CENTRE FOR SOCIAL POLICY STUDIES

UNIVERSITY OF GHANA

AN INVESTIGATION OF YOUTH IN CYBERCRIME IN THE AYAWASO EAST CONSTITUENCY OF GREATER ACCRA

BY

NANA OBIRI YEBOAH LEWIS

10508025

THIS DISSERTATION IS SUBMITTED TO THE UNIVERSITY OF GHANA, LEGON, IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE AWARD OF MASTER OF ARTS SOCIAL POLICY STUDIES DEGREE

JULY, 2015

DECLARATION

I hereby declare that this submission is my own work and that it contains no material previously published for an award of any degree in this university of any other university. All references made to other studies have duly been acknowledged.

Nana Obiri Yeboah Lewis

(Candidate)

Signature ……

(Date: ……../ ……. /……)

Dr. George Domfe

(Supervisor)

Signature ……..

(Date: ……../ …..……. /……)

DEDICATION

This dissertation is dedicated to God Almighty, my family members, friends and loved ones

ACKNOWLEDGMENT

I am first and foremost grateful to my supervisor Dr. George Domfe of the Centre for Social Policy Studies, University of Ghana for his invaluable advice, supervision, and encouragement right up to the completion of this project. The Lord God Almighty bless you.

The completion of this work has been made possible also through the support of all other lecturers at the Centre for Social Policy Studies. I am grateful for their support and help.

I am also grateful to Mr. Kwesi Nyantakyi and the entire staff of the Ghana Football Association for their contribution and support.

My final acknowledgement goes to all my family and friends especially my wife, for her wonderful support and to my daughter thank you for holding up for me during times when I was engrossed in my studies and coming home late, thank you.

ABSTRACT

Cybercrime, an offence that is committed against individuals through the internet, has bedevilled the global online industry as well as the reputation of countries. All efforts to combat it has proven futile. The need to investigate it thoroughly and bring about ways of combating it and policing the online space necessitated the study to be conducted. This study investigated the causes, modus operandi, and the state of intelligence of the menace. Methodologically, the study used mixed approach (mix of quantitative and qualitative methods) to sample 111 participants (11 key informants, 60 youths engaged in cybercrime, and 40 community members faced with cybercrime issues) in Ayawaso East Constituency to derive the primary data for the attainment of the study objectives. The findings based on analytical evidence showed that, demographic characteristics of respondents has an influence on cybercrime. In addition, it was established that, employment, computer illiteracy, and moral principles which bears on awareness creation and education on cybercrime help people to restrain from the influencing factors that push others into cybercrime practices. Moreover, the study demonstrated that policing cybercrime is a big challenge for the security agencies as well as the affected communities. Conclusively, cyber-crime presents enormous challenges to society, especially developing societies that are trying to catch-up with the technology revolution, yet are relatively weaker to respond to the challenges of this development. The study recommended partnership, improvement in law enforcement, and adoption of best practices (such as sophisticated ITC technologies) from countries that have been able tackle cybercrime issues to address the menace in Ghana.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AGDoA	Attorney General's Department of Australia
CID	Criminal Investigation Department
GSS	Ghana Statistical Service
GLSS	Ghana Living Standard Survey 6
GNA	Ghana News Agency
HND	Higher National Diploma
ICT	Information and Communication Technologies
ITU	International Telecommunications Union
JHS	Junior High School
MoU	Memorandum of Understanding
SHS	Senior High School
USA	United State of America

CHAPTER ONE

INTRODUCTION

1.1 Background

The penetration of information and communication technologies (ICT) has been on the increase in recent years across Africa (International Telecommunications Union [ITU], 2008; Longe, Ngwa, Wada, Mbarika, & Kvasny, 2009). Although basic access to the internet in most parts of sub-Saharan Africa still depends on public access points such as cybercafés; nations like Nigeria, Cameroon and Ghana have facilities for mobile internet access through satellite connections and fibre optic cables (Longe et al., 2009). This increase in penetration of ICT, especially in West Africa, has spurred on growth in ICT-based businesses and services including electronic government, electronic commerce and electronic banking services. Unfortunately, the growth in the use of ICT has also raised the possibility of new criminal activities (Mbaskei, 2008; Plot, 2010).

The internet has become a double-edged sword providing opportunities for individuals and organisations and also bringing with it an increased information security risk (Magele, 2005). There exists an era of information technology renaissance. Desktop computers, as well as mobile devices such as: laptops, smart phones and tablets that are connected wirelessly, have easy access to corporate networks and information online. All these connectivity have made business environment incredibly efficient.

There is no doubt that internet has changed the way business is conducted. However, this change has come with associated risks, commonly referred to as cybercrime. Cybercrime is a term for any illegal

activity that uses a computer as its primary means of commission (Halder & Aishankar, 2011). Also, the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography, stealing identities, or violating privacy.

Cybercrime, especially through the internet, is usually common among youths. The African Union (AU) defines a "youth" as any person between the ages of 15 and 35 years (Magele, 2005). For the purpose of this research, AU definition is accepted.

In Ghana, unlike the late 1990s were computers were assigned to and used by the rich minority class, today thanks to mass production and rapid rise in cheap second hand computers, many of the youths (whether employed or unemployed) are able to purchase computers at an affordable price tag. Even though few internet service providers have sprung up, provision of internet connectivity in both wireless and cable connection has made the use of computers among the youths very useful but as well problematic. As such, the use of computer to breach laws regarding cybercrime among the youths has been the order of the day.

A latest notable reported case that occurred in Ghana was when Robert Wexler—a U.S. Congressman in Florida was communicated by a Ghanaian young man of age 27 in an attempt to blackmail Robert with information that was pilfered from Robert's rejected internal hard drive that had had its way to Ghana through importation of used computer market (Abugri, 2011, as cited in Warner, 2011). This case is not unique and will never be untill appropriate measures have been adopted to clean up Ghana internet space. The study is part of this effort. It seeks to investigate the activities of the youths engaged in cybercrime in the Ayawaso-East Constituency in order to suggest policies to deal with the menace before it gets out of hand.

1.2 Problem Statement

Cases of online fraud pertaining to credit card crimes, contractual crimes, offering jobs, and advanced fee fraud have been fairly documented (Magele, 2005; Longe et al., 2009). A research conducted by Rivest, Shamir and Adleman (RSA) (2015) in 2014 revealed that the cybercrime trend continues to increase as cybercriminals persistently adopts new efficient technology and profitable attack strategies. A study by Richardson (2008) disclosed that new technologies that cybercriminals capitalize on includes but not limited to system vulnerabilities, ignorance and gullibility on the part of users to perpetrate their heinous crimes. These approaches appear lucrative. Globally, financial losses occasioned by cybercrimes in the United States alone increased dramatically from $52.5 million in 2006 to $67 million in 2007 (ITU, 2007). A study in Australia by the Attorney General's Department of Australia disclosed that the non-governmental cost of cybercrime is about 2 billion dollars annually (Attorney General's Department of Australia [AGDoA], 2013). This means that, as cybercriminals are earning through their acts, there is a huge cost burden not only on individual victims but governments as well. There must be a better way to prevent this cost.

More than ever, the cybercrime trends reported in 2015 by the RSA (2015) demonstrates a terrible trend: cybercrime-as-a-service marketplace progressively and continually to mature; cybercriminals hunt for more bang for the buck and intensify large-scale retail as well as financial attacks; and cybercrime threats continue to widen more targeted and much more advanced. In the year 2014, the RSA AntiFraud Command Center discovered approximately 500,000 cyber-attacks—averagely 11% increase year over year (RSA, 2015). The trend remains progressive because internet connectivity makes it much easier for criminals to act beyond national boundaries when conducting their illegal

affairs. With over 200 countries connected to the internet and still counting, cybercrime has become a global issue that requires a multi-stakeholder effort including governments, the private sector, civic and legal institutions, individuals and other social organizations (Westby, 2003; Broadhurst, 2006) to help maintain the positives of internet as we are all beneficiaries. In this modern world, cybercrimes are within the reach of the youth in most communities, and this is fuelled on by the success of some individuals who are involved in it. This lure of richness, all made possible by just sitting behind a computer for long hours is one possible reason for the increment of cybercrime. One other possible reasons including mass youth unemployment (Reingold, 1999).

Whilst the majority of young people today have access to the internet and computers another major associated issue is the lack of its proper usage. Even worse others do not have access or exposure at all which is now becoming a blessing in disguise. With inadequate supervision, the youth now resort to using the internet as a tool for many vile practices which are unlawful, illegal, fraudulent, harmful may also be connected with immoral activities such as streaming unhealthy videos that could lead the youth into immoral life style. The effect of these unwanted social conducts creates confusion in the economy, a threat to social lives and a hindrance to economic growth (Young Entrepreneurs Sphere, 2012).

Literature is, however, sparse on nation-specific extent of these fraudulent cyber activities as well as nation-specific measures put in place to address them. For instance, Ghana in 2008 was ranked among the top ten for the source of fraudulent cyber activities in the world with Nigeria ranking 3rd in the 2008 Internet Crime Report (ITU, 2009). A study by Warner (2011) also affirmed that, Ghana is now among the topmost ten countries engaged in the practices of cybercrime. This unsavoury distinction

is not something that needs to be entertained. To help the Ghana government counter and contribute to the global war against cybercrime, an empirical investigation into cybercrime practices in Ghana has become necessary.

1.3 Research Questions

The study sought to address the following questions.

1) What are the factors that drive (push and pull) youths into cybercrime?
2) How are the youth engaged in cybercrime practices able to circumvent or protect themselves from the law and police arrest?
3) What is the state of police intelligence and policy development to deal with cybercrime?

1.4 Objectives of the Study

The main objective of the study is to investigate activities of the youths in cybercrime. The following specific objectives were designed to achieve the main objective:

1) To explore the factors that drive (push and/or pull) youths into cybercrime.
2) To examine the experiences of the youths engaged in cybercrime.
3) To examine the state of intelligence and policy development of cybercrime.

1.5 Significance of the Study

There is limited academic work on cybercrime in the developing and emerging economies. Most of the information on cybercrime in these countries are heard or seen from the media. Considering the importance of ICT to the socio-economic advancement of the nation, it is time that many academic exercises were undertaken to provide a comprehensive evidence-based policy to deal with the

problem.

- The findings of the study will shed more light on combating online/internet fraud, as the study explores the security strategies that cybercriminals use to circumvent laws against cybercrime or avoid police arrest.
- The study will lead to a deeper understanding of various types of internet fraud available through an integrative review of dimensions of crimes committed online from a global perspective.
- The findings of the research will serve as decision variables or input for policy makers. As the findings will based on an unadulterated information from people directly engaged in cybercrime. Added to this, the study will make applicable policy recommendations based on the findings that policy-makers can adopt and apply with minimum efforts (cost).
- The study will create more awareness in the minds of its readers, about how vulnerable people can be. Thus stems from the fact that, techniques that cybercriminals use will be made known and the counter measures will as well be available.

1.6 Limitations

The study is limited because, the time required to submit the completed research report is so short that it constrained the researcher in gathering a wider data during his data collection. Moreover, there was difficulty in obtaining the required data since some of the key respondents were too busy and very reluctant to give the answers the research sought to find.

1.7 Organisation

Chapter 1 of this study introduces the background of the study by explaining the two main concepts of the study, youth unemployment and cybercrime. The chapter also discusses the research problem and concludes with the organization of the study. Chapter 2 presents a review of the literature on the association between youth unemployment and cybercrime. Chapter 3 is the methodology and this provides details on the procedures used for data collection and analysis. Chapter 4 contains an analysis of the data and presentation of the discussion of the results. Chapter 5 offers a summary and conclusion of the research findings, implications for practice, and recommendations for policy engagements.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter discusses literature on cybercrime and youth unemployment. It begins with discussions on the theoretical framework. This is followed by discussions on the conceptual framework and recent empirical works on the general causes of crime and its modalities.

2.2 Theoretical framework

The study employs social strain theory to explain how existing societal structures could lead (pull and/or push) people into social vices like crime. Social strain theory appears to suggest that certain strains increase the likelihood of crime. Individuals who experience these strains become upset, and therefore tend to undertake crime as a coping mechanism. Social strain theory was developed by an American Sociologist called Robert K. Merton in the year 1968. The theory emphasizes that social structures may pressure citizens to commit crimes. Strain may be structural, which refers to the processes at the societal level that filter down and affect how the individual perceives his or her needs or be individual, which refers to the frictions and pains experienced by an individual as he or she looks for ways to satisfy individual needs (Merton, 1968). These types of strain can insinuate social structures within society that then put pressure on citizens to become criminals.

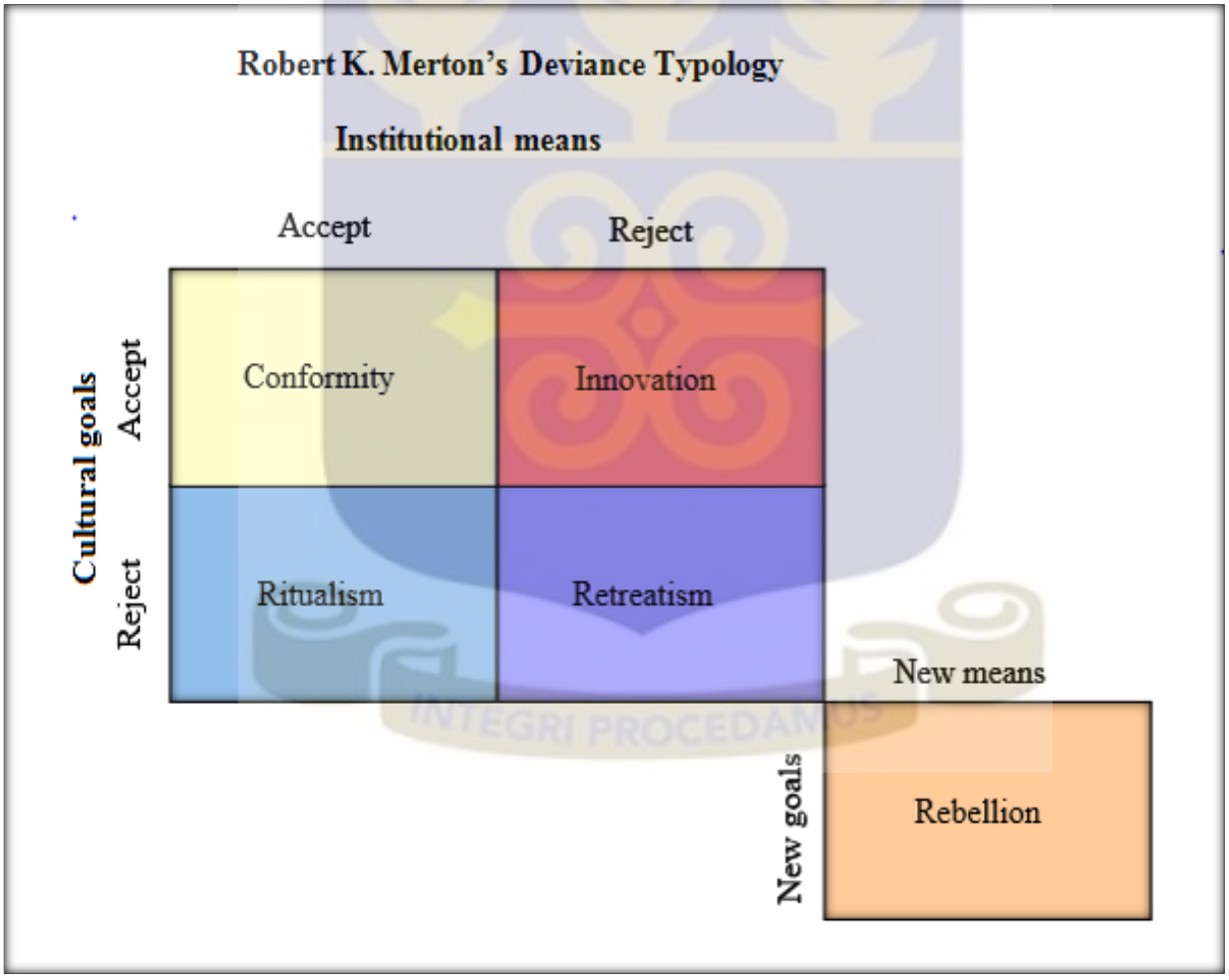
It is the first major strain theory of crime developed in the 1930s. The theory was developed in the midst of the Great Depression, and therefore it mainly focused on that type of strain involving the inability to achieve monetary success. According to Merton, everyone in the United States—

regardless of class position—is encouraged to strive for monetary success (Merton, 1968). At the same time, lower-class individuals are frequently prevented from achieving such success through legal channels (Merton, 1968). In particular, the parents of lower-class children often do not equip them with the skills and attitudes necessary to do well in school. Lower-class individuals often attend inferior schools, and they often lack the funds to obtain college educations or start their own businesses (Boundless, 2015; Halder & Aishankar, 2011). As a consequence, they more often find themselves unable to achieve their monetary goals through legal channels (Choi, 2008). The theory is relevant to the economic situation in the country today. The mentality of the getting rich quickly at all cost has become the order of the day (Choi, 2008; Guillaume, 2009). In his discussion of deviance Merton proposed a typology of deviant behaviour that illustrated the possible discrepancies between culturally defined goals and the institutionalized means available to achieve these goals. A typology is a classification scheme designed to facilitate understanding (Holzer, 1991). In this case, Merton was proposing a typology of deviance based upon two criteria: (1) a person's motivations or his adherence to cultural goals; (2) a person's belief in how to attain his goals. According to Merton, there are five types of deviance based upon these criteria (Merton, 1968).

For example, individuals may assault the peers who harass them (Halder & Aishankar, 2011). Crime also may be used to alleviate negative emotions; for example, individuals may engage in illicit drug use in an effort to make themselves feel better (Choi, 2008). Strain theories are among the dominant explanations of crime, and, as discussed in this chapter, certain strain theories have had a major impact on efforts to control crime. All strain theories acknowledge that most individuals cope with strains in a legal manner (Boundless, 2015; Choi, 2008; Merton, 1968; Guillaume, 2009; Halder & Aishankar,

2011; Holzer, 1991). For example, most individuals cope with monetary problems by doing such things as cutting back on expenses, borrowing money, or working extra hours. It is therefore critical to explain why some individuals engage in criminal coping. After presenting a basic overview of strain theories, this chapter describes how strain theories have been used to explain group differences, such as gender differences, in crime. The chapter concludes with a discussion of the policy implications of strain theories.

