KWAME NKRUMAH UNIVERSITY OF SCIENCE AND TECHNOLOGY
INSTITUTE OF DISTANCE LEARNING (IDL)
DEPARTMENT OF HISTORY AND POLITICAL STUDIES

THE CHALLENGES TO FIGHTING CYBER-CRIME IN GREATER ACCRA REGION OF GHANA

BY

WILLIAM KOFI APKALU AKPESEY

A thesis submitted to the History and Political Studies Department/ Institute of Distance Learning, Kwame Nkrumah University of Science and Technology, Kumasi in partial fulfilment of the requirements for the award of the degree of

Master of Public Administration

JUNE 2019

CERTIFICATION

I hereby declare that this submission is my own work towards the Master Programme and that, to the best of my knowledge, it contains no material previously published by another person nor material which has been accepted from the award of any other degree of the University, except where due acknowledgement has been made in the text.

William akpesey …… ……

Name of Student Signature Date

Certified by

Dr. Edward brenya …… ……..

Supervisor Signature Date

Certified by

Dr. George bob-millar…….. ……

Head of department Signature Date

ACKNOWLEDGEMENT

I am very grateful to God Almighty for his grace to complete this work. Dr. Edward Brenya, my supervisor helped me tremendously to complete this work, I am grateful to him for the maximum effort and commitment he put in to shape this thesis. May the grace of God be on him forever.

I am also indebted to Dr. Mohammed Abass, who taught us and whose encouragement and pieces of advice helped me carry on. I am grateful to Dr. Dramani Kipo-Sunyehzi whom I consulted many times before I started the course.

Finally, I am exceedingly grateful to my brother (Assistant Commissioner of Police Mr. Normesinu of Ghana Police Service, Accra) who supported me to complete this work on time, and to all my other siblings I am grateful.

DEDICATION

I dedicate this work to my wife Naomi Akpesey and lovely children Julius Akpesey, Patricia Akpesey, and Christian Akpesey for the support they have given me to complete this work on time. I am most grateful to them.

ABSTRACT

Cybercrime in all its forms is a growing worldwide phenomenon. As the frontiers of Information and Communication Technology (ICT) expand, so does the opportunity for dubious individuals and groups to engage in internet fraud. ICT has become essential to the operations of government, corporate institutions and individuals, but the benefits accruing from the growing access is being undermined by miscreants who are exploiting its capabilities to the detriment of others. This has tainted Ghana's reputation in the global environment. The crux of this thesis is to examine the challenges faced by the Ghana Police Service in fighting cybercrime.

The research was situated within the Accra metropolis and employed a quantitative method of data collection. Questionnaires were administered through multiple means i.e. in person and e-mail. A total of 298 police personnel were conveniently sampled with 198 questionnaires returned suggesting a 66.4% response rate.

The study revealed that the main issue confronting the Police Service is that the Service is logistically under-resourced in terms of internet facilities, computers and the necessary technology to track fraudsters. The study further found that inadequate training of unit personnel and difficulty in collaborating with Telecom service providers prove to be challenges confronting the Police Service in fighting cybercrime.

The study also revealed that online romance fraud, mobile phone fraud, US visa lottery scam and Rent apartment scam accounted for some of the highest cases of internet fraud. the research ends with the recommendation that institutions of state especially the Attorney General's office should set schedule for reviewing the existing laws to address the peculiarities of cybercrime offences as well as drawing a legal framework to cater for the protection of the country's cyberspace.

TABLE OF CONTENT

LIST OF TABLES

CHAPTER ONE

INTRODUCTION

1.0 Introduction

Every effective criminal justice system thrives on a functioning and responsive police service and many of the impediments judicial services in developing countries are confronted with directly affect the police force on a daily basis. Ever increasing population growth rates, increasing spate of crime faced by an under resourced police service conspire to make crime prevention, detection and investigation a difficult one. A police force already overstretched by the resurgence of international crime, such as the illegal drug trafficking, money laundering, and terrorism has to contend with a relatively new form of criminal activity called cybercrime. Sinrod and Reilly (2000) notes that cybercrime across the world has actually grown with rapid development in information technology and the use of the internet.

Cybercrime is defined by the oxford dictionary as a crime that involves a computer either being the object of the crime (hacking, spamming, and phishing) or deployed as a tool to commit an offense (child pornography, internet fraud, hate crimes,). The online dictionary of technology suggests that cybercriminals may use computer technology to access personal information, business trade secrets or use the internet for exploitative or malicious purposes. Criminals can also use computers for communication and document or data storage. Criminals who perform these illegal activities are sometimes referred to as hackers.

Sinrod, Reilly, (2000) distinguishes various forms of cybercrimes:

(a) Phishing: this involves using messages from fake email to unlawfully access an internet user's personal information. The internet user's information once

acquired could be used in identity theft or a misuse of the victim's personal information to malicious intent.

(b) Hacking: Hacking crimes is defined as computer user who intends to gain unauthorized access to another individual or company's computer system" (Sinrod, Reilly, 2000). Hackers are usually very specialized and skillful in computer applications. It therefore requires similar or superiors level of skillfulness in information technology to track and fight them off. Hackers are able to steal directly from banks and financial institutions. They may also hack into a nation's security installations and steal nationally classified information.

(c) Cracking: almost similar to hacking, cracker seeks to gain access to other people or institution's computer systems. However, crackers are more vicious and aggressive in their aim of directly stealing information from victims' computer without their consent. Whitehouse (2015) observe that a combine team of well-versed well equipped crackers and hackers is capable of bringing a whole nation' security systems to a halt.

(d) Grooming: grooming entails making sexual advances to minors via the internet (Sinrod, Reilly 2000). Other forms of cybercrime include spreading hate and inciting terrorism; distributing child pornography; and engaging deceptive conversation with people via the social media with the view to defrauding them of their valuables such as money, jewelry or using their credit card details for unauthorized transactions.

Just like most of the police forces of ex-British colonