIBRS, National Incident-Based Reporting System. (2015). UniformCrim Reporting Programme. NIBRS

Neiss, M., Leigland, L., Carlson, N. and Janowsky, J. (2009).*Age differences in perception and awareness of emotion.* J. Neurobiology Aging, 30: 1305-1313. DOI: 10.1016/j.neurobiolaging.2007.11.007.

Ngo, F.T. and Paternoster, R. (2011).*Cybercrime victimisation: An examination of individual and situational level factors.* Int. J. Cyber Criminol., 5: 773-793.

NCSIR, Norton Cyber Security Insights Report. (2016). Key Findings. Available on https://us.norton.com/internetsecurity-emerging-threats-personal-impact-cybercrim.htm. Retrieved on 23rd February, 2018.

Odumesi, J.O. (2006). *Combating the menace of cybercrime: The Nigerian Approach (Project)*.Department of Sociology, University of Abuja, Nigeria p.45.

Okeshola, F. B., & Adeta, A. K. (2013). The nature, causes and consequences of cyber crime in tertiary institutions in Zaria-Kaduna state, Nigeria. *American International Journal of Contemporary Research*, *3*(9), 98-114.

Olaide, M., & Adewole, R. (2011). Cybercrime embarrassing for victims.

Olayemi, O. J. (2014). A socio-technological analysis of cybercrime and cyber security in Nigeria. International Journal of Sociology and Anthropology, 6(3), 116.

Olowu, D. (2009). *Cyber-Crimes and the Boundaries of Domestic Legal Responses: Case for an Inclusionary Framework for Africa.* J. Inform. Law Technol. (JILT), http://go.warwick.ac.uk/jilt/2009_1/olowu.

Oumarou, M. (2007).*Brainstorming advanced fee fraud: 'Faymania' – the Camerounian experience*, in N. Ribadu, I. Lamorde and D. Tukura (Eds), *Current trends in advance fee fraud in West Africa*, EFCC, Nigeria 33–34.

Paluck, E. L., & Cialdini, R. B. (2014). Field research methods. Handbook of research methods in social Science.

Pati, P. (2003). Cybercrime, New Delhi [Online]. Available: http://www.naavi.org/pati/pati_cybercrimes_dec03.htm [Accessed 20 February 2015].

Park, B. Y., Wilson, G., Berger, J., Christman, M., Reina, B., Bishop, F., ... & Doan, A. P. (2016). Is Internet pornography causing sexual dysfunctions? A review with clinical reports. Behavioral Sciences, 6(3), 17.

Pittaro, M., & Schmalleger, F. (Eds.). (2009). *Crimes of the Internet*. Prentice Hall.

Puzzanchera, C. (2010). *Juvenile Arrests (2007)*. DIANE Publishing.

Quarshie, H. O., and Martin-Odoom, A. (2012). Fighting cybercrime in Africa. *Computer Science and Engineering*, *2*(6), 98-100.

Reyns, B. (2010). *Being pursued online: Extent and nature of cyberstalking victimisation from a lifestyle/routine activities perspective.* PhD Dissertation, University of Cincinnati, Ohio, USA.

Reid, S. T. (2015). *Crime and criminology*. Wolters Kluwer Law and Business.

Saini, H., Rao, Y. S., and Panda, T. C. (2012).*Cyber-Crimes and their Impacts: A Review.* International Journal of Engineering Research and Applications (IJERA), ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 2, Mar-Apr 2012, pp.202-209.

Salifu, A. (2008).*Impact of Internet crime on development, Journal of Financial Crime,* 15, 4, 432–444.

Saluja, S., Bansal, D. and Saluja, S. (2012). *Cyber Safety Education in High Schools*. International Conference on Computer Technology and Science (ICCTS 2012) IPCSIT vol. 47 (2012), IACSIT Press, Singapore DOI: 10.7763/IPCSIT.2012.V47.21.

Sarkar, S. (2012). The role of information and communication technology (ICT) in higher education for the 21st century. *Science*, *1*(1), 30-41.

Seltzer, L. F. (2011). *What Distinguishes Erotica from Pornography*. Psychology Today.

Shakarian, J., Gunn, A. T., & Shakarian, P. (2016). Exploring malicious hacker forums. In Cyber Deception (pp. 259-282). Springer, Cham.