Figure 2.1: Social Strain Theory



Source: Adapted from Robert K. Merton Deviance Typology (1938)

- **Conformity**

Conformity involves the acceptance of the cultural goals and means of attaining those goals (Boundless, 2015; Halder & Aishankar, 2011).

- **Innovation**

Innovation involves the acceptance of the goals of a culture but the rejection of the traditional and/or legitimate means of attaining those goals. For example, a member of the Mafia values wealth but employs alternative means of attaining his wealth; in this example, the Mafia member's means would be deviant (Guillaume, 2009; Holzer, 1991).

- **Ritualism**

Ritualism involves the rejection of cultural goals but the normal acceptance of the means for achieving the goals (Choi, 2008; Merton, 1968).

- **Retreatism**

Retreatism involves the rejection of both the cultural goals and the traditional means of achieving those goals (Choi, 2008; Halder & Aishankar, 2011; Holzer, 1991).

- **Rebellion**

Rebellion is a special case wherein the individual rejects both the cultural goals and traditional means of achieving them but actively attempts to replace both elements of the society with different goals and means (Boundless, 2015; Choi, 2008).

Robert Merton published his "Social Structure and Anomie" in 1968. In this article, Merton set forth a theoretical framework for explaining crime rates that differed from the Chicago school criminologists (Merton, 1968). For example, theorists such as Oumarou (2007) and Westby (2003)

held that urban slum areas foster criminal behaviour through the generational transmission of deviant cultural value. Thus, social disorganization theory assumes that the rejection of conventional middle-class values results in high rates of crime in urban slum communities (Holzer, 1991). Merton (1968), on the other hand, argued that it was the rigid adherence to conventional American values that caused high rates of crime and deviance. In essence, he believed that the widespread conformity to American culture in general, and the American obsession with economic success in particular, produced high levels of serious crime (Merton, 1968).

In essence, Merton's work contained a discussion of how culture and social structure could cause high crime rates. Merton (1968) noted that the American culture, as stated above, places economic success at the pinnacle of social desirability. The emphasis on attaining economic success, however, is not matched by a concurrent normative emphasis on what "means" are legitimate for reaching the desired "goal" (Choi, 2008; Merton, 1968). This problem is then exacerbated by the social structural component discussed by Merton, which highlights the structural barriers that limit individuals' access to the legitimate means for attaining the goal of economic success (Lipsey & Chrystal, 2007; Merton, 1968). This disjunction between culturally ascribed goals (that is economic success) and the availability of legitimate means to attain such goals (that is social structural limits) in turn puts pressure on the cultural norms that guide what means should be used to achieve the culturally prescribed goal (Lipsey & Chrystal, 2007).

Merton (1968) referred to this weakening of cultural norms as "anomie." His adoption of the term "anomie" is based on Durkheim's (1915) reference to the weakening of the normative order in society, or, put differently, how institutionalized social norms may lose their ability to regulate individuals'

behaviour. In particular, Merton (1968) noted that institutionalized norms will weaken, and anomie will set in, in societies that place an intense value on economic success. When this occurs, the pursuit of success is no longer guided by normative standards of right and wrong. Rather, Merton (1968) noted, "the sole significant question becomes: Which of the available procedures is most efficient in netting the culturally approved value?"

Merton was careful to note that there were a number of ways in which individuals may adapt to the "strains" brought on by the inability to secure pecuniary success, and not all of these adaptations are deviant (Merton, 1968). In his famous typology, Merton (1968) proposed that there were a number of adaptations possible in response to social systems that have anomie and blocked opportunities. These adaptations are: innovation, in which the goals are pursued but legitimate means are eliminated and illegitimate means are used; ritualism, in which the goals are abandoned but the legitimate means are pursued; retreatism, in which the goals are abandoned as well as the means; and rebellion, in which the social structure – both goals and means – is rejected and a new structure is advocated (Agnew, 1992; Merton, 1968). A fifth adaptation is conformity, in which the goals are accepted and pursued, along with the legitimate means (Durkheim, 1915). Although Merton failed to articulate what factors determine which deviant adaptations will be adopted (as he acknowledges in his 1968 article); his theory predicts that rates of deviance will be greater when the level of anomie is higher and when the extent of blocked opportunities is greater (Merton, 1968). Conversely, conformity will be common in social systems when goals and legitimate means are clearly articulated and promoted and when opportunities are equal across individuals and social groups (Durkheim, 1915).

Relating to the Social Structure Theory is the Institutional Anomie Theory.

In Boundless' (2015) Strain Theory, Merton's Anomie Strain Theory was extended and partially reformulated. Although Morgan and Kreuger (1993) agreed with Merton's view of American culture, they found his analysis of social structure incomplete. Rather than focusing solely on the limitations of the economic structure as the primary source of structural pressure to innovate (that is commit crime), Morgan and Kreuger's (1993) analysis centres on the criminogenic influence of a variety of social institutions in American society. Drawing heavily on Marxist theory, they argue that the cultural penchant for pecuniary rewards is so all-encompassing that the major social institutions (that is, the polity, religion, education, and the family) lose their ability to regulate passions and behaviour. Instead of promoting other social goals, these institutions primarily support the quest for material success (that is, the American dream) (Morgan & Kreuger, 1993). For example, Boundless (2105) and Sharma (2007) contend that "education is regarded largely as a means to occupational attainment, which in turn is valued primarily insofar as it promises economic rewards".

In short, to the extent that social institutions are subservient to the economic structure, they fail to provide alternative definitions of self-worth and achievement that could serve as countervailing forces against the anomic pressures of the American dream. To summarize, Merton's institutional anomie theory holds that culturally produced pressures to secure monetary rewards, coupled with weak controls from non-economic social institutions, promote high rates of instrumental criminal activity (Merton, 1968).

The majority of studies that have empirically tested institutional anomie theory have employed property and violent crime as dependent measures. Following is an examination of the empirical

findings of studies that have investigated institutional anomie theory.

General Strain Theory

Agnew's (1992) general strain theory posits that strain leads to negative emotions, which may lead to a number of outcomes, including delinquency. The specific strains discussed in the theory include the failure to achieve positively valued goals (e.g., money or status), the removal of positively valued stimuli (e.g., loss of a valued possession), and the presentation of negatively valued stimuli (e.g., physical abuse). While many specific types of strain may fall into these categories, Agnew has attempted to specify the conditions under which strain may lead to crime. Strains that are 1) seen as unjust, 2) high in magnitude 3) associated with low social control, and 4) create some incentive to engage in criminal coping are most likely to lead to violence and delinquency (Agnew, 1992).

According to the general strain theory, individuals experiencing strain may develop negative emotions, including anger, when they see adversity as imposed by others, resentment when they perceive unjust treatment by others, and depression or anxiety when they blame themselves for the stressful consequence (Agnew, 1992). These negative emotions, in turn, necessitate coping responses as a way to relieve internal pressure (Boundless, 2015). Responses to strain may be behavioural, cognitive, or emotional, and not all responses are delinquent (Agnew, 1992). General strain theory, however, is particularly interested in delinquent adaptations. General strain theory identifies various types of delinquent adaptations, including escapist (e.g., drug use), instrumental (e.g., property offences), and retaliatory (e.g., violent offences) outcomes. Coping via illegal behaviour and violence may be especially true for adolescents because of their limited legitimate coping resources, greater influence from peers, and inability to escape many stressful and frustrating environments (Boundless,

2015).

General strain theory has attempted to specify the factors which increase the likelihood that individuals will cope with strain by committing crime. Sharma (2007) contends that crime becomes a likely outcome when individuals have a low tolerance for strain, when they have poor coping skills and resources, when they have few conventional social supports, when they perceive that the costs of committing crime is low, and when they are disposed to committing crime because of factors such as low self-control, negative emotionality, or their learning history. Empirical research has offered some support for the above. Holzer (1991), for example, found that individuals with the personality traits of negative emotionality and low constraint were more likely to respond to strain with crime. Such individuals are impulsive, overly active and quick to lose their tempers.

2.3 Conceptual Framework

The conceptual framework of the study includes the various concepts of the study and the interrelationship among them. Since concepts are abstraction or generalization from experience or the result of transformation of existing concepts, the conceptual framework seeks to illustrate how the concepts work in a real world.

2.3.1 The concept of cybercrime

The internet has offered a huge platform for useful research purposes. However, cybercrime is a worldwide problem that is costing countries billions of dollars. According to the ITU (2007), as early as 2003 the United States was already leading the world in percentage of cyber-attacks at 35.4 percent, followed by South Korea at 12.8 percent. Countries with high rates of computer piracy, such as Russia, have reacted slowly to cybercrime (Plot, 2010). As a result, many hackers and other cyber criminals

can flourish in countries with few internet crime laws while attacking richer countries through their computer because it lacks rules and codes of a central authority which governs it as such internet has no geographical demarcation as remarked by (Guillaume, 2009).

Cybercrimes simply put are crimes that are committed using the computers and networks (Oumarou, 2007). There are several types of cybercrimes some of which include; cyber terrorism, fraud-identity theft, drug trafficking deals, malware, cyber stalking, spamming, logic bombs and password sniffing (Plot, 2010).

Urbanization is one of the causes of cybercrime in Ghana; it is the massive movement of people from rural settlements to cities (Meke, 2012). According to Meke (2012), urbanization is considered as the massive physical increment in urban polutation mainly due to rural migrants in quest for a prosperous life. This result in a heavy competition amongst the growing populace more especially the elites, as such the elites find it lucrative to invest in the crime of cyber because it is a business that requires less capital to invest and they are popularly called "Yahoo Boys" (Oumarou, 2007). In his article "Urbanization and cybercrime in Nigeria" Meke (2012) reiterated urbanization as one of the major causes of cybercrime in Nigeria and Urbanization will be beneficial if and only if good jobs can be created in the cities where population growth is increasing, in his article, he emphasized that urbanization without crime is really impossible. As such the elites amongst them find it lucrative to invest in the cybercrime because it is a business that requires less capital (Oumarou, 2007).

Cybercrime can be associated with high rate of unemployment, harsh economic conditions, and poor educational system (Zenou, 2000). There is an adage that says "an idle mind is the devils workshop", as such most of our youth will use their time and knowledge as a platform for their criminal activity,

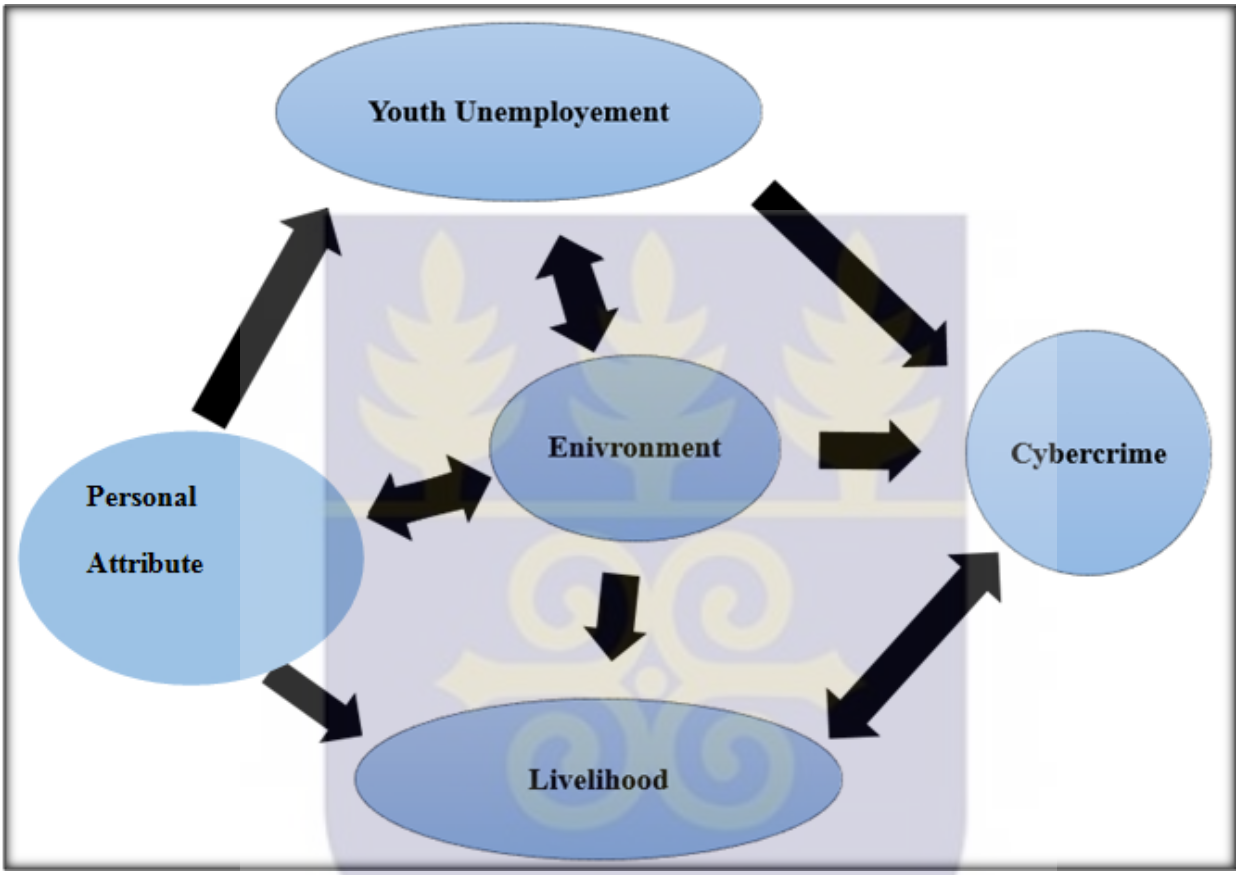
in order to improve their livelihood and to make ends meet (Anah, Funmi, & Makinde, 2012).

Another cause of cybercrime is the quest for wealth (Zenou, 2000); there exist a large gap between the rich and the average, as such many strive to level up using the quickest means possible, since for any business to thrive well, the rate of return in the investment must be growing at a geometric rate with a minimal risk (Lipsey & Chrystal, 2007). Most cyber criminals require less investment and a conducive environment. Ghana is such an environment and many cyber criminals take advantage of that (Anah et al., 2012).

The Ghanaian legislation must implement strict laws regarding cyber criminals and when criminal offences occur, perpetrators must be punished for the crime they have committed because cybercrimes reduces the nation's competitive edge for failure to prosecute, cyber criminals can take advantage of the weak gaps in the existing penal proceedings (Boateng, 2002). Weak or fragile laws regarding cyber criminals exist in Ghana, unlike in the real world where criminals such as armed robbers are treated with maximum penalties (Boateng, 2002). Unfortunately, the nation is not well equipped with sophisticated hardware to track down the virtual forensic criminals (Broadhurst, 2006). Laura (2012) states that "African countries have been criticized for dealing inadequately with cybercrime as their law enforcement agencies are inadequately equipped in terms of personnel, intelligence and infrastructure, and the private sector is also lagging behind in curbing cybercrime". Ghana is not an exception to this rule. Furthermore, it is therefore paramount that the nation's legislation should ensure proper implementation of their laws against cybercrime (Boateng, 2002).

2.3.2 Interrelationship amongst the concepts

Figure 2.2: Interrelationship amongst the Concept of Cybercrime and its Influential Factors



Source: Author's Own Creation, 2015

2.4 Empirical Literature

It seeks to provide evidence on the various phenomena being explored by recent studies to explain the causes of cybercrime. Cybercrime is one of the words frequently used by individuals in our contemporary society (ITU, 2007). To understand the true meaning of cybercrime, there is the need to understand the split meaning of Cyber and Crime. The term "Cyber" is a prefix used to describe an

idea as part of the computer and Information age and "Crime" can be described as any activity that contravenes legal procedure mostly performed by individuals with a criminal motive (Anah, Funmi, & Makinde, 2012). Cybercrimes are defined as: "Offences that are committed against individuals or groups 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 (Chat rooms, emails, noticeboards and groups) and mobile phones" (Halder & Aishankar, 2011). Such crimes may threaten a nation's security and financial health (Hansell, 2007). Thus, cybercrime can simply be explained as crimes carried out with the aid of a computer system (Plot, 2010).

From the perspective of ICT for development, it is not misplaced to say that cybercrime portends some dangers and have the potential to stall the developmental contributions accruable from a well-harnessed ICT adoption, spread and usage in sub-Saharan Africa (Longe et al., 2009). Cyber fraud has a potential to widen the digital divide, crumble the information infrastructure and affect consumer confidence in online transactions (Salifu, 2008; Longe et al., 2009; Oumarou, 2007).

In some countries in West Africa, cyber-crimes are performed by people of all ages ranging from young to old, but in most instances the young (Sharma 2007; Zenou, 2000). Several youths engage in cyber-crime with the aim of emerging as the best hacker, or as a profit making venture since the tools for hacking in our modern world has become affordable by many ("Young Entrepreneurs Sphere," 2012). Mbaskei (2008), in his publication on "Cybercrimes: Effect on Youth Development" noted that secret agents of the United Parcel Service (UPS) smashed a record scam with a face value of $2.1billion (about N252 billion) in Lagos. The interception was done within three months. Some of

the instruments uncovered by the UPS were documents like Wal–Mart Money orders, Bank of America cheques, U.S postal service cheques and American Express travellers' cheques. This record scam is made possible as a result of the large number of young people who now see Cybercrimes or internet fraud as a source of livelihood (Mbaskei, 2008).

Youth unemployment describes persons within a specified age bracket who are unemployed (Zenou, 2000). As mentioned in section 2, according to the international standard definition of unemployment (13th ICLS 1982), the "unemployed" comprise all persons above the age specified for measuring the economically active population who, during the reference period, satisfy the following three conditions simultaneously:

a. "without work": that is, not in paid employment or self-employment, as specified by the international definition of employment;
b. "currently available for work": that is, available for paid employment or self-employment during the reference period (or shortly after); and
c. "seeking work": that is, had taken specific steps in a specified recent period (typically the last four weeks) to seek paid employment or self-employment (Zenou, 2000).

2.4.1 Characteristics of cybercriminals

Most literature works on cybercrime contend that, the demographics of people engaged in cybercrime is the same everywhere cybercrime is perpetrated. A research study by the AGDoA (2013) demonstrated that, over 75% of the cybercriminals perpetrating fraud and other internet crimes in Australia are males and more than half are residing in urban centers like California, New York, Florida, Illinois, Texas, Georgia, and Pennsylvania, and these centers are among the most populated

cities. Similarly, a study by Okeshola and Adeta (2013) in Zaria with 400 participants illustrated that, an extreme proportion (89%) of cybercriminals were males, of which 88% were within the ages of 18 and 30 years. Again, their study pointed out that 60% of cybercriminals were university graduates, and most (60.5%) were married couples (Okeshola & Adeta, 2013).

2.4.2 Cybercrime in Ghana

The use of the internet in Ghana has also seen a significant increase since the liberalization of the telecommunication industry in the 1990s (ITU, 2008). The country had 43 Internet users per 1,000 people in 2008 as compared to 1 Internet user in 1999 (ITU, 2008). The number of PC ownership doubled to 52 owners per 1,000 people between 1999 and 2005 (ITU, 2007).

Until 1990 Ghana had no record in the cybercrime books. In today's world, Ghana is not exempted from the literature works on cybercrime. A "broad overview of the rise and practice of cybercrime in Ghana" by Warner (2011) disclosed that Ghana gained unsavoury record alongside Cameroon and Nigeria as among the top ten cybercrime producing states. Historically, the term and practices of cybercrime in Ghana begun early 1990s and became intensive in the late 2000s where second hand computers proliferated the electronic market in country. Warner (2011) confirmed in his study that, in Ghana the term cybercrime is relatively something new, which came to rise within the period of 1990 and 2000. During this period, credit card was the only crime activity existing online but now it has extended; its practice is widespread and on an international level. With its widespread, the practice of cybercrime in Ghana according to Warner (2011) is observably to be in three dimensions. The first and most common among cybercriminals is that they will contact the Westerners either through social networking websites like Twitter, Facebook, and Tango or through internet dating sites like porn.com,

mylove.com et cetera, with their main targets being Americans and British under false identity (Ghana News Agency, 2009; Warner, 2011). This is what is called according to Warner (2011) "Romance Fraud". The second kind, is termed "Fold Coat", which follows the same false identification strategy but through a fake gold dealings, whereby Westerners will be contacted online with agreements to fly to Ghana with the aim of surveying investment-potential gold mining concessions. After all agreements have been made and documents validated through inappropriate means and connivance, scammers will sit at hotels where the Westerners visited then process all information and documentation online, this gives them (Westerners) the hope of investment returns but at the last hour, when all payment have been made, the Ghanaians (scammers) will inform the Westerners that they will return the next day but will never come back again. The third and the last genre of cybercrime is the indigenous estate fraud where the victims are natives of Ghana but living in diaspora. This kind of cybercrime occurs as Ghanaians living in abroad find it difficult to return to Ghana until retirement, hence consult local people for their real estate accomplishments. This particular crime occurs when scammers (cybercriminals) online contact Ghanaians residing in diaspora to assist them build their houses or as agents to cater for their real estates. Most reported cases concerning this type of crime shows that in the long run these so called agents run away with moneys being sent to them from diaspora for the construction of the estates.

Not different from other cybercriminals, most of the Ghanaians engaged in cybercrime are males. Warner (2011) in his study estimated 90% as males (men) involved in the practices of cybercrime in Ghana and below 30 years. Of this category, Abugri (2011) disclosed that, most of them reside in the capital towns like Accra, Takoradi and Kumasi, where internet service or café is accessible and

affordable. Abugri (2011) added that, most of these people are perfectly located in slums like Nima, Maamobi, Accra New Town and Mallam Atta. Evidence by the Ghana News Agency (GNA) (2009) is that most of cybercriminals in Ghana are either underemployed or unemployed.

With regards to the state of intelligence and policy development in deterring people from engaging in cybercrime, much effort has been made but yet real action is minimal. The Ghanaian Government has made concerted efforts to create a 'knowledge-based economy' thereby making Ghana an ICT –driven economy (Longe et al., 2009). The Ghana Government having recognized the need to make the country gain its popularity and peace in favourable terms to attract and retain investors, the Ministry of Communication, has begun executing stringent measures to combat cybercrime as it poses an increasing threats to individuals as well as the country's security apparatus (Warner, 2011). In speech delivered by the Minister of Communication (Mr. Haruna Iddrisu) in 2009, he explained that the Ghana government has set up an emergency Cyber Crime Response Team, to review existing legislature that governs the information communication and technology (ICT) programmes and activities as a suitable means to strengthen the country's cyber security (GNA, 2009).

Mr. Iddrisu in his speech called upon the criminal investigation department (CID) to strengthen the capacity of the e-Crime Department of the Ghana security agency in an effort to curtail cybercrime in Ghana (GNA, 2009). This according to the CID Headquarters (2012), the CID of the Ghana police service has signed a memorandum of understanding (MoU) with the e-Crime Bureau Incorporation in Accra to strengthen the capacity of the CID within the arena of e-Crime and cyber intelligence monitoring and gathering. Thus, the Ghana Police Service, do not have the capacity and mechanism to track and kick-out those engaged in the cybercrime practices ("CID Headquarters," 2012). Warner

(2011) disclosed that till the year 2008, Ghana had no laws specifically governing cybercrime practices hence the police service handled (treated) cybercriminals as if they were just defrauders. He added that in 2008, the government of Ghana, passed an Electronic Transaction Act (Act 772) even though the Act purposely aimed at criminalizing cybercrime and as well resultantly empower the police service to prosecute suspected criminals, the government still worries as the future of the cybercrime are no more computer based rather cell-phone based (Warner, 2011). The fact still remains that, Ghana does not have a strong existing laws and fully developed capacity to combat cybercrime among the youths.

2.5 Causes of Cybercrime

People work because of several reasons. So many people perpetrate because of many reasons. Every decisions and/or action of humans has a reason. People are into cybercrime because of the reasons discussed below:

- Attitudinal and Choice

As an omnipotent being, humans have a choice to do or not to do. According to Okeshola and Adeta (2013), people engage in crime because of their decision or willingness to do and this is based on the attitude of the person. People with good moral principles (attitude) do not involve themselves in criminalities and vice versa. Shehu (2014) explained that, the motivation for people to commit crime or act criminally is determined by the free will (choice) of those people.

- Urbanization

Recent rate of urbanization is high. Simply because, rural migrants are increasing. This has led to the increasing number of urban residents posing lots of deviant activities. Hassan, Lass, and Makinde

(2012) in Nigeria, identified urbanization as one of the causes of cybercrime. They claimed urbanization without crime is impossible because an increasing rate of urban population brings about tight competition in search of a better living and as such one of the lucrative and potential sector to better living is where the elites invest—cybercrime.

- Unemployment

Youths not engaged in any economic activity pose a threats to that economy, as the adage goes, "The devil always find the work for an idle man". Scholars like Hassan et al. (2012), Okeshola and Adeta (2013), Warner (2011), and Reingold (1999) opined that high rate of unemployment brings about lots of criminal activities, including cybercrime.

- Get-Rich-Quick Attitude (Quest for Money/Financial Gains)

The eagerness and aggressiveness to get money within the shortest time motivates people into cybercrime. A study by Shehu (2014) disclosed that, many poor people make it possible to level up the lager gap between the rich and the poor through cybercrime. The ITU (2007) reported that, people perpetrate cybercrime because it provides them the enabling environment to make rich quicker.

- Poverty

Poverty seems to be everywhere there is a problem. Evidence provided by Magele (2005) in South Africa, and Meke (2012) revealed that, poor people are more into cybercrime than the rich people. Adding to this, Sharma (2007), believed and asserted that, there is a direct correlation between poverty and crime, simply because poor people are more likely to commite crime than rich people.

- Fame (Societal Recognition)

The advocates of social strain theory hold that societal structures also motivates people to commit crime. This is not different from what Hassan et al. (2012) articulated that, people want to be

recognized in society by displaying their wealth. Similarly, Zenou (2000) identified fame to be among the major cause of cybercrime. He explained that, some societies acknowledge people who have money and extravagant properties and this motivates people to engage in cybercrime practices. With regards to fame, Warner (2011) explained that, for people (especially peers) to prove to their colleagues that they are capable of hacking or breaking codes, most of the youths are gingered to engage in these cyber criminalities.

- Fragile Cybercrime Laws (Feeble Institutional Framework)

Longe and Chiemeke (2006) and AGDoA (2013) mentioned that, the continual act of committing internet crime by people is because of existence of weak institutional structures to track and capture cybercriminals and poor defined laws guiding cybercrime. According to Hansell (2007) and Ani (2011), this motivates people to disregard the consequential results of perpertrating crime online. Okeshola and Adeta (2013) hold that, cybercrime exist everywhere there is weak cybercrime laws.

- Parenting

Even though people make the decision to enter into cybercrime practices, Okeshola and Adeta (2013) and Shehu (2014) believe lack of good moral upbringing from guardians and parents promotes or redefine the attitude of children negatively which most often leads to juvenile delinquencies. According to Meke (2012), many parents in today's world transfer crime values to their children through socialization. Okeshola and Adeta (2013) added that, parents of today have neglected their rightful and parental duties which has made most children irresponsible.

- Easiness to Perpetrate

Advanced knowledge in ICT and its affordability, according to Shehu (2014) makes people indulge in cybercrime. Hassan, et al., (2012) added that, in Nigeria, because of the influx of second hand

computers, and availability of modems or wireless networks, the practice of committing crime online is cheap and simple.

- Laziness

Because perpetrating crime on the net is easy and cheap (simple), many lazy people are into it. Evidence is based on what Oumarou (2007) unfolded in his study that, most of the people engaged in cybercrime are economically active people but are neither seeking or willing to work. This is what Okeshola and Adeta (2013) explained that, internet has made it simple and easy; one has to sit in his/her comfortable zone to perpetrate.

2.6 Conclusion

This research thus, sought to establish an association between labour slack and the upsurge of cybercriminal activities, particularly internet fraud.

CHAPTER THREE

METHODOLOGY

3.1 Introduction

This chapter discusses the various methods employed to answer the research questions. It describes the geographical area where the study was conducted, the study design the population and the sample.

3.2 Research Design

The design of the study is very relevant in carrying out the entire research activities and in quest for answers to the research questions. It is basically the framework created to attain what the study was meant to achieve. The framework that the study employed is that of case study and descriptive survey. Together, it is a descriptive case study design. According to Pickard (2007), a descriptive case study is one that is focused and detailed, in which propositions and questions about a phenomenon are carefully scrutinized and articulated at the outset. It helps to specify the boundaries of the case, and it contributes significantly to the rigor of the finished case study.

The basis for adoption of descriptive case study design is the fact that the study strives to explore an increasingly recurring socio-economic problem within its real life context to gather in-depth empirical facts and reports them as they unfold. And this design comparing to experimental and correlation designs, deals exactly so hence the most appropriate.

Moreover, a case study allows for "empirical investigations of a particular contemporary phenomenon within a real life context, using multiple sources of evidence" such as questionnaires, interviews and documentary analysis (Boateng, 2014).

3.3 Research Setting

The study was conducted at Ayawaso East Constituency of the Greater Accra Region. It has an average population size of 400,000. It consists of five (5) electoral areas Kanda, Nima West, Mamobi East, Mamobi West and Kwao Tsuru. The main economic activity of this area is trading. The area is largely dominated by youths with many having attained education up to the junior high school level. Most school dropouts tend to menial jobs to support their families and for survival.

Ayawaso East Constituency was selected because the people and the constituency in totality has been clouded as a crime prone area with high occurrence of all manner of crimes including cybercrime. In addition, numerous press reports have made reference to allegations that some towns like Nima, Mamobi, and Kanda shelter most criminals that are engaged in cybercrime activities. Moreover, the setting is in close proximity to the researcher hence transportation cost during field survey was minimised.

3.4 Research Approach (Method)

This presents all the methods (approaches) that were used to achieve the purpose of the study. According to Boateng (2014), researchers have the option of making a choice between three research approaches, namely qualitative, quantitative and mixed method. In the case of this study, the phenomenon under investigation is social in nature, very sensitive considering its criminality and as well involves multiple humans, hence a mixed method approach involving both quantitative and qualitative methods preferably was the best choice. Each method has unique characteristics hence combining the various methods makes it appropriate in dealing with different situations of this nature of phenomenon.

Burns and Grove (1993) define quantitative approach as formal, objective and systematic process to describe and test relationships and interactions among variables. A questionnaire administration was the main technique for the quantitative method. According to De Vaus (2002), "a questionnaire is used to collect original data for information from a sample." A questionnaire administration became relevant for the study because the target population was too large to be covered. In this study, the information was collected through self-administered questionnaires distributed personally to the subjects (respondents) by the researcher.

A questionnaire administration was used because it provides a quantifiable data that brings to bear an accurate account of the characteristics, for example behaviour, opinions, abilities, beliefs, and knowledge of a particular individual, situation or group. This method was chosen to meet the objectives of the study, namely to determine the extent to which labour slack plays a hand in the increase of cybercrime within the Ayawaso–East Constituency (Burns & Grove, 1993).

Qualitative is the other approach of the mixed method. Qualitative method involves measuring data which is usually related to human actions and the grounds behind them. The method is mostly used in behavioural sciences (De Vaus, 2002) and is centered on non-numeric (qualitative) data. Qualitative data cannot be quantified and measured in relation to a quantity. In other words, thus, qualitative research is inefficient when it comes to identifying, measuring or quantifying a single statistic (Pickard, 2007). However, an advantage of this research technique is the ability to examine given phenomena with respect to multiple human perspectives (De Vaus, 2002). The free nature of research allows a more rich input that might contribute to a more specific learning outcome (Pickard, 2007).

Qualitative method is more appropriate for human oriented study research. Lack of numeric scoring

allows freedom of choice on both questions and answers, and can offer a great input of knowledge to the study. A great disadvantage in comparison with quantitative approach however, is that the data cannot always be quantified. In this study the information was collected through face to face interviews, which was done personally by the researcher. Then, a focus group method was followed. A focus group discussion was used to collect the qualitative data. This technique is a form of qualitative approach in which a group of people are asked about their opinions, beliefs, and attitudes towards a product, service concept, advertisement, idea or packaging. In executing this technique, questions are asked in an interactive group setting where participations are allowed to freely talk and with other group members (Morgan & Kreuger, 1993).

Expert interviews was used to collect the qualitative data. Expert interview is a form of qualitative method in which a key informants are asked about their perceptions, opinions, beliefs, and attitudes towards a product, service, concept, advertisement, idea, or packaging. Questions are asked in an interactive group setting where participants are free to talk with other group members (Morgan & Kreuger 1993).

The main purpose of conducting an expert interview is to draw upon respondents' attitudes, feelings, beliefs, experiences and reactions in a way in which would not be feasible using other methods, for example observation, one-to-one interviewing, or questionnaire surveys. These attitudes, feelings and beliefs may be partially independent of a group or its social setting, but are more likely to be revealed via the social gathering and the interaction which being in a focus group entails. Compared to individual interviews, which aim to obtain individual attitudes, beliefs and feelings, focus groups elicit a multiplicity of views and emotional processes within a group context. The individual interview is

easier for the researcher to control than a focus group in which participants may take the initiative. Compared to observation, a focus group enables the researcher to gain a larger amount of information in a shorter period of time. Observational methods tend to depend on waiting for things to happen, whereas the researcher follows an interview guide in a focus group. In this sense focus groups are not natural but organised events. Focus groups are particularly useful when there are power differences between the participants and decision-makers or professionals, when the everyday use of language and culture of particular groups is of interest, and when one wants to explore the degree of consensus on a given topic (Morgan & Kreuger 1993).

3.4.1 The Study Population and Sample

According to Burns and Grove (1993:779), a study population is defined as all elements (individuals, objects and events) that meet the sample criteria for inclusion in a study. The study population is the entire Ayawaso East Constituency members and that consist the youths, the aged, commuters, natives, and non-natives.

Mouton (1996:132) defines a sample as elements selected with the intention of finding out something about the total population from which they are taken. A sample of 111 participants were selected from the Constituency for interviews through multistage sampling technique. The sample included 100 respondents (youths who are cybercrime culprits and those who are not) and 11 interviewees (parents, opinion leaders and professionals). Available subjects were entered into the study until the total sample size of 111 was reached. Respondents who met the sample criteria were identified by the researcher at the Ayawaso East Constituency, to participate in the research.

3.4.2 The sampling criteria

The 100 respondents (youths) had to meet the following criteria to be included in the sample.

a. be mentally sound in order to consent to participation

b. be willing to participate

c. be 15 years or older and below 35 years

d. obtain the consent of parents/guardians to participate if they are less than 18 years of age

e. be of either sex or any race

3.4.3 Sampling Technique

As a result of the complex and sensitivity of issues bothering on criminality, the study adopted multiple (multistage) sampling techniques in selecting 111 participants for the survey. These approaches were cluster sampling to select clusters (electoral areas), quota sampling technique to select 11 key informants (interviewees), snowball to select 60 respondents (youths) who have ever been involved in cybercrime and systematic random sampling to select 40 respondents (youths) not have ever been engaged in cybercrime from the chosen clusters.

The constituency is naturally divided into five electoral areas. Therefore, in applying the cluster sampling technique, the study considered each electoral area as a cluster. Names of these clusters were written on pieces of papers and placed in a dark container. A ten year old boy was asked to pick two pieces randomly and it came out that Nima and Mamobi electoral area were selected after which 50 respondents (30 ever involved and 20 never involved in cybercrime) were interviewed in each

electoral area. Because of the criminality nature and the fear of being arrested for crime, it was necessary that a non-probability approach of sampling was deployed in selecting 60 youths, above the age of 15 years and below 35 years, who have each been involved in cybercrime. A snowball approach was used in tracking 60 respondents who have ever been involved in cybercrime in the two clusters. A rapport developed with them encouraged them to lead us to interview more cybercrime culprits.

A systematic random sampling approach was then used to interview 40 respondents (individuals) who have never been engaged in the practices of cybercrime and with ages within 15 and 35 years. On the day of interviewing these 40 respondents, in entering the cluster, any youth in the first house who was ready to be interviewed was included in the sample. After this, 40th more houses were skipped and in the next 42st house any youth available and ready to be interviewed was considered. If the respondent refused, the youth in the next available house was considered. About, to such respondents were interviewed each day until the total of 30 were interviewed in each cluster.

In the case of qualitative interviews, a quota sampling technique was used to select one Cybercrime expert from Cybercrime Unit of Ghana Police Service, two leaders of youth association in each cluster, two opinion leaders (Assemblymen) in each selected cluster, and one religious leader in each cluster for expert interviews. In all, eleven (11) interviewees (key informants) were selected for in-depth interview.