Shinder, D.L.(2002).*Scene of the Cybercrime: Computer Forensics Handbook*. Syngress Publishing Inc. 88 Hingham Street, USA.

Smith R. G., Grabosky P. N. and Urbas G. F. (2004).*Cyber criminals on trial*, Cambridge University Press, Cambridge..

Sprecher, R., and Pertl, M. (1988).*Intra-Industry Effects of the MGM Grand Fire*, Quarterly Journal of Business and Economics, 27: 96-16.

Statistics Canada. (2002). *Canadian Community Health Survey Cycle 1*.Mental Health and Well-being.

Stephenson, P., & Gilbert, K. (2013). *Investigating computer-related crime*. CRC Press.

Sutherland, E. (1939).*Principles of Criminology.Fourth edition.*

Sutherland, E. H., Williams, F. P., & McShane, M. D. (2015). Differential association. Edwin Sutherland: On Analyzing Crime.

Taylor, R. W., Fritsch, E. J., & Liederbach, J. (2014). *Digital crime and digital terrorism*. Prentice Hall Press.

Thomas, D., and Loader, B. (2000).*Cybercrime: law enforcement, security and surveillance in the information age.*Routledge, London, J. Soc. Policy 30(1):300.

Titi, K. M. (2003).*Code of ethics, professionalism and responsibilities*.Al-Ahliyyah Amman University, Ardhah, Jordan.

Twumasi, P.A. (2001). *Social research in rural communities (Second edition)*. Ghana Universities Press, Accra.

United Nations Office on Drugs and Crime. (UNODC, 2013). Comprehensive Study on Cybercrime. New York: UN

Vaisu, L., Warren, M., and Mackay, D. (2003). Defining fraud: Issues for organizations from an information systems perspective. *PACIS 2003 Proceedings*, 66.

Wall, D. S. (2015). The Internet as a conduit for criminal activity.

Wall DS (2001).*Maintaining order and law on the internet*. In: Wall, D.S. (Ed.), Crime and the internet. London: Routledge pp.167-183.

Walsham, G. (2012). Are we making a better world with ICTs? Reflections on a future agenda for the IS field. *Journal of Information Technology*, *27*(2), 87-93.

Wang, H.S., Chou, C. H. and Tsai, S. N. (2008).*A preliminary study of the education of internet security implied in a movie based English class in Taiwan's private vocational continuation high school*. CNTE2008, Chichu, Taiwan.

Warner, J. (2011). *Understanding Cyber-Crime in Ghana: A View from Below.* International Journal of Cyber Criminology (IJCC) ISSN: 0974 – 2891 Jan – July 2011, Vol 5 (1): 736–749.

Wolak, J., Mitchell, K., and Finkelhor, D.(2006). *Online victimization of youth: Five years later*.Report # 0706-025, National Centre for Missing and Exploited Children Bulletin, Alexandria, VA.

Yar, M. (2013). Cybercrime and society. Sage.

Yar, M. (2012). Crime, media and the will-to-representation: Reconsidering relationships in the new media age. *Crime, Media, Culture*, *8*(3), 245-260.

Yar, M. (2006). Cybercrime and society. *London: Thousand Oaks*.

Yar, M. (2005).*The Novelty of Cybercrime: An assessment in Light of Routine Activity Theory*.European Journal of Criminology. 2: 407-427.

Zweig, J. M., Yahner, J., Visher, C. A., & Lattimore, P. K. (2015). Using general strain theory to explore the effects of prison victimization experiences on later offending and substance use. *The Prison Journal*, *95*(1), 84-113.

APPENDIX A: QUESTIONNAIRE

UNIVERSITY DEVELOPMENT STUDIES

FACULTY OF INTEGRATED DEVELOPMENT STUDIES

DEPARTMENT OF SOCIAL, POLITICAL AND HISTORICAL STUDIES

My name is Ruhia Abu, a Master of Philosophy in Social Administration student from the University for Development Studies (UDS). The purpose of this survey is to assess cybercrime and its implication on secondary education in the Tamale Metropolis of the Northern Region. In view of this I will be grateful for the completion of this questionnaire. Please answer as frankly as possible, you are assured of confidentiality.

INSTRUCTION: Please thick [√] appropriate box and provide brief answers as possible.