3.4.4 Data collection Processes

3.4.4.1 Data collection instrument

A questionnaire employed as a data collection instrument. A questionnaire is a printed self-report form

designed to elicit information that can be obtained through the written responses of the subjects Grove 1993).

Questionnaires as an instrument of data collected was used for the following reasons.

a. They ensured a high response rate as the questionnaires will be distributed to respondents to complete and will be collected personally by the researcher.

b. They required less time and energy to administer.

c. They offered the possibility of anonymity because subjects' names will not be required on the completed questionnaires.

d. There was opportunity for bias as they were presented in a consistent manner.

Most of the questions were closed-ended, which made it easier to compare the responses of respondents. Apart from the advantages that have been listed above, questionnaires have weaknesses. For example, there is the question of validity and accuracy (Burns & Grove 1993). The subjects might not reflect their true opinions but might answer what they think will please the researcher, and valuable information may be lost as answers are usually brief. Further probing were used during the interviews to minimise this weakness.

The respondents were assured that their identity would never be exposed during analysis. This provided atmosphere for them to be truthful.

3.4.5 Reliability and Validity

3.4.5.1 Reliability

Polit and Hungler (1993) referred to reliability as the degree of consistency with which an instrument measures the attribute it is designed to measure. The questionnaires which were answered revealed consistency in responses. Reliability can also be ensured by minimising sources of measurement error like data collector bias. Data collector bias was minimised by the researcher being the only one to administer the questionnaires, and standardizing conditions such as exhibiting similar personal attributes to all respondents, e.g., friendliness and support.

The physical and psychological environment where data was collected was made comfortable by ensuring privacy, confidentiality and general physical comfort. Subjects were requested not to write their names on the questionnaires to ensure confidentiality.

3.4.5.2 Validity

The validity of an instrument is the degree to which an instrument measures what it is intended to measure (Polit & Hungler 1993). Content validity refers to the extent to which an instrument represents the factors under study. To achieve content validity, questionnaires will include a variety of questions on the methods, reasons and outcomes of cyber-criminal activities within the Ayawaso East Constituency. (Polit & Hungler 1993).

Questions were based on information gathered during the literature review. Content validity was further ensured by consistency in administering the questionnaires. All questionnaires were distributed to subjects by the researcher personally. The questions were formulated in simple language for clarity and ease of understanding. Clear instructions were given to the subjects for the researcher to complete

the questionnaires for those subjects who were not be able to not read.

All the subjects were complete the questionnaires in the presence of the researcher. This was done to prevent subjects from giving questionnaires to other people to complete on their behalf. For validation, the questionnaires were submitted to a researcher and statistician. As a result more questions were added to ensure higher representativeness. Rephrasing of some questions was done to clarify the questions and more appropriate alternative response choices were added to the closed-ended questions to provide for meaningful data analysis (Burns & Grove 1993).

External validity was ensured. Burns and Grove (1993) refer to external validity as the extent to which study findings can be generalised beyond the sample used. All the persons approached to participate in the study were have to complete the questionnaires. It is anticipated that some persons who were to be approached might refuse to participate.

Generalizing the findings to all members of the population was therefore be justified. Seeking subjects who were willing to participate in a study can be difficult, particularly if the study requires extensive amounts of time or other types of investment by subjects. If the number of the persons approached to participate in a study declines, generalizing the findings to all members of a population is not easy to justify. The study needs to be planned to limit the investment demands on subjects in order to increase participation. The number of persons who were to be approached and who might have refused to participate in the study were reported so that threats to external validity can be judged. As the percentage of those who decline to participate increases, external validity decreases (Burns & Grove 1993).

3.4.6 Pretesting and Questionnaires

A pre-test refers to a trial administration of an instrument to identify flaws. When a questionnaire is used as a data gathering instrument, it is necessary to determine whether questions and directions are clear to subjects and whether they understand what is required from them. This is referred to as the pretesting of a questionnaire (Polit & Hungler 1995).

The researcher pretested the questionnaire on six respondents meeting the set criteria at the Ayawaso East Constituency. All of them will answer the questions and no single question will be changed following the pretest.

3.4.7 Ethical considerations

The conducting of research requires not only expertise and diligence, but also honesty and integrity. This is done to recognize and protect the rights of human subjects. To render the study ethically, the rights to self-determination, anonymity, confidentiality and informed consent were observed.

Subjects' consent were obtained before they completed the questionnaires. Burns and Grove (1993) define informed consent as the prospective subject's agreement to participate voluntarily in a study, which is reached after assimilation of essential information about the study. The subjects were informed of their rights to voluntarily consent or decline to participate, and to withdraw participation at any time without penalty.

Subjects were informed about the purpose of the study, the procedures that would be used to collect the data, and assured them that there were no potential risks or costs involved. Anonymity and confidentiality was maintained throughout the study. Burns and Grove (1993) define anonymity as

when subjects cannot be linked, even by the researcher, with his or her individual responses. In this study anonymity was to be ensured by not disclosing the respondent's name on the questionnaire and research reports and detaching the written consent from the questionnaire.

When subjects are promised confidentiality it meant that the information they provided were not publicly reported in a way which identifies them (Polit & Hungler 1995). In this study, confidentiality will be maintained by keeping the collected data confidential and not revealing the subjects' identities when reporting or publishing the study (Burns & Grove 1993:99). No identifying information were entered onto the questionnaires, and questionnaires were only numbered after data has been collected (Polit & Hungler1995).

The ethical principle of self-determination was also be maintained. Subjects were treated as autonomous agents by informing them about the study and allowing them to voluntarily choose to participate or not. Lastly, information was provided about the researcher in the event of further questions or complaints. Scientific honesty is regarded as a very important ethical responsibility when conducting research. Dishonest conduct includes manipulation of design and methods, and retention or manipulation of data (Brink, 1996). The researcher tried to avoid any form of dishonesty by recording truthfully the answers of those subjects who were not be able to read or write. Manipulation of data was not be done as the supervisor and an independent statistician entered the data from the questionnaires into the SPSS computer software program. The statistician produced the results independently of the researcher to avoid subjective collaboration. The open-ended questions which were analysed by the researcher was also be checked by the supervisor for confirmation of credibility.

3.4.8 Data Analysis

After the data was collected it was organised and analysed. For analysis of the quantitative data, a computer programme called Statistical Package and Services Solution (SPSS) was used. Data was analysed by the technique of descriptive statistics. Frequency tables were drawn and from these the data were presented in pie diagrams and bar graphs. Thematic analysis was used to analyse the qualitative data.

3.5 Conclusion

The researcher used a mixed method, descriptive survey design. Interviews and questionnaires were administered by the researcher to collect the data from a convenient sample of 40 subjects. The questionnaires had both closed and open-ended questions. The sample characteristics included people who are mentally sound and are willing to participate.

Permission was obtained from the municipal assembly. Consent were obtained from the subjects themselves. Anonymity, self-determination and confidentiality were ensured during administration of the questionnaires and report writing. Questionnaires were distributed to subjects to ensure validity. Reliability and validity was further increased by pretesting the questionnaire. This chapter describes the research methodology, including the population, sample, data collection instruments as well as strategies used to ensure the ethical standards, reliability and validity of the study.

CHAPTER FOUR

ANALYSIS AND DISCUSSION OF RESULTS

4.1 Introduction

The previous chapter discussed the various techniques and approaches used to conduct the study, specifically to obtain the primary data as well as the secondary information. The purpose of this chapter is solely to presents the statistical outcome and analysis of primary data.

The analysis begun with the demographic profile of respondents of the quantitative survey and key informants for the qualitative interview. This is followed by the coding framework and network of themes from the perspective of key informants and the frequency results from the perspective of respondents.

4.2 Demographic Profile of Respondents

The demographic profile of participants are divided into two: respondents of the quantitative survey and key informants for the qualitative interview. This is because the researcher wants to draw a distinction between the participants in terms of their status.

4.2.1 Respondents of the quantitative survey

In the Table 4.1, the statistical results displayed shows the demographic profile of 100 respondents interviewed. It first shows the background profile of the youths (respondents) engaged in cybercrime and then followed by respondents who are not engaged in cybercrime but facing cybercrime as a social problem in Ayawaso East Constituency.

Table 4.1: Respondents' Demographic Characteristics

		Respondents Engaged in Cybercrime (Cyber criminals)		Respondents facing Cybercrime as a social problem	
Variables	**Category**	**Frequency**	**Percent**	**Frequency**	**Percent**
Gender	Male	57	95%	23	57.5
	Female	3	5%	17	52.5
	Total	60	100	40	100
Age	15 to 19 years	22	36	-	-
	20-24 years	10	16.7	-	-
	25 to 29 years	28	46.8	-	-
	30 to 34 years	-	-	1	2.5
	35 to 39 years	-	-	8	20
	40 to 44 years	-	-	11	27.5
	45 to 49 years	-	-	15	37.5
	50 and above	-	-	5	12.5
	Total	60	100	40	100
Marital Status	Single	60	100	3	7.5
	Married	-	-	22	55
	Divorced	-	-	15	37.5
	Total	60	100	40	100
Education	No Formal education	-	-	5	12.5
	Basic level	6	10	12	30
	Secondary level	35	58.3	18	45
	Technical/Vocational	7	11.7	-	-
	Tertiary level	12	20	5	12.5
	Total	60	100	40	100
Religion	Christian	22	36.7	15	37.5
	Muslim	38	63.3	25	62.5
	Total	60	100	40	100
Place of Origin	Northern Region	17	28.3	19	47.5
	Volta Region	10	16.7	8	20
	Greater Accra Region	11	18.3	11	27.5
	Ashanti Region	10	16.7	2	5
	Eastern Region	9	15	-	-
	Non-Ghanaian	3	5	-	-
	Total	60	100	40	100

Ethnicity	Ewe	12	19.9	5	12.5
	Ashanti	10	16.7	6	15
	Fante	3	5	-	-
	Ga	3	5	9	22.5
	Dagomba	7	11.7	2	5
	Bulsa	4	6.7	3	7.5
	Busawga	4	6.7	3	7.5
	Hausa	14	23.3	12	30
	Total	60	100	40	100
Occupation	Footballer	3	5	-	-
	Trader/Private business person	6	10	20	50
	Internet Café Attendant	3	5	-	-
	Marketing Promoter	3	5	-	-
	Not working, Student	22	36.7	-	-
	Not working, looking for job	23	38.3	-	-
	Civil/Public servants	-	-	15	37.5
	Casual worker	-	-	5	12.5
	Total	60	100	40	100
Residency	Resident of Ayawaso-East Constituency	47	78.3	24	60
	Non-resident of Ayawaso-East Constituency	13	21.7	16	40
	Total	60	100	40	100

Source: Author's Field Data, 2015

Gender

The statistical data provided in the Table 4.1 shows that, majority (95%) of the respondents who have ever engaged in cybercrime were males, females were extremely few (5%). This means that, in Ghana, specifically Ayawaso East Constituency, the practices of cybercrime is commonly predominant among the male youths. This confirms what Warner's (2011) stated that most of the Ghanaians engaged in cybercrime are males and what the AGDoA (2013) reported that most of those engaged in cybercrime are males. This finding is also similar to Okeshola and Adeta's (2013) finding in Nigeria that an extreme proportion (89%) of cybercriminals were males. Although, proportionally, there is

difference between Ghana and Nigeria in terms of age of cybercriminals, one can based on this finding to assert that cybercriminals in West Africa are predominantly males. Again, the fact is well established, cybercrime is a criminal activity of the males (both boys and adults).

In the same Table 4.1, the descriptive statistics showed that, of the respondents not engaged in cybercrime, most (57.5%) were males. This means that, majority of the males living in the study area are much worried about the existence of the practices of cybercrime in the study area.

Age

In the above table (Table 4.1), it is shown that, a greater proportion (46.8%) of respondents ever engaged in cybercrime were between the ages of 25 and 29 years while the few (16.7%) were between the ages of 20 and 24 years. Clearly, most of the cybercriminals in Ghana are young, similar to what Okeshola and Adeta (2013) discovered in Zaria in Nigeria that, 88% of 400 respondents were within the ages of 18 and 30 years.

Contrarily, the statistics in Table 4.1 demonstrates that, for those not engaged in cybercrime, a greater proportion (37.5%) were between the ages of 45 and 49 but only one (2.5%) was between 30 and 34 years. This means, majority (37.5%) were growing old (between 45 and 49 years). It is therefore not surprising that they are worried about the existence of cybercrime in the study area as people at this particular age seem to be more concerned about socioeconomic lifestyle.

Marital Status

In Table 4.1, the marital status shows that, none of the youths engaged in cybercrime had neither married nor divorced; they (100%) were all single. This could mean that, cybercrime does not

necessarily engage married couples. Thus, an activity for the young individuals to make a living or create wealth.

Inversely, the descriptive statistics revealed that majority (55%) of the respondents not engaged in cybercrime were married couples (see Table 4.1). This could mean that, married couples do not engaged in cybercrime and do not depend on online criminal activities for either wealth creation or livelihood. Again, this finding confirms that, cybercrime is an activity of the unmarried youths.

Education

Boundless (2105) and Sharma (2007) contend that "education is regarded largely as a means to occupational attainment". Findings from the analysis of quantitative illustrated that, most of the respondents engaged in cybercrime have not attained tertiary education. Based on the statistics in Table 4.1, as high as 35 (58.3%) were with SHS qualification, only few (10%) had basic (primary) education. Understanding of this is that, youths engaged in cybercrime are secondary school students. Even though, this finding contradicts that of Okeshola and Adeta (2013) where 60% of cybercriminals were discovered to be university graduates, understanding of this is simple, young intellectuals are more engaged in the practices of cybercrime. Based on Okeshola and Adeta (2013) findings and this, indirectly this could mean that, cybercrime is an intellectual phenomenon.

The data on Table 4.1 furthermore reveals the demography of respondents not engaged in cybercrime seems to be the same as that of those engaged in it. The descriptive statistics on their educational profile shows that, most (45%) were with secondary school qualification. This could mean that, their educational attainment makes them know that cybercrime existing in the study area is a social problem. Debatably, one could ask, why those engaged in cybercrime do not recognize it as a social

problem? Section 5.2.2 could help understand and grasp the answer based on the views of the participants.

Religious Background

A greater proportion (63.3%) of youths engaged in cybercrime were with Muslim background. As Table 4.1 illustrates, with a recorded value of (63.3%) for Muslims, it was made known that religiously, of the youths engaged in cybercrime, most of them were with Muslim origin. One can base on this to affirm that, more of the Muslim youths are engaged in cybercrime than any other youth with different religious background. However, one cannot conclude that Muslims are cybercriminals. The distinction here is, both Christians and Muslim youths are engaged in the practices of cybercrime but the Muslim youths are more. This could be a perfect reflection of Ayawaso East Constituency demography. The selected constituency is dominated by Muslims. But still, the act of committing crime on the internet involves more Muslim youths.

Not different from that of respondents ever engaged in cybercrime, the results of the descriptive analysis demonstrates that, majority (62.5%) of respondents not engaged in cybercrime were with Muslim background. That is although more Muslim youths were engaged in the practices of cybercrime, most of the people bothered with the existence of cybercrime in the study area were Muslims. Still to say, it could be a perfect reflection of the demographic nature of the study area.

Occupation

Youth unemployment describes persons within a specified age bracket who are unemployed (Zenou, 2000). In the Table 4.1, the descriptive analysis on the occupational status of respondents engaged in cybercrime demonstrates that, an extreme proportion (75%) of the youths engaged in cybercrime were

not working (unemployed), of which 36.7% were students and the highest proportion (38.3%) were looking for job. This is a refutation to Oumarou's (2007) statement that, most of the people engaged in cybercrime are neither seeking nor willing to work. But the understanding of this is that, cybercrime involves two category of youths—students and non-students but jobless. A perfect evidence that most of the cybercriminals in Ghana are either underemployed or unemployed (GNA, 2009). Economically, regarding the means through which people use to make a living, cybercrime even though is painted evil (crime), it is the alternative means for the unemployed youths to survive perhaps economic hardship. Unemployment is an observable sign of economic recession; it is a state of a country's economic status, hence unemployed youths engaged in cybercrime is a reflection of the state of a country's young labour force.

Concerning those not engaged in cybercrime, from the figures in the Table 4.1, it is evidence that majority (50%) were traders or private businessperson and the few (12.5%) were casual workers. This outcome shows that, the driving economic activity in the constituency is predominantly the private enterprise (sector). As majority are traders, it means the natives of the study area do their individual works; they do not depend on the government. One can based on this to conclude that, Ayawaso East Constituency is lacking public jobs and that is why most youths are unemployed. And that, in ability of the youths to create their own jobs has influenced them into cybercrime.

Place of Origin

The study strived to find out the place of origin of those engaged in cybercrime, as seen in Table 4.1 it was made known that, about 28.3% of the cybercriminals in the study area were of Northern origin but the few (5%) were non-Ghanaians. This means that, more of the youths from the Northern region

in Ayawaso East constituency practice cybercrime. Or to better to say, most of the cybercriminals came from Northern region. This affirms that most of the cybercriminals reside in the capital towns like Accra, Takoradi and Kumasi, where internet service or café is accessible and affordable (Abugri, 2011). Still to this, the study discovered that the youth minority (5%) engaged in cybercrime were not Ghanaians. Perhaps, these three people were transients purposely to avoid being tracked by the intelligence agency.

Most (47.5%) of respondents not engaged in cybercrime few (5%) were from Ashanti Region but majority (47.5%) were from the Northern region. It is not surprising that they are more concerned with the practices of cybercrime in the study area, perhaps most of them are the parents of the youths engaged in cybercrime. Simply because they are all from the same region and residents of the same community.

Ethnicity

The ethnic background of respondents engaged in cybercrime showed that, the greatest proportion (23.3%) were with Hausa background but the few (5%) were with Fante and Ga background, respectively. This is not surprising because more Muslim youths were recorded to be dominating the practices of cybercrime. Other youths from different ethnic background were engaged in cybercrime but those with Fanti and Ga background, were the few. There must be a reason for this, if further research is made to cover a wider sample size.

The trend of the demographic profile seems the same as that of the youths engaged in cybercrime. Once again, an extreme proportion (30%) of the 40 respondents not engaged in cybercrime were with

Hausa background but the few (7.5%) were with Bulsa and Busawga background, respectively. This means most of the Hausa people in the study area are facing cybercrime as a social problem.

Residential Status

Having discovered the place of origin and the ethnic background, the researcher probed to find out if really (truly), youths engaged in cybercrime were residents (natives) of Ayawaso East Constituency. The statistical findings (see Table 4.1) showed that, most (78.3%) of the youths engaged in cybercrime at the study area were natives or reside in the same town. This means what Abugri (2011) asserted that, most of those engaged in cybercrime are located in slums like Maamobi, Accra New Town and Mallam Atta is true. In addition, the finding by the AGDoA (2013) that, more than half of 75% of the cybercriminals perpetrating fraud and other internet crimes in Australia are residing in urban centres like California, New York, et cetera, and are among the most populated cities is true.

Evidence provided in the Table 4.1 showed that, an extreme proportion (60%) of the respondents not engaged in cybercrime were residents of the study area. This means they were directly experiencing the negativity of cybercrimes among the youth in the area.

4.2.2 Key informants of the qualitative survey

The Table 4.2, displays the detailed background of the 11 key informants selected for in-depth structured interviews. Also, the table displays their code (**R)** as a representative identification. This code was used throughout the thematic content analysis and as well all the analysis and discussions performed in this chapter and the discussion made in the preceding chapter for easy identification.

Table 4.2: Demographic Characteristics of Key Informants

Interviewee (R)	Personality	Sex	Age	Marital Status	Religious Status	Occupation	Education Level	Tribal Origin	Years living in Ayawaso-East Constituency
R.1	Chief Superintendent (GPS-CU)	M	46	Married	Christian	Police Service	SHS	Ga	7
R.2	Imam	M	56	Married	Muslim	Imam	No formal education	Hausa	26
R.3	Pastor	M	59	Married	Christian	Pastor	JHS	Ashanti	15
R.4	Assemblyman	M	49	Widowed	Christian	Businessman	JHS	Ga	21
R.5	Assemblyman	M	52	Divorced	Muslim	Car Dealer	SHS	Dagomba	12
R.6	Assemblyman	M	45	Married	Muslim	Headmaster	Tertiary	Dagomba	18
R.7	Assemblyman	M	50	Married	Muslim	Station Master	SHS	Gonja	13
R.8	Youths Association leader	M	48	Divorced	Christian	Businessman	JHS	Ewe	14
R.9	Youths Association leader	M	38	Single	Muslim	Driver	No formal education	Kokomba	9
R.10	Youths Association leader	M	45	Married	Muslim	Welder	JHS	Kokomba	17
R.11	Youths Association leader	M	35	Single	Muslim	Butcher	No formal education	Mamprusi	11

Source: Author's Field Data, 2015

On the side of the interviewees (key informants), the statistical findings of their demographics showed that, all the interviewees were male adults. This mainly due to their position as some were Assemblymen, Imam, pastor, and community youths leaders. All were within the ages of 35 and 50, of which many (5) were within the ages of 40 and 49 years. This means they are also matured and have a detailed knowledge in cybercrime. The findings on their religious background shows that, many (7) were Muslims. Educational status, proved that majority (4) were JHS graduates and business is the main occupation of the majority (2). The findings on the residential status proved that, all the eleven (11) key informants interviewed reside in the same study area for over 6 years but less than 27 years.

4.3 Factors that drive (push and pull) youths into cybercrime

This section aims at achieving the first specific objective of the study, hence participants were asked to identify the factors or reasons that drive youths into cybercrime. Analysis of responses were divided into three perspectives. The views of: respondents engaged in cybercrime, those not engaged in cybercrime and key informants. This is to help determine distinction among the categories of participants on the factors that influence the youth into cybercrime. Then, followed by the discussion.

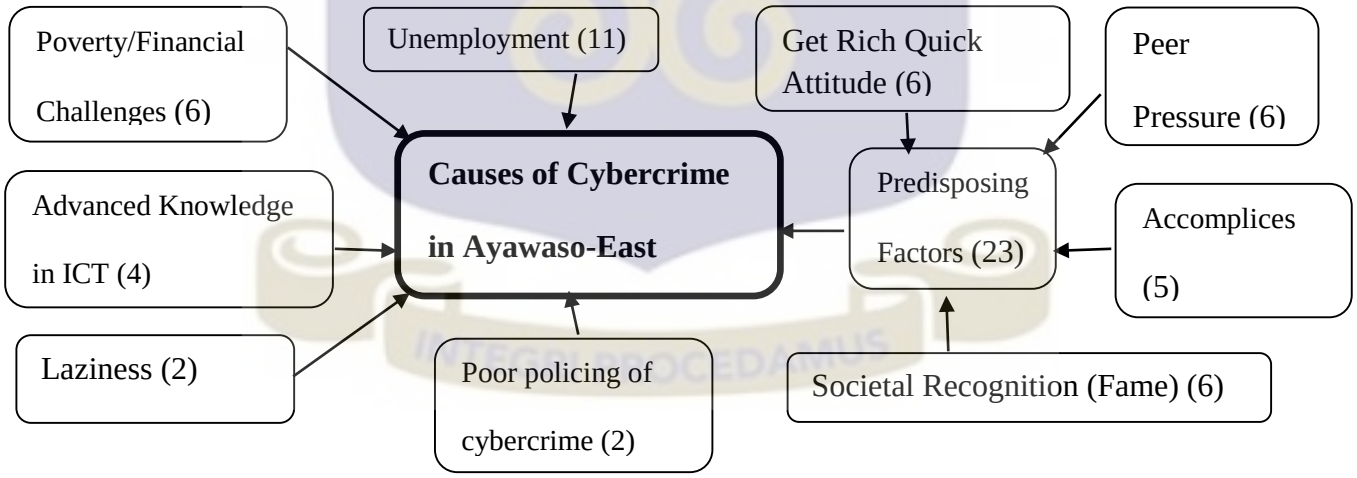
Table 4.3 shows the coding framework on the factors that drive youths into cybercrime based on the views of key informants interviewed. From the Table 4.3 and Figure 4.1, the factors according to key informants that drive youths into cybercrime were: Poverty/Financial Challenges (6 responses), Unemployment (11), Advanced Knowledge in ICT (4 responses), Laziness (2 responses), Poor policing of cybercrime (2 responses), and predisposing factors (23 responses)—Get Rich Quick Attitude (6 responses), Societal Recognition (Fame) (6 responses), Accomplices and Peer Pressure (6 responses) (see Figure 4.1).

Table 4.3: Coding Framework on Factors that influence people into Cybercrime by Key Informants

Global and Organizing Themes		R.1	R.2	R.3	R.4	R.5	R.6	R.7	R.8	R.9	R.10	R.11	Total
Factors that drive (push and pull) youths into cybercrime													11
Predisposing Factors	Get Rich Quick Attitude	*		*			*	*		*		*	6
	Societal Recognition (Fame)	*	*		*		*	*		*			6
	Accomplices	*	*	*		*						*	5
	Peer Pressure	*		*	*		*		*		*		6
Poverty/Financial Challenges					*		*	*		*	*	*	6
Laziness		*		*		*							3
Unemployment			*	*	*	*	*	*	*	*	*	*	10
Advanced Knowledge in ICT		*	*	*					*				4
Poor policing of cybercrime		*		*									2

Source: Author's Field Data, 2015

Figure 4.1: Thematic Network on the factors that influence people into Cybercrime based on Key Informants' perspectives



Source: Author's Field Data, 2015

From the views of respondents engaged in cybercrime practices, the factors that drive them into cybercrime as displayed in the Table 4.4 below were: Unemployment (45 responses), Peer pressure (28 responses), Educational challenges (15 responses), et cetera. See Table 4.4 for details and the statistical results. These factors were obtained when respondents were presented with an open-ended questions to freely provide the needed responses.

Table 4.4: Factors that influence youths into cybercrime according to respondents engaged in cybercrime

Cybercriminals' views on the causes of Cybercrime	And	Frequency	Percent
Unemployment	60	45	75
Poverty	60	43	71.7
Peer pressure	60	28	46.7
Educational challenges	60	15	25
Because of lucrative nature of cybercrime	60	32	53.3
Proliferation of internet cafes	60	29	48.3
Easy access to internet service	60	16	26.7
Advanced knowledge in ICT	60	13	21.7

Source: Author's Field Data, 2015

Those (respondents) who were not engaged in cybercrime but facing it as a social problem, mentioned some of the factors as: Unemployment (90%), Weak policing (57.5%), Attitude (Stubbornness) (30%), et cetera. See Table 4.4 for more of the factors and the statistical results.

Table 4.5: Factors that influence youths into cybercrime according to respondents facing cybercrime as a social problem

The views of individuals faced with cybercrime problems on the factors that drive people into cybercrime	Sample	Frequency	Percent
Get Rich Quick Attitude	40	36	90
Unemployment	40	36	90
Poverty	40	30	75
Weak policing	40	23	57.5
Proliferation of internet cafes	40	35	87.5
Attitude (Stubbornness)	40	12	30
Educational challenges	40	12	30
Easy access to internet service	40	29	72.5

Source: Author's Field Data, 2015

The internet has offered a huge platform for useful research purposes, however, some recalcitrant have turned its usefulness into negativity which has become a worldwide problem that is costing countries billions of dollars. As Merton's Social Strain Theory appears to suggest that certain strains increase the likelihood of crime. Hence, the first specific objective of the study aimed at identifying the factors (push and pull) that drive people into cybercrime. The qualitative and quantitative analysis performed showed that: *Poverty/Financial Challenges, Unemployment, Predisposing Factors (Get Rich Quick Attitude, and Peer Pressure, Accomplices, Societal Recognition [Fame]), Poor policing of cybercrime, Advanced Knowledge in ICT, Laziness, Educational challenges, the lucrative nature of cybercrime, Proliferation of internet cafes, Attitude (Stubbornness)* and *Easy access to internet service* as the various factors that drive people into cybercrime. These factors identified and discussed below go further to confirm the central theme of Merton's social theory that societal structures could lead (pull and/or push) people into social vices like crime.

a) Poverty/Financial Challenges

Findings from both qualitative and quantitative data analysis showed that, poverty or financial challenges could drive people into cybercrime. This what one Assemblyman said;

> My brother…it is money…it is money. To get money pay rent, water and electricity today is not easy. They feed themselves and that is what they use to live.[R4]

Two of the youth's association leader also explained;

> "The thing it is money, There is no money…things are hard ooh my bro ... things are hard."[R10]

The other said;

> "Finally, I will say people are poor that is why they tell lies and then collect money from people."[R11]

The finding confirms earlier finding by Magele (2005) and Meke (2012) that appears to suggest that the poor are more into cybercrime than the rich people. And also, means that, conformity is not common in the social system of the Ayawaso Consitutuency, that would articulate societal goals and its legitmate means to promote equal opportunities across individuals and social groups (Durkheim, 1915). More seriously, it is in this situation that Merton's theory predicts that the rates of deviance will be greater when the level of anomie is higher and when the extent of blocked opportunities is greater (Merton, 1968). This term 'anomie' according to Merton in explanation of the strain theory refers to the weakening of cultural norms.

b) Unemployment

Scholars like Hassan et al. (2012), Okeshola and Adeta (2013), Warner (2011), and Reingold, (1999) opined that high rate of unemployment brings about lots of criminal activities, including cybercrime. Similarly, the study disclosed that, cybercrime is also caused by unemployment.

Two Assemblymen explained;

> "Most of them are not working…that is what they do to live."[R4]

The other said;

> "I think they do not work. Massa! They do not work, they are always in the room."[R6]

Corroboratively, 90% of the respondents who were engaged in cybercrime mentioned that unemployment forced them into cybercrime. This unemployment issue could be attributed to the inability of the private sector which is the largest employment avenue to offer opportunities to job seekers. Perhaps the current energy crisis and the high lending rate by financial institutions have affected the creation and expansion of businesses, which could have offered the opportunities to the unemployed labour force in order to help people not turn to criminal activities, such as cybercrime as their means of survival. This suggests that, unemployment is a 'Rebellion' factor, as based on the views of participants interviewed is a major influencing factor letting people (cybercrime culprits) rejects both the cultural goals and traditional means of achieving them but actively attempts to replace both elements of the society with different goals and means (Boundless, 2015; Choi, 2008).

c) Predisposing Factors

Findings from the qualitative data proved that predisposing factors influence people to go into cybercrime. This was disclosed by 23 responses as displayed in the code frame (see Table 4.3) in chapter four. These predisposing factors includes:

- ***Get Rich Quick Attitude***

Finding from the thematic content revealed that, people enter cybercrime because they want to get rich quick or within the shortest possible time. This is what a the Imam and a police personnel interviewed said,

> "Erh…I will say most of them do not want to go through the normal life processes. They all want to get the money now! But it is not so in life Boss. It is not so…take your time, work hard and God willing four, five years your time will come. But these cybercriminals don't think this way. They need the money now."[R2]
>
> "First and foremost, this kind of "get rich attitude" that most of them in have that is driving them into this activity."[R2]

This finding was not just based on only the views of interviewees but 36 of the respondents not engaged in cybercrime said it (see Table 4.5 above). This validates what Shehu (2014) and Lipsey and Chrystal (2007) disclosed that, many poor people make it possible to level up the lager gap between the rich and the poor through cybercrime. It also reaffirms that of Choi (2008) and Guillaume (2009), that the mentality of the getting rich quickly at all cost has become the order of the day.

- ***Peer Pressure***

Findings from the qualitative data corroborate with the quantitative data that, peer pressure force people into cybercrime. Evidence is based on what the police man interviewed detailed;

> "…some are doing it because, they are under peer pressure to do it. They are in groups so you see somebody doing it…you are in school and you see somebody who has dropout of school and is going to do cyber fraud…he is able to buy car! He is riding in car. So the next thing that pressure influences another young person…he also decides to abandon education and go into this cyber fraud. So peer pressure too is one"[R1].

This could be the reason why most of those engaged in cybercrime reside in one particular place. And possibly, a way used to alleviate negative emotions or to relieve internal pressure (Boundless, 2015; Choi, 2008).

- ***Accomplices***

It was discovered through the interview that sometimes those who are already into cybercrime strive hard to pull other into it by either exhibiting their wealth gained through cyber fraud or any online crime. This what the Imam interviewed said about accomplices;

> "Some of the cybercrime culprits (suspects) use their fraud earnings and materials like cars et cetera, to rig in their colleagues who are not involved. So they are also increasing in the number of people that engaged in cybercrime."[R2]

- ***Societal Recognition (Fame)***

The social strain theory by Merton (1968) explained that, certain societal structures motivates people to commit crime. Also, Lipsey and Chrystal (2007), opined that the disjunction between culturally ascribed goals (that is economic success) and the availability of legitimate means to attain such goals in turn puts pressure on the cultural norms that guide what means should be used to achieve the culturally prescribed goal. In support of what the social strain theory and Lipsey and Chrystal (2007), pointed out, the study discovered that, societal recognition and adherence to these recognition motivates people into cybercrime. In this case, Merton (1968) proposed a typology of deviance based

upon two criteria: (1) a person's motivations or his adherence to cultural goals; (2) a person's belief in how to attain his goals. This is precisely discovered as one youth association leader explained,

> "…society…so we tend to worship people who have wealth…we adore them…we give them a big positions….in society we recognize them irrespective of how they acquire their wealth."[R9]

This finding confirms that, some societies acknowledge people who have money and extravagant properties and this motivates people to engage in cybercrime practices (Zenou, 2000). On a global perspective, the finding brought out establishes that in Ghana economic success is place at the pinnacle of societal desirability as in the case of United State of America (Merton, 1968). Undoubtedly, the fact is, societal recognition is not wrong but the rejection of the legitimate means of attaining it is condemnable and this is what Guillaume (2009) and Holzer (1991) term it 'Innovation' of the social strain theory.

It must be well noted that, the predisposing factors discussed above perfectly explain what Merton's (1968) Strain theory emphasizes that social structures may pressure citizens to commit crimes.

d) Poor policing of cybercrime (Fragile laws)

Okeshola and Adeta (2013) hold that, cybercrime exist everywhere there is weak cybercrime laws. This is the case of Ghana, as respondents interviewed mentioned that, because there is no well-defined law regulating the operational activities of the internet users, people take advantage of that to engage in all manner of criminal practices on the internet. This is strictly a 'Retreatism', according to the social strain theory (Choi, 2008; Halder & Aishankar, 2011; Holzer, 1991). Due to poor (fragile) laws against cybercrime, individuals engaged in internet crime have reject both the cultural goals, and traditional means of obtaining them, rather, resort to illegitimate means (cybercrime) in achieving

their own goals.