SECTION A: DEMOGRAPHIC CHARACTERISTICS OF RESPONDENT

1. Sex of respondent

a. Male b. Female

2. Age of Respondent

a. 13 – 17 years b. 18 – 22 years c. 23 – 27 years d. 28 years and above

3. Religious affiliation\denomination of respondent

a. Islam b. Christianity c. Other (Specify) ……..

SECTION B: RESPONDENTS AWARENESS OF CYBER CRIME (SAKAWA)

4. Do you know what cybercrime (or sakawa) entails? a. Yes b. No

5. If yes to Q6, what do you know about cybercrime (or sakawa)?

……

……

……

……

6. How often do you hear of people involve in cybercrime (or sakawa activities)?

I. very often ii.Often iii. Not often iv. Never

7. If you have ever heard of people involve in cybercrime (or sakawa activities), what was (or were) this (or these) activities about?

……

……

……

……

……

8. Which of the following places did you know cyber crime (or sakawa) is carried out?

a. Internet café b. Home c. computer lab d. Hotels e. Government Office f. Private office

9. Have you ever accessed the following sites while on the internet?

- Social media a. Yes b. No
- Google search a. Yes b. No
- E-mail a. Yes b. No
- Academic research a. Yes b. No
- Internet phoning a. Yes b. No
- Pornography a. Yes b. No
- Spamming a. Yes b. No
- Piracy a. Yes b. No

RESPONDENT'S VIEW ON THE SOCIAL ATTRIBUTES OF CYBER CRIMINALS OR SAKAWA GUYS

10. What is the age category of most sakawa guys you know?

a. 13 – 17 years b. 18 – 25 years c. 26 – 35 years d. 36 and above years

11. What is the sex of most sakawa guys you know?

a. Male b. Female

12. What is the religion of most sakawa guys you know?

a. Islam b. Christianity c. Traditionalist d. Any religion

13. What is the educational qualification of most sakawa guys you know?

a. Primary b. JHS c. SHS d. Tertiary

14. What is the marital status of the parents of most sakawa guys you know?

a. Never married b. Married c. Divorce d. Separated e. Widowed f. Cohabitation

SECTION C: RESPONDENT'S VIEW ON THE CAUSES OF SAKAWA (CYBER CRIME)

15. Please rank the following by assigning numbers 1, 2, 3,…7 to the items with 1 representing the item that mostly causes sakawa and 7 representing the least cause of all the items.

- Easy access to internet …….
- Weak laws …….
- Peer group influence …….
- Poverty …….
- Unemployment …….
- Defective socialisation …….
- Corruption …….

16. List any other cause(s) of sakawa that you know which is not mentioned in question 4 above (if any).

i. ……

ii. ……..

iii. ……

17. Are there ways by which the causes can be avoided or addressed? a. Yes b. No

18. If yes to Q11, what are some of the ways the causes above can be addressed?

……

……

……

……

SECTION D: RESPONDENT'S VIEW ON HOW CYBER CRIME (SAKAWA) AFFECTS ACADEMIC PERFORMANCE

19. Does cybercrime (or sakawa) has effects on Senior High Students? a. Yes b. No

20. If yes to Q13, what effects does cybercrime (or sakawa) have on Senior High Students?

……

……

……

21. Are there ways by which the effects can be minimized or avoided? a. Yes b. No

22. If yes to Q11, what are some of the ways the effects can be minimized or avoided?

……

……

……

……

Some statements will be made in this section. Please choose one of the five options that follow the statement to indicate the extent to which you agree or disagree with that statement. Please read (or listen) carefully before you choose.

23. Sakawa guys come to school (or class) early.

i. I strongly disagree ii. I disagree iii. I neither agree nor disagree iv. I agree v. I strongly agree

24. Sakawa guys perform poorly in examinations.

i. I strongly disagree ii. I disagree iii. I neither agree nor disagree iv. I agree v. I strongly agree

25. Some sakawa guys stop coming to school.

i. I strongly disagree ii. I disagree iii. I neither agree nor disagree iv. I agree v. I strongly agree

26. Most sakawa guys are school drop outs

i. I strongly disagree ii. I disagree iii. I neither agree nor disagree iv. I agree v. I strongly agree

27. Sakawa guys are punctual at school

i. I strongly disagree ii. I disagree iii. I neither agree nor disagree iv. I agree v. I strongly agree