> "Our laws old. Our laws do no clearly define the charges for committing cybercrime. You get these people, you take them to court, then you cannot back the charges with laws (Arts.). We prosecute them as fraudsters."[R1]

Twenty three (23) respondents not engaged in cybercrime practices also mentioned that, because of weak policing that is why people engage in cybercrime. This means that, unlike armed robbers whereby they are directly charged or prosecuted upon their offense, for cybercriminals it is not so. It therefore means that, a cybercriminal when caught can get scot-free if s/he defends his/her case by a good lawyer. This well reaffirm Okeshola and Adeta (2013) assertion and confirms that in Ghana the laws regarding cybercrime activities are weak or fragile cybercriminal laws exist (Boateng, 2002).

e) Laziness

According to Oumarou (2007), most of the people engaged in cybercrime are economically active people but are neither seeking nor willing to work. In this context, Oumarous emphasis is on 'laziness' and this corroborates with the statement below by one Assemblyman,

> "…they want to be rich. They don't want to do any hard work."[R7]

f) Advanced Knowledge in ICT

Technology in today's world has advanced to a level that, one can do almost everything without assistance. The information technology has improved internet activities as well as human understandings about innovation. Twenty three respondents engaged in the practices of cybercrime disclosed that, advanced knowledge in ICT force them to engage in cybercrime. This is not surprising as it was demonstrated that, most of the youths engaged in cybercrime are the intellectuals. This is

what a pastor said about this finding,

> "Ah…ah…ah. Look, today even my little boy can use my phone to open my email. This people go to computer school to learn that and they come, they use it to steal instead of doing it good."[R3]

This finding could be attributed to the 'Innovation' aspect of the social strain theory. This is so because, advanced knowledge in ICT that alone is an innovation which help people achieve their societal goals but within this context, cybercrime culprits rejects the legitimate means of using ICT to achieve their goals (Guillaume, 2009; Holzer, 1991).

g) Educational challenges

Boundless (2015) and Sharma (2007) contended that "education is regarded largely as a means to occupational attainment, which in turn is valued primarily insofar as it promises economic rewards". Not misinterpreting Boundless (2015) and Sharma (2007), their statements could mean educational challenges is a projection of occupational challenges. And this is a precise prescription of what both respondents engaged in cybercrime and those not engaged in cybercrime mentioned that challenges associated with education are the reasons that force people into cybercrime. Even though, they could not get the opportunity to explain but this could be what Boundless (2015) and Halder and Aishankar (2011) stressed in explaining Merton's strain theory, "Parents of lower-class children often do not equip them with the skills and attitudes necessary to do well in school. Lower-class individuals often attend inferior schools, and they often lack the funds to obtain college educations or start their own businesses." This is could possibly means people from the lower class background reject both the cultural goals and the traditional means of achieving them, rather persistently attempts to obtain different goals through different means. A perfect exemplification and explanation of the 'Rebellion'

dimension of the social strain theory by Boundless (2015) and Choi (2008).

h) The lucrative nature of cybercrime

According to the ITU (2007), the losses that USA alone incurred through cybercrime increased from $52.5 million in 2006 to $67 million in 2007. Not only USA, the AGDoA (2013) reported that non-government cost of cybercrime is about 2 billion dollars annually. This means that, people's earnings through cybercrime worth millions of dollars. Not surprising that the descriptive analysis of quantitative data disclosed that because cybercrime is lucrative that is why people engage in it.

i) *Proliferation of internet cafes*

The findings showed that, because of the establishment of internet cafes in most centers of the study area that is why people are engaged in cybercrime. This was disclosed by 29 respondents engaged in cybercrime and 35 respondents not engaged in cybercrime. A confirmation that the use of the internet in Ghana has seen a significant increase since the liberalization of the telecommunication industry in the 1990s (ITU, 2008). Again this finding means that nations like Nigeria, Cameroon and Ghana have facilities for mobile internet access through satellite connections and fibre optic cables (Longe et al., 2009).

j) *Attitude (Stubbornness)*

According to Okeshola and Adeta (2013), people engage in crime because of their decision or willingness to do and this is based on the attitude of the person because people with good moral principles do not involve themselves in criminalities and vice versa. In support of Okeshola and Adeta

(2013), the study based on the responses of 12 respondents not engaged in cybercrime to point out that, attitude (stubbornness) is among the factors driving people into cybercrime (see Table 4.5 above).

k) *Easy access to internet service*

Findings from descriptive analysis on respondents' views (see Table 4.4 and 4.5) proved that easy accessibility of internet services influence people into cybercrime. This finding corroborates with what one policeman expressed;

> "Yes! It has---it has. Because, when there is access people will by all means use it fluently so the public café ...the public café… that have sprung up are all contributing to cybercrime."[R1]

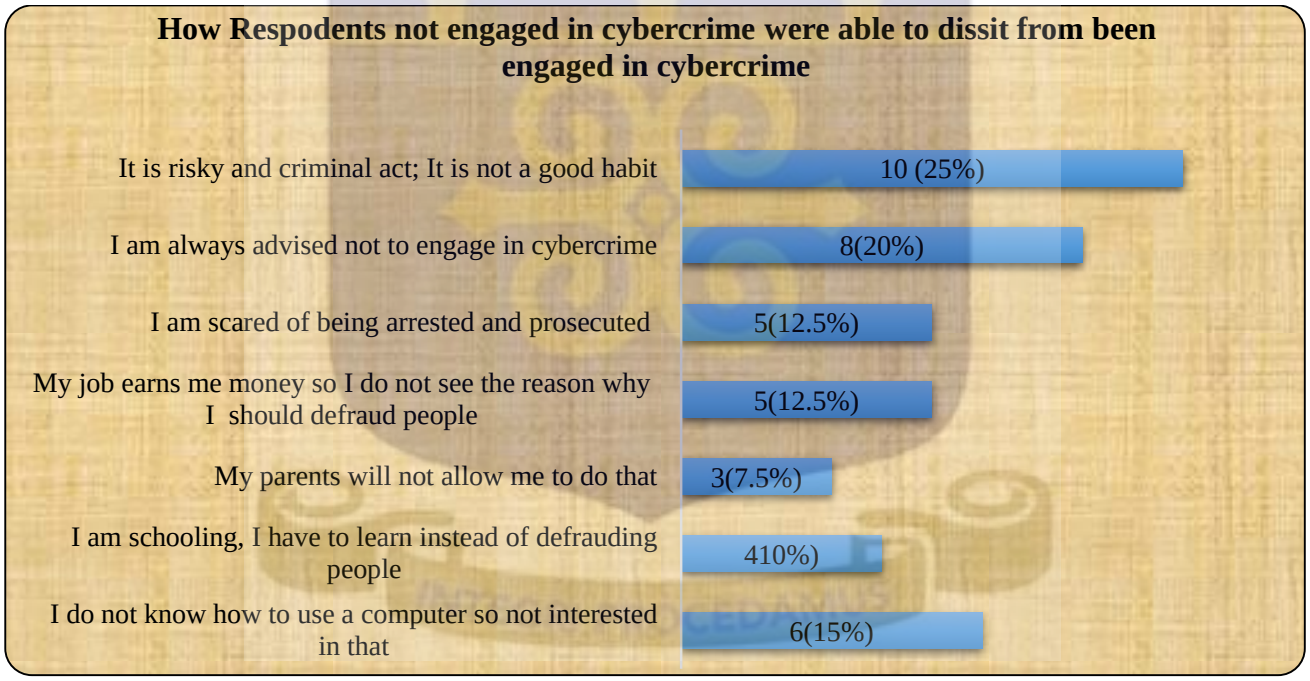
This outcome is strictly 'Retreatism' of the social strain theory in that, provision of easy access to internet service is not a rejection of both cultural goals and the traditional means of achieving them (Choi, 2008; Halder & Aishankar, 2011; Holzer, 1991). The outcome as well is in conformity to what Hassan, et al., (2012) added that, in Nigeria, because of the influx of second hand computers, and availability of modems or wireless networks, the practice of committing crime online is cheap and simple. Which suggest that, crime becomes a likely outcome when (…) the costs of committing crime is low (Sharma, 2007).

In summary, the various factors deliberated upon in this section of analysis, corroborate with what Merton carefully brought to bear in explaining his social strain theory that there are a number of ways in which individuals may adapt to the "strains" brought on by the inability to secure pecuniary success, and not all of these adaptations are deviant (Merton, 1968).

4.3.1 How Respondents not engaged in cybercrime were able to restrain from the factors that push and pull other people into committing internet crime

As outlined in the chapter three of the study, of the two categories of respondents selected: 40 were those not engaged in cybercrime. This category of respondents were asked optionally to state or explain how they were able to manage or not influenced by the factors that indeed influenced their colleagues to be engaged in cybercrime? The responses that disclosed have been presented in the Figure 4.2 below.

Figure 4.2: How Respondents not engaged in cybercrime were able to deal with factors that induced their colleagues into cybercrime



Source: Author's Field Data, 2015

The figure above reveals how respondents not engaged in cybercrime were able to survive the factors that induced their colleagues into cybercrime practices. As Figure 4.2 presents, as high as 25% of this category of respondents were able to deal with the aforementioned factors (see Table 4.4 and 4.5 and

Figure 4.2 above) because they recognized that the act is *risky and criminal, therefore not a good habit.* That is moral principles restrained them from being engaged in cybercrime practices. This finding supports the assertion by Okeshola and Adeta (2013) that, (…) people with good moral principles (attitude) do not involve themselves in criminalities.

Further, 20% stated that, they were *always advised not to be engaged in cybercrime*. As to whether the advice came from their parents or not, they did not disclose. However, it signals that advice and obedience help people manage influencing factors that lead others into committing cybercrime. Much more, 12.5% explained that they were *scared of being arrested and prosecuted* that helped them dealt with factors compelling other people into cybercrime practices. Meaning, people are able to disengage in cybercrime practices by virtue of fear of prosecution. All these factors: *moral principles, obedience, advice* and *fear of prosecution,* bear on awareness creation and education. Based on this finding, it is therefore appropriate for one to draw the distinction that, people who are able to manage to survive the influencing factors that compel other people into committing internet crime behaves in accordance with socially accepted conventions (norms). This strengthens the social strain theory, especially the conformity aspect (dimension) which centers on the acceptance of the cultural goals and means of attaining those goals (Boundless, 2015; Halder & Aishankar, 2011).

Moving forward, as it follows in the Figure 4.3, 15% of this category of respondents also explained that because they *do not know how to use computer, they were not interested in engaging in cybercrime.* This means computer illiteracy restrain people from engaging in cybercrime practices; obviously indisputable as all cybercrime culprits were identified to be computer literates (see Section 4.3). This outcome as well supports the social strain theory in terms of its 'Retreatism'. More to the

factors, 10% of the respondents, claimed they were *schooling hence would have to learn instead of defrauding online*. The rest (10%) of the respondents stated that, their *job earns them money so do not see the reason to engage in defrauding people online*. This strengthens the explanation provided by Shehu (2014) that, the motivation for people to commit crime or act criminally is determined by the free will (choice) of those people. And the 'Ritualism' aspect of the social strain theory that cultural goals are rejected but the legitimate means of achieving goals are pursued (Choi, 2008; Merton, 1968).

According to the strain theory, as disclosed by Merton, there were a number of ways in which individuals may adapt to the "strains" brought on by the inability to secure pecuniary success, and not all of these adaptations are deviant (Merton, 1968). The study supports what the theory emphasized based on the understanding deduced from the analysis in this section that, *employment, computer illiteracy,* and *awareness creation and education on cybercrime* thus help people manage the influencing factors of engaging in (committing) cybercrime practices. Hence, will make 'Conformity' very common in social systems when goals and legitimate means are clearly articulated and promoted and when opportunities are equal across individuals and social groups (Durkheim, 1915).

Comparatively, deducing from the analysis on the various factors that help some respondents restrained from cybercrime practices and those that induced others into committing cybercrime, one can strongly proclaim that resorting to cybercrime as a means of achieving societal goals is highly behavioural and partly cognitive and emotional (Agnew, 1992). In addition, this finding support what Sharma (2007) contends that, "crime becomes a likely outcome when individuals have a low tolerance for strain, when they have poor coping skills and resources, when they have few conventional social supports, and when they are disposed to low self-control and negative emotionality.

4.4 The experiences of the youth engaged in cybercrime with the Ghana law

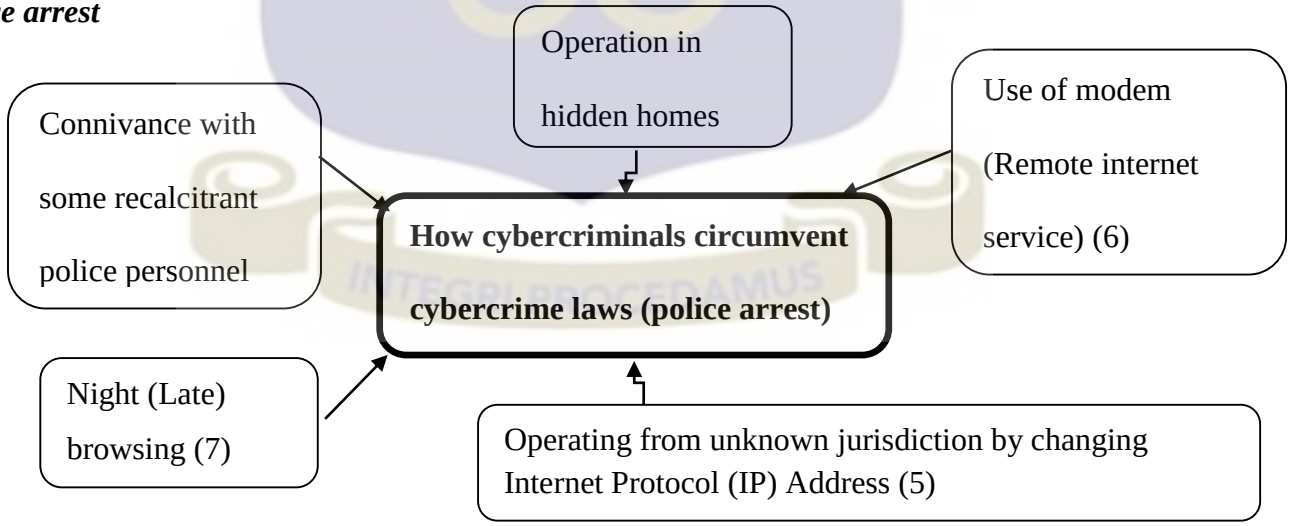
This section of the chapter discusses how cybercriminals circumvent police arrest and/or laws regarding cybercrime. The discussion is made from the perspectives of the three category of participants, for the sake of brevity.

Table 4.6: Key Informants' views on how Cybercriminals Circumvent police arrest or laws regarding cybercrime

Global and Organizing Themes	R.1	R.2	R.3	R.4	R.5	R.6	R.7	R.8	R.9	R.10	R.11	Total
How cybercriminals circumvent cybercrime laws												
Night (Late) browsing	*	*			*	*	*			*	*	7
Use of modem (Remote internet service)	*			*		*		*	*		*	6
Connivance with some recalcitrant police personnel	*		*		*	*		*		*		6
Operating from unknown jurisdiction by changing Internet Protocol (IP) Address	*	*		*			*				*	5
Operation in Hidden homes	*	*								*		3

Source: Author's Field Data, 2015

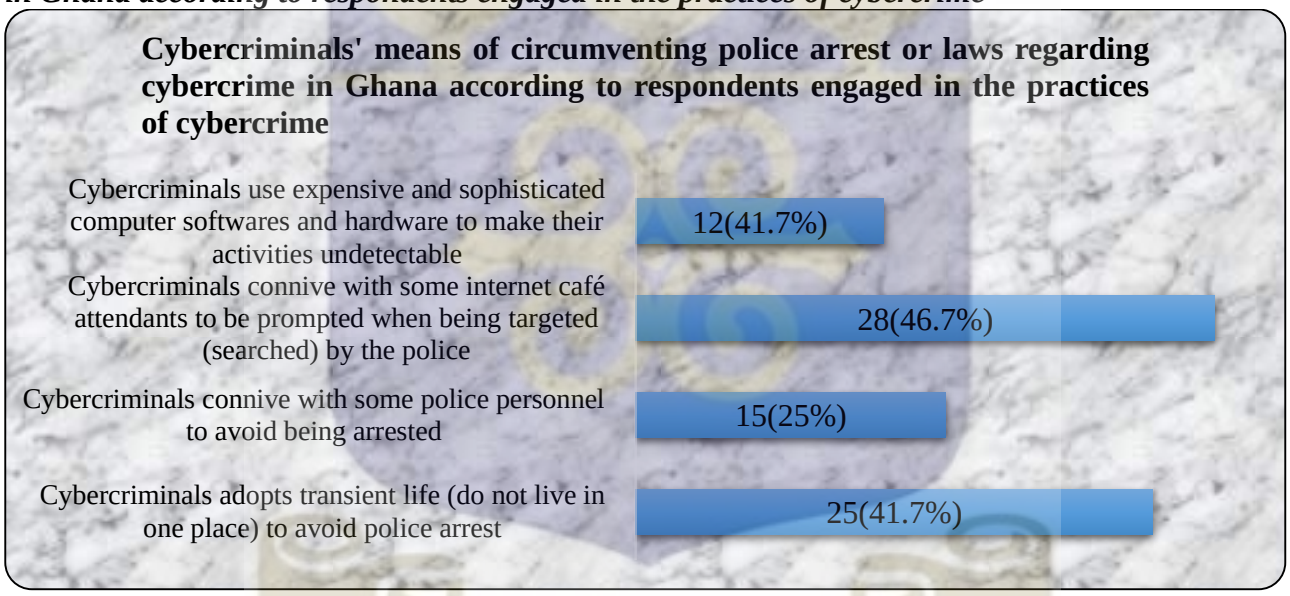
Figure 4.3: Thematic Network on how Cybercriminals circumvent laws regarding cybercrime or police arrest



Source: Author's Field Data, 2015

According to the 11 key informant interviewed, they mentioned numerous ways on which cyber criminals use to avoid police arrest or circumvent laws regarding their operations. These means include: Connivance with some recalcitrant police personnel (6 responses), Night (Late) browsing (7 responses), Operating from unknown jurisdiction by changing Internet Protocol (IP) (5 responses), Operation in Private homes (3 responses), and Use of modem (Remote internet service) (6 responses). The Figure 4.3 displays the results based on the global theme and organizing theme and Table 4.6 displays how the responses were derived.

Figure 4.4: Cybercriminals' means of circumventing police arrest or laws regarding cybercrime in Ghana according to respondents engaged in the practices of cybercrime



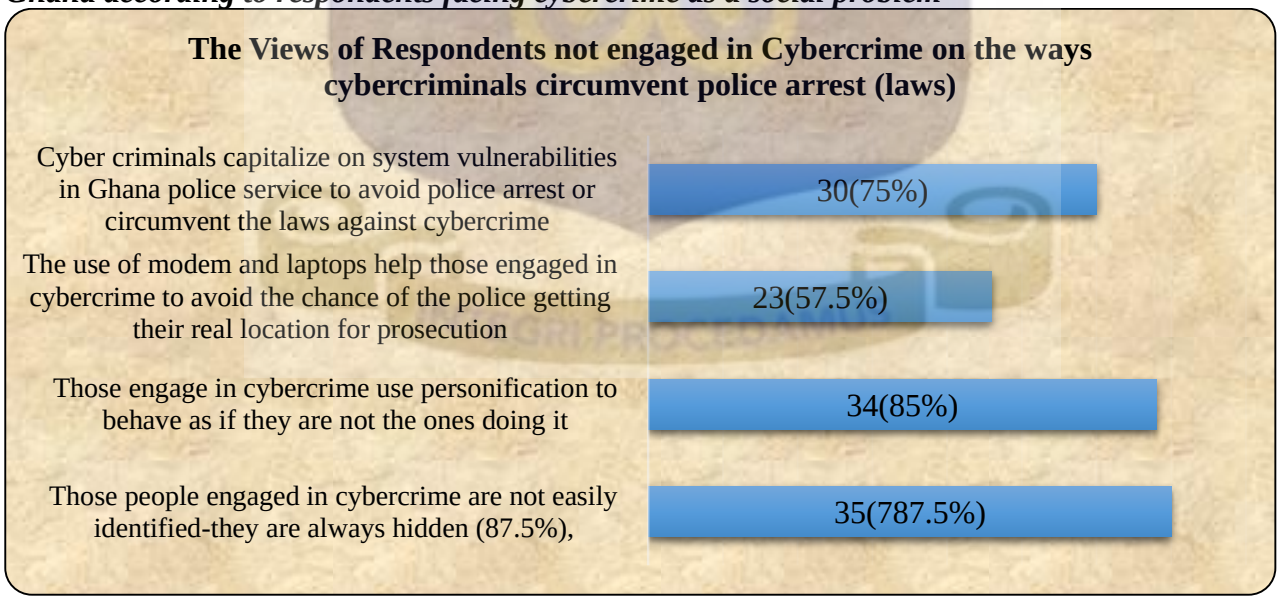
Source: Author's Field Data, 2015

As displayed in the Figure 4.4, respondents engaged in cybercrime disclosed that, *Cybercriminals adopts transient life (do not live in one place) to avoid police arrest (41.7%),* Cybercriminals connive with some police personnel to avoid being arrested *(25%), Cybercriminals connive with some internet café attendants to be prompted when being targeted (searched) by the police* (46.7%), and

Cybercriminals use expensive and sophisticated computer softwares and hardware to make their activities undetectable (71.7%), were the means they use to avoid police arrest or circumvent the laws regarding cybercrime in Ghana. See Figure 4.4 for statistical values.

For those (respondents) not engaged in cybercrime, these: Cyber criminals capitalize on system vulnerabilities in Ghana police service to avoid police arrest or circumvent the laws against cybercrime (75%); The use of modem and laptops help those engaged in cybercrime to avoid the chance of the police getting their real location for prosecution (57.5%); Those engage in cybercrime use personification to behave as if they are not the ones doing it (85%); and Those people engaged in cybercrime are not easily identified-they are always hidden (87.5%), are the means cybercriminals use to avoid police arrest and circumvent the laws regarding cybercrime in Ghana (see Figure 4.5 for details).

Figure 4.5 Cybercriminals' means of circumventing police arrest or laws regarding cybercrime in Ghana according to respondents facing cybercrime as a social problem



Source: Author's Field Data, 2015

4.4.1 Discussion on the experiences with the law (How cybercriminals circumvent the laws)

The thematic and descriptive analysis performed on acquired data revealed that: *Connivance with some recalcitrant police personnel; Night (Late) browsing; Operation in Private homes; Use of modem (Remote internet service);* and *Operating from unknown jurisdiction by changing Internet Protocol (IP) Address*, are the strategies that are used by those engaged in cybercrime to circumvent laws guiding cybercrime. These are explained below.

a) Connivance with some recalcitrant police personnel

It was discovered that some police personnel within the Ghana police service collaborate these cybercriminals to circumvent to avoid being caught by the police. This was discovered based what 15 respondents engaged in cybercrime revealed, which corroborated with the below statement from one police officer;

> "Yes! There are some of the frauds you see that, some policemen---let me say recalcitrant policemen have played some role which hare very bad."[R1]

This situation could happen perhaps because, the police personnel are all humans and react to situations or might be that they as well benefit from cybercrime. But the fact established here (in this section) authenticates Morgan and Kreuger's (1993) analysis of Merton's Anomie Strain Theory that centres on the criminogenic influence of a variety of social institutions in American society that instead of promoting other social goals, these social institutions primarily support the quest for material success. The understanding of the is that, certain existing institutions responsible for combating cybercrime are rather engaged directly or indirectly in increasing the practices of cybercrime that is bedeviling the society as a whole.

b) Night (Late) browsing

Browsing during the night was detected as another strategy used to avoid arrest or circumvent the laws against cybercrime. This finding is based on what the Pastor unfolded;

> "…where young people bring their own people…peers 10 people…15 people in a room with computers and browse in the night, only in the night."[R3]

c) Operation in Hidden homes

It was highlighted from the analysis that, cybercriminals secretly hide in some unknown homes to use their internet services to do their desirous crimes. This confirmatory comment; "*...in the privacy of your own home, nobody is there to see you*,"[R1, R2] came out from a police man and Imam.

d) Use of modem (Remote internet service)

Internet technology has made it very simple and easy to access internet services everywhere and anywhere**.** This has helped cybercriminals a lot, as it enable them operate everywhere and anytime. This was stated by an Assemblyman;

> "…they are using the computer, they are using the internet so they are operating from somewhere which is not known to us…"[R8]

In the same vein, 23 respondents not engaged cybercrime added that the use of modem and laptops help those engaged in cybercrime to avoid the chance of the police getting their real location for prosecution (see Figure 4.5 above).

e) Operating from unknown jurisdiction by changing Internet Protocol (IP) Address

Evidence garnered form the interviewees showed that, there is no fixed geographical location that cybercriminals use to operate. This is because the internet protocol (IP) Address sometimes are dynamic hence can be changed anytime or twist to different country, region or community. Hence,

tracking these criminals makes it difficult. This statement came from the police man;

> "…some of the fraudsters are outside the jurisdiction, for instance, the fact that the IP Address is in Accra does not automatically mean that the person is in Accra. The person can be operating from another country…"[R1]

Moving forward, the respondents not engaged in cybercrime also brought out some resilient strategies that were used by people engaged in cybercrime to circumvent cybercrime laws.

f) Cyber criminals capitalize on system vulnerabilities in Ghana police service to avoid police arrest or circumvent the laws against cybercrime?

In Ghana, because the mechanism used to check or monitor the operation activities of people on the net are either weak or not existing, many recalcitrant take advantage of that to do illegal things. It was discovered that, cybercriminals capitalise on the system vulnerabilities in the Ghana police service to avoid being caught by the police.

g) Difficulties in identifying cybercriminals

Those people engaged in cybercrime are not easily identified. They are always hidden. This is what was discovered in the analysis, according to 35 respondents not engaged in cybercrime. This means that what the policeman stated is highly true that, these cybercriminals operate from a jurisdiction that is difficult to detect.

Furthermore, respondents engaged in cybercrime practices as well pointed out the below strategies that were used to avoid jurisdictional prosecution or police arrest.

- **Cybercriminals adopts transient life (do not live in one place) to avoid police arrest**

Findings from the descriptive analysis of respondents engaged in cybercrime proved that, the youths engaged in cybercrime (cybercriminals) all adopt what is called **'transient lifestyle'.** That is they (cybercriminals) do not stay in one particular place for longer hours or days. Perhaps, due to fear or suspicion.

- **Cybercriminals connive with some internet café attendants to be prompted when being targeted (searched) by the police**

As high as 28 respondents engaged in cybercrime disclosed that some of the strategy that they use to avoid arrest is by consensus with the café attendants (see Figure 4.5 above). As to whether they give the café attendants money or not they did not disclose it. They did not as well explain how they connive with the café attendance as the questionnaire used did not give them that opportunity for detailed expressions. However this is a sensitive information (issue) that needs to be dealt with; something that needs not to be entertained. It is within this context that Agnew (1992) specified, the conditions under which strain may lead to crime, that strains that create some incentive to engage in criminal coping are most likely to lead to violence and delinquency.

- **Cybercriminals use expensive and sophisticated computer softwares and hardware to make their activities undetectable**

Modern internet gadgets are what the cybercriminals use to avoid being caught by the police. These expensive and modern computer softwares include proxy servers and applications allowing them to browse by proxy (anonymously). This is in doubt confirms that Ghana is not well equipped with

sophisticated hardware to track down the virtual forensic criminals (Broadhurst, 2006).

In summary, the results presented and interpreted in this section of the analysis fit in the explanation of social strain theory by Merton that the normative order or the institutionalized social norms may be weakened or lose their ability to regulate individuals' behaviour and that anomie will set in, in societies that place an intense value on economic success (Durkheim, 1915).

4.5 The state of intelligence and policy development to deal with cybercrime

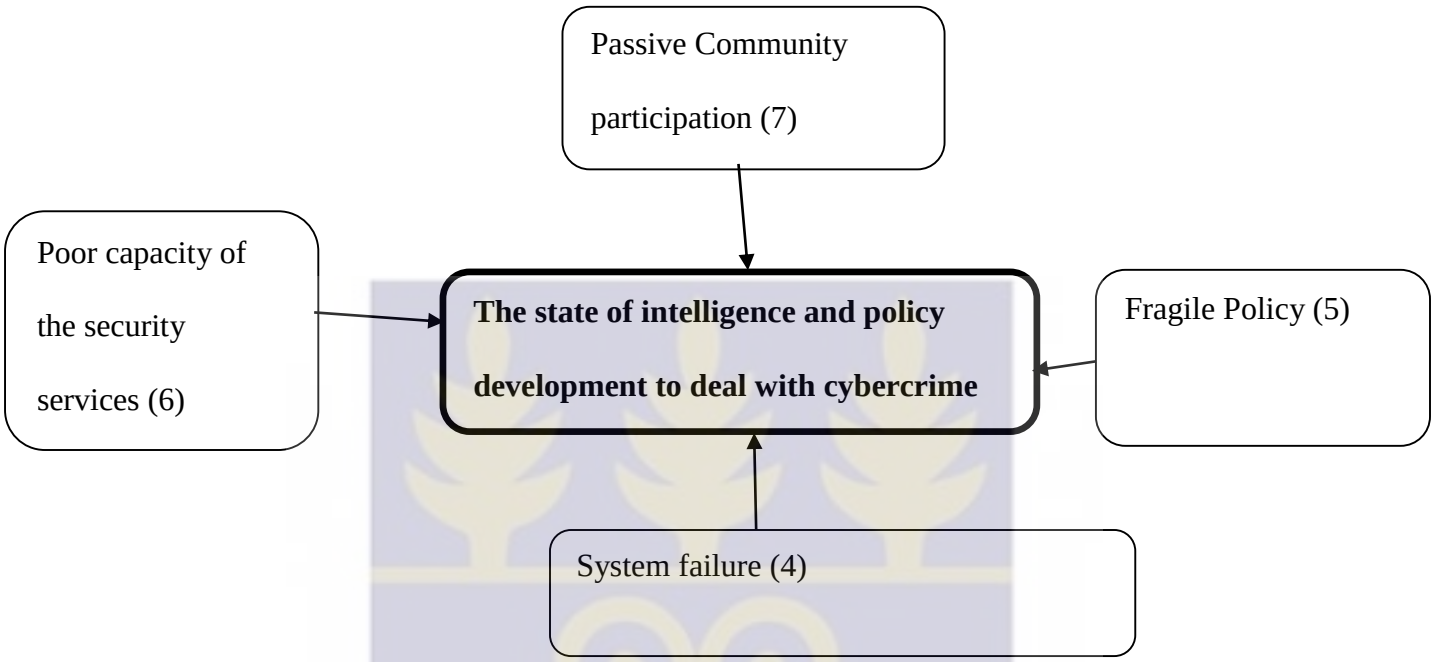
This section of the chapter seeks to examine the state of policing of cybercrime and solicits ideas and policy initiatives to determine how policing of cybercrime legislation will make it difficult for people to be involved in cybercrime.

Table 4.7: Coding Framework on the state of intelligence and policy development in dealing with Cybercrime based on key informants' perspectives

Global and Organizing Themes	R.1	R.2	R.3	R.4	R.5	R.6	R.7	R.8	R.9	R.10	R.11	Total
State of intelligence and policy development												
Passive Communication Participation		*		*		*	*	*		*	*	7
Poor capacity of the security services	*		*		*	*		*	*			6
Fragile Policy	*	*		*					*		*	5
System failure		*		*			*				*	4

Source: Author's Field Data, 2015

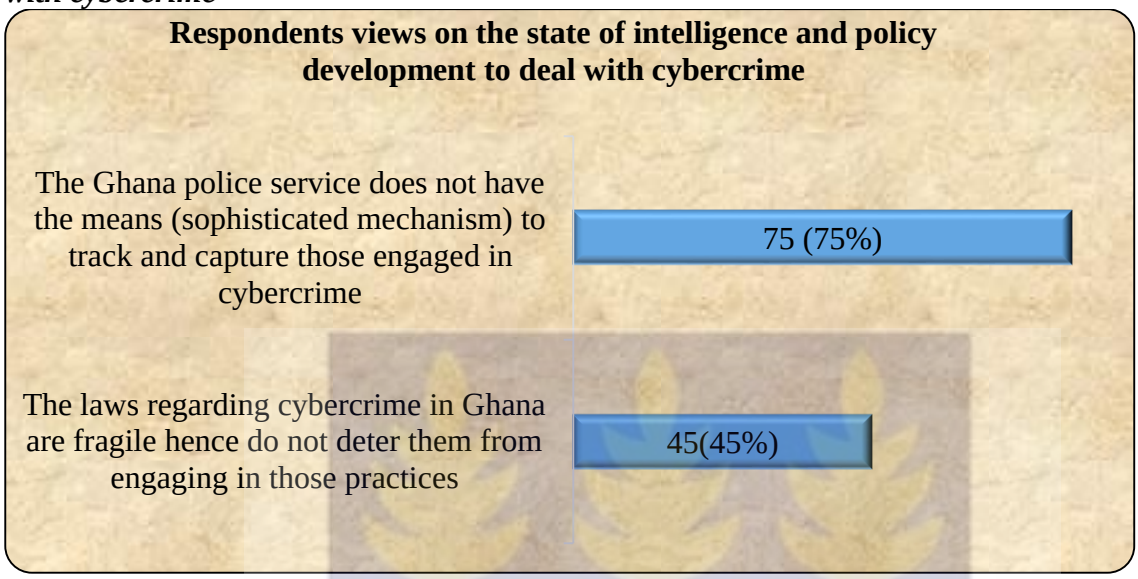
Figure 4.6: Thematic Network on the state of Intelligence and policy development



Source: Author's Field Data, 2015

Figure 4.6 and Table 4.7 shows that the state of intelligence in combating cybercrime is bad. These: Passive Communication Participation (7 responses), Poor capacity (6 responses), Fragile Policy (5 responses) and system failure (4 responses) are the various responses that came up from the analysis as part of the process to determine the state of policing cybercrime in Ghana.

Figure 4.7: The views of respondents on the state of intelligence and policy development to deal with cybercrime



Source: Author's Field Data, 2015

The statistical results displayed in the Table 4.7 shows that, 75% of the 100 respondents interviewed responded that the Ghana police service does not have the means (sophisticated mechanisms) to track and capture those engaged in cybercrime, and 45% also made it known that the laws regarding cybercrime in Ghana are fragile hence do not deter them from engaging in those practices.

4.5.1 Discussion on the state of intelligence and policy development

The third and final objective of the study seeks to examine the state of intelligence and policy development of cybercrime. To achieve this, all participants were asked to express their views on the state (nature) of security intelligence in policing crime in the constituency and the appropriate means of addressing this problem from an enforcement point of view. From both qualitative and quantitative data, the state of intelligence in policing cybercrime is weak because of the following factors discussed below.

- Passive Community Participation

Cybercrime is a societal phenomenon, combating it needs the active involvement of all stakeholders. It came to light that community participation in policing cybercrime is non-existent. This is what the Imam interviewed disclosed about this finding;

> "Look, we are here but we don't know what the police are doing about this... our summons are always against acts like this but the people don't even care to help stop this."[R.2]

As community participation in controlling cybercrime is identified to be minimal, it means that strains that are associated with low social control could leads to crime (Agnew, 1992).

- Poor capacity of the security services

The operations of cybercrime is dynamic. Technologies have made it so. But the security services in combating remain inadequately resourced to keep them abreast with the current trends of the modus operandi of cybercriminals. From the qualitative analysis, interviewees pointed out that, the capacity of the security services in combating cybercrime is poor. Evidence is based on what the one Assemblyman and the police officer articulated;

> "We all want to help the police in combating this but the perpetrators are very smart and they are using technologies to stay ahead of the police..."[R.5]

> "Now we need a kind of cyber training you know…people… we the investigators who are doing criminal investigations and the cybercrime investigations, we need special training. But unfortunately, this training is not available to many people as possible so they will be able to detect cybercrime as possible."[R.1]

This finding is a confirmation that, the recurrent act of cybercrime practices by people is due to the existence of weak institutional structures to track and capture cybercriminals (Longe & Chiemeke, 2006; AGDoA, 2013).

- Fragile Policy

Longe and Chiemeke (2006) and AGDoA (2013) mentioned that, the continual act of committing internet crime by people is because of (…) poor defined laws guiding cybercrime. Boateng (2002) asserted in his study that weak or fragile laws regarding cyber criminals exist in Ghana. Precisely, the study discovered that the continual perpetration of cybercriminals is because of existence of fragile policy in the country. Out of the 100 respondents interviewed, 45 explained that, the laws regarding cybercrime in Ghana are fragile hence do not deter cybercriminals from engaging in those practices. This corroborate with what the police officer stated during the in-depth interview;

> "Hmmm! [Laughing]. We still use the old law. The "Criminal Offenses Law Act 29 of 1960". The Electronic Transaction law has---has not been helpful in the investigation of cybercrime but we still rely on the old laws. We need new laws! New laws to deal with even erh the electronic evidence that we gather---there must be a new law for them to be admitted in evidence and those kind of thing."[R.1]

According to Hansell (2007) and Ani (2011), this motivates people to disregard the consequential results of perpertrating crime online. This finding reaffirms what Okeshola and Adeta (2013) hold that, cybercrime exist everywhere there is weak cybercrime laws. This means Ghanaian legislation must implement strict laws regarding cyber criminals and when criminal offences occur, perpetrators must be punished for the crime they have committed because (…) cyber criminals can take advantage of the weak gaps in the existing penal proceedings (Boateng, 2002).

- System Failure

A study by Richardson (2008) disclosed that new technologies that cybercriminals capitalize on system vulnerabilities. Analysis of the qualitative data showed that, indeed there exist system failure in the security structures. This statement from one Youth leader reaffirmed,

> "There is no system to check this things, you know what? The…the…system is weak…not like Europe, here the system is not in place to even anticipate a problem and deal with it."[R.9]

Laura (2012) states that "The law enforcement agencies in Africa are inadequately equipped in terms of personnel, intelligence and infrastructure, and the private sector is also lagging behind in curbing cybercrime".

- Lack of means to track and capture cybercriminals

The descriptive analysis performed on the views of 100 respondents, 75 explained that, the Ghana police service does not have the means (sophisticated mechanisms) to track and capture those engaged in cybercrime. This finding is in accordance with what Broadhurst (2006) opined that, the nation is not well equipped with sophisticated hardware to track down the virtual forensic criminals.

CHAPTER FIVE

SUMMARY AND DISCUSSION OF FININDGS

5.1 Introduction

Chapter 5 offers a summary and discussion of the researcher's findings, implications for practice, and recommendations for future research. The chapter first begins with the discussions of the findings then summarise it into various objectives and then draw conclusion from it. A recommendation will be made to determine the way forward in curtailing cybercrime in Ghana.

5. 3 Summary of Major Findings

The main objective of the study is to investigate activities of the youth in cybercrime. The following specific objectives were designed to achieve the main objective:

5.3.1 Demographic characteristics

The study discovered that, the demographic profile of respondents ever engaged in cybercrime seems to have some influence on the practices of cybercrime. The quantitative analysis performed on the demographic profile of respondents showed that, of the respondent engaged in cybercrime, an extreme proportion were males, of which majority were young adults, between the ages of 25 and 29 years. All the respondents engaged in cybercrime were not married and most of them were SHS graduates. It was revealed that, of these respondents engaged in cybercrime a greater proportion were of Muslim background and Northern origin. Moreover, a greater proportion were unemployed, and resident (native) of Ayawaso East Constituency. The study based on this findings to establish that, the practice of cybercrime is predominantly an activity of the young adults who are SHS graduates and

unemployed with most from Northern part of Ghana and of Hausa background. Furthermore, the study discovered that, the predominant occupation in the study area is private enterprise.

5.3.2 Factors that drive youths into cybercrime

There are numerous contributory factors influencing the youth into cybercrime. The analysis made on both qualitative and quantitative data revealed that, people engage in online crime because of: Poverty/Financial Challenges, Unemployment, Predisposing Factors (Get Rich Quick Attitude, and Peer Pressure, Accomplices, Societal Recognition [Fame]), Poor policing of cybercrime, Advanced Knowledge in ICT, Laziness, Educational challenges, the lucrative nature of cybercrime, Proliferation of internet cafes, Attitude (Stubbornness) and Easy access to internet service. These factors were revealed by those who engage in cybercrime, those who were not involved in cybercrime but faced with it and the key informants. These factors are socio-economic.

Directly associated to the above, it was, based on the views of respondents not engaged in cybercrime, established that *employment, computer illiteracy,* and *moral principles which all together relates to awareness creation and education on cybercrime* help people manage to survive the influencing factors of committing cybercrime.

5.3.3 How cybercriminals circumvent or protect themselves from the laws

Committing crime through the internet is regarded criminal yet people throw any caution to the wind and are involved in it. This is because of their ability to exploit their victims by circumventing the laws or police arrest through: connivance with some recalcitrant police personnel; night (late) browsing; operating in private homes; using of modem (remote internet service); operating from

unknown jurisdiction by changing internet protocol (IP) address, capitalizing on system vulnerabilities within the Ghana Police Service, connivance with some internet café attendants to be prompted when being targeted (looked for) by the police, and use of sophisticated computer softwares and hardware to make their activities undetectable. These means of circumventing the laws against cybercrime was revealed by all the participants interviewed.

5.3.4 The state of intelligence and policy development of cybercrime

The study based on the views of participants to establish that, the state of intelligence and policy development in policing cybercrime is weak. The reason being that, the exiting law used to prosecute cybercriminals is an old law which needs to be reformed to meet the present challenges in the fight against cybercrime. From the analysis, it was revealed that, Passive Community Participation, Fragile Policy, Poor capacity of the security services, System Failure and the lack of means to track and capture cybercriminals were the physical characteristics of the state of intelligence and policy development of cybercrime.

5.4 Conclusion

Cyber-crime presents enormous challenges to society, especially developing societies that are trying to catch-up with the technology revolution, yet are relatively weaker to respond to the challenges of this development.

It came out of the study that unemployment could drive the youth into cybercrime. This is because there is no viable social protection to provide livelihood to the unemployed. Therefore, the youth who are unemployed and do not receive any income would engage themselves in anything that would

provide food and their basic needs of life. The study therefore concludes that the youth enter into cybercrime to maintain livelihood.

The study revealed that poverty/financial challenges could lead many youth into taking up cybercrime to compensate for their inability to generate enough financial resources for their survival. This is because of the unavailability of jobs and economic hardships bedevilling the society. The study at this stage concludes that the youth who are poverty stricken take up to cybercrime to ensure their survival.

It came out of the study that most youth involved in cybercrime are able to prevent detection by the law enforcement agencies. This is because of their use of sophisticated computer softwares and with the tacit connivance of some law enforcement officers. Therefore, the youth who are involved in cybercrime are able to avoid detection and carry on with their acts. The study therefore concludes that many cybercriminals are able to carry on with their activities.

The study revealed that system vulnerabilities within the Ghana Police Service has allowed cybercrime to be perpetrated since the law enforcement agencies lack the requisite capacity and equipment to combat cybercriminals. This is because of a lack of retooling and budgetary support to enable them combat cybercrime. The study at this stage concludes that in the absence of the necessary support for the security agencies, the youth will find cybercrime a safe haven for their survival and wealth creation.

It came out of the study that passive community participation could allow more youth to go into cybercrime. This is because people in the communities refuse or fail to tip-off the security agencies or reprimand their wards who involved in cybercrime. Therefore, the youth who are involved in

cybercrime continue to engage in such activities. The study therefore concludes that the lack of community participation is contributing to many youth entering into cybercrime.

The study revealed that the absence of policy framework regarding the prosecution of cybercriminals has provided a fertile ground for the youth to engage in cybercrime. This is because of the fragile policies in place. The study at this stage concludes that the prosecution of cybercrime cases lacks appropriate legislation.

5.5 Policy Recommendation

The study at this stage based on the conclusion, recommends the following:

- The youth enter into cybercrime to make a living, it is suggested that a policy is enacted to provide unemployed benefits to the unemployed youth. It is also suggested that government reduces the policy rate to bring down cost of credit so more people can open up businesses.
- The issues with the youth borders on socioeconomic challenges, among them poverty. There is a need for government to create a conducive business environment by improving the energy situation for businesses to thrive and absorb the widening unemployed labour force.
- The widening poverty gap can lead many youth into cybercrime to boost their livelihood. It is imperative for government to provide forms of social protection to these youth to avert possible vulnerabilities. It is suggested that skills and entrepreneurship training be made available to the youth so they can venture into profitable businesses to improve their livelihood.
- Cybercrime is a global phenomenon which can be best dealt with through cooperation. This menace needs the adoption of best practices from countries that have been able to tackle cybercrime issues such as United States of America, France, and Britain. One of the strategies

discovered in the study that cybercriminals adopt to circumvent cyber laws or police arrest is the use of sophisticated computer technologies, which are sourced from these same countries. Cooperating with such countries will be an effective assistance in combating the menace.

- It is important that as law enforcement and international co-operation are improved, the capacity and quality of Ghana's prosecuting and intelligence agencies should be enhanced through a productive exchange between the private sector and public officials. It is imperative that, the capacity of law enforcement personnel are improved and well equipped to deal with the dynamics of the computer technology era.

- There should be more investment in research and development involving academia, the legal profession and law enforcement agencies. There is the need for more research in fashioning out criminal laws to deal with the cybercrime.

References

Abugri, S. (2011) Ghana: Internet criminals cashing in on e-waste. *New African*. Retrieved January 24, 2011, from http://www.sydneyabugri.com/Home2/features/217ghana-Internet-criminals-cash-in-on-e-waste-dumping.html.

Agnew, R. (1992). Foundation for a General Strain Theory. *Criminology*, 30(1), 47-87.

Anah, H. B., Funmi, D. L., & Makinde, J. (2012). Cybercrime in Nigeria: Causes, Effects and the Way Out. *E-journal of science* .

Ani, L. (2011). *Cyber Crime and National Security: The Role of the Penal and Procedural Law.*

Attorney General's Department of Australia. (2013). *National Plan to Combat Cybercrime. Commonwealth of Australia.* Accessed March 23, 2015 from http://www.ag.gov.au/

Boateng, K. A-S. (2002). An Analytical Study of the Labour Market for Tertiary Graduates in Ghana.

Boateng, R. (2014). *Research Made Essay*. Accra: PearlRichards Foundation

Boundless. (2015). Strain Theory: How Social Values Produce Deviance. *Boundless Sociology*. Retrieved 20 Jan. 2015 from International Labor Organization (October 1982).

Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime, Policing. *An International Journal of Police Strategies & Management, 29(3)*, 408 – 433.

Burns, N. & Grove, S.K. (1993) *The practice of nursing research conduct, critique & utilization* (second edition), Philadelphia: W.B. Saunders.

Choi, K. (2008). *Computer crime victimization and integrated theory: An empirical study.*

Criminal Investigation Department Headquarters. (2012). *Criminal Investigation Department (CID) Signs Memorandum of Understanding with e-Crime Bureau Inc. on e-Crime Investigations Capacity Building*. (Press Release). Accra: Criminal Investigation Department Headquarters.

De Vaus, D. A. (2002). *Surveys in Social Research* (5th Edition). Crows Nest: Allen & Unwin.

Durkheim, E. (1915). *The Elementary Forms of Religious Life*. New York: Free Press.

Ghana Statistical Service. (2012). *2010 Population and Housing Census.* Accra: Author.

Ghana News Agency. (2009). Ghana to set up cybercrime response team. http://ghanabusinessnews.com/2009/08/19/ghana-to-set-up-cyber-crime-response-team/

Guillaume, L. F. (2009). Fighting Cybercrime: Technical, Juridical and Ethical Challenges. *Virus Bulletin Conference.*

Halder, D., & Aishankar, K. (2011). *Cyber crime and the Victimization of Women: Laws, Rights, and Regulations.* Hershey, PA, USA: IGI Global.

Hansell, S. (2007). *Social network launches worldwide spam campaign* . New York: New York Times.

Hassan, B. A., Lass, D. F., Makinde, J. (2012). Cybercrime in Nigeria: Causes, Effects and the Way Out. ARPN Journal of Science and Technology, 2(7), pp. 626-629.

Holzer, H. J. (1991). The Spatial Mismatch Hypothesis: What Has the Evidence Shown. Urban Studies, Vol. 28, pp. 105–22.

International Telecommunications Union. (2008). Africa, ICT Indicators 2007, ITU World Telecommunication/ICT Indicators Database, Geneva.

International Telecommunications Union. (2007). *ICT Statistics Database*. Geneva: ITU.

Lipsey, R. G., & Chrystal, A. (2007). Economics (Eleventh Ed.). Oxford: Oxford University Press.

Longe & Chiemeke, S. (2006). The Design and Implementation of An E-Mail Encryptor for Combating Internet Spam. In Proceedings of the 1st International Conference of the International Institute of Mathematics and Computer Sciences, June Covenant University, Ota, Nigeria, 1 - 7.

Longe, O., Ngwa, O., Wada, F., Mbarika, V., & 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.

Magele, T. (2005). E-security in South Africa, White Paper prepared for the ForgeAhead e-Security event. Retrieved October 22, 2009.

Mbaskei, M. O. (2008). *Cybercrimes: Effect on Youth Development.*

Meke, E. S. N. (2012). *"Urbanization and Cyber Crime in Nigeria: Causes and Consequences".*

Merton, R. K. (1968). *Social Theory and Social Structure* (1968 enlarged Ed.). New York, NY, US: Free Press.

Morgan, D. L. & Kreuger, R. A. (1993). 'When to use focus groups and why' in Morgan D.L. (Ed.) *Successful Focus Groups*. London: Sage.

Okeshola, B. F. & Adeta, K. A. (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.*

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

Pickard, A., J. *(2007). Research methods in information.* London: Facet Publishing.

Plot, J. (2010). *Top five computer crime and how to protect yourself from them.* Publication of Justin plot.

Reingold, D. A. (1999). Social Networks and the Employment Problem of the Urban Poor'. Urban Studies, Vol. 36, No. 11, pp. 1907–32.

Richardson, R. (2008). 2008 CSI Computer Crime and Security Survey, Computer Security Institute.

RSA. (2015). Cybercrime 2015: An Inside Look At The Changing Threat Landscape

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

Sharma, R. (2007). *Peeping into a hacker's mind. Can criminological theories explain hacking?* Social Science Research Network.

Shehu, Y. A. (2014). Emerging Issues in Cyber-Crime: Causes, Implications and Effects for the Legal Profession. *Online Journal of Social Sciences Research, 3 (7),* pp 169-180.

Warner, J. (2011). Understanding Cyber-Crime in Ghana: A View from Below. *International Journal of Cybercrime, Vol 5 (1):* 736–749.

Westby, J. R. (2003). International Guide to Combating Cyber Crime, American Bar Association, Section of Science and Technology Law, Chicago, IL.

Young Entrepreneurs Sphere. (2012). [Online Article]. Available in http://www.yessphere.com/atit/.

Zenou, Y. (2000). Urban Unemployment, Agglomeration and Transportation Policies. *Journal of Public Economics, Vol. 77,* pp. 97–133.

Appendix I

HOUSEHOLD QUESTIONNAIRE

I am a post-graduate student of the University of Ghana, undertaking **An Investigation Of Youth In Cybercrime In The Ayawaso East Constituency Of Greater Accra**. This study is part of the requirements leading to the award of a Master of Arts Degree in Social Policy Studies. You are assured that the information you provide will be treated as confidential and used for academic purposes only. Thank you.

INSTRUCTION: Please tick/mark (v) in the box and write where necessary.

SECTION A: GENERAL BACKGROUND OF RESPONDENT

1. Gender: a. Male ( ) b. Female ( )

2. Age: …….

3. Marital status: a. b. Single ( ) c. Married ( ) d. Separated ( ) e. Divorced ( ) f. Widowed ( )

4. Educational level: a. None/No schooling ( ) b. Basic ( ) c. Technical/Vocational School ( ) d. Secondary ( ) e. Tertiary ( ) e. No formal schooling ( )

5. What is your religion: a. Christianity ( ) b. Islam ( ) c. Traditionalist ( ) d. None of the above ( )

6. Place of origin (Where do you come from?): …….....

7. Ethnicity: Are you an, a. Ewe ( ) b. Ashanti ( ) c. Fante ( ) d. Ga e. Dagomba f. Dagati g. Frafra h. If none, specify ……..

8. Employment Status: What is your occupation (what work are you currently doing)?
   a. Specify …….....…
   b. Not working, Student ( ) c. Not working, looking for work ( ) d. Not ready to work ( )

9. Do you live within Ayawaso East Constituency**?** a. Yes ( ) b. No ( ) c. No idea ( )

SECTION B: FACTORS THAT DRIVE (PULL AND/OR PUSH) YOUTHS INTO CYBERCRIME

13. Kindly indicate the type of cybercrime that you think is commonly practiced in this Constituency?

a. Credit card crimes ( ) b. Social Network Scam ( ) c. Password sniffing ( ) d. Facebook hacking ( ) e. Other ( ) Please specify……...……

14. What are the factors or reasons that influence (push and/or pull) people to go into cybercrime practices (activities)? Kindly state all the possible answers below.

a) ……

b) ……

c) ……

d) ……

e) ……

f) ……

15. **Please if you are not engaged in cybercrime practices,** optionally, state or explain how you were able to manage or not influenced by the factors that indeed induced your colleagues into cybercrime practices?

a) ……

b) ……

c) ……

d) ……

e) ……

f) ……

g) ……..

SECTION C: The experiences of youths engaged in cybercrime with the Ghana law as cybercrime conflicts with Ghanaian laws. That is how those engaged in cybercrime are able to circumvent or protect themselves from Ghana cybercrime laws and police arrest.

15. Are you aware of any existing laws against cybercrime in Ghana?

a. Yes ( ) b. No ( ) c. Not Sure ( )

16. Please indicate below, any information on how those engaged cybercrime are able to avoid police arrest or circumvent the laws against cybercrime in Ghana. This is to identify how cybercriminals in their act are able to circumvent or protect themselves from Ghana cybercrime laws and police arrest. Kindly state all the possible answers below.

a) ……

b) ……

c) ……

d) ……

SECTION D: The state of intelligence and policy development to deal with cybercrime. That is, the extent of policing of cybercrime legislation to make it difficult to be involved in cybercrime

17. What is your view about the state of intelligence in combating cybercrime in **Ayawaso-East Constituency? Please state all if possible.**

a) ……

b) ……

c) ……

d) ……

18. Kindly give any advice against cybercrime in **Ayawaso-East Constituency**

……

……

Thank You

Appendix II

INTERVIEW GUIDE

I am a post-graduate student of the University of Ghana, undertaking **An Investigation Of Youth In Cybercrime In The Ayawaso East Constituency Of Greater Accra**. This study is part of the requirements leading to the award of a Master of Arts Degree in Social Policy Studies. You are assured that the information you provide will be treated as confidential and used for academic purposes only. Thank you.

Date: ……/……../…….. Duration: ……hr(s), …… min(s)/ ……..Days

EXPERT INTERVIEW

Participants (Interviewees):

One representative of Ghana Police Service-Cybercrime Units

Two Youth Association leaders in Ayawaso-East District

Two Opinion leaders—Assemblymen

Two Religious leaders—Iman/Pastor.

SECTION A: BACKGROUND INFORMATION OF RESPONDENT

1. Please describe yourself. (Age, profession, occupation, marital status, number of children, educational background, religion)

SECTION B: PERSPECTIVE OF CYBERCRIME

2. Is cybercrime prevalent is this Constituency?

3. How different is it from other forms of crime?

4. Do you think the youth in this Constituency engage in cybercrime?

5. What do you think are the main causes of these practices among the youth?

6. What are some of the cybercrimes you know that the youths in this Constituency practice?

SECTION C: FACTORS PROMOTING CYBERCRIME

7. What do you think are the main causes of these practices among the youth?

8. Are children also engaged in the practice of spending almost all their time at the internet cafe?

9. Do you think unemployment can cause the youth to engage in cybercrime. How?

SECTION D: POLICING OF CYBERCRIME

10. Mention some of the challenges you think are affecting policing of cybercrime.

11. Do you think policing cybercrime has prospects in this Constituency? How?

12. What do you think are the effect of cyber-crime practices in general and in terms of Ghana's reputation?

13. What do you think can be done to improve policing of cybercrime in this Constituency and Ghana in general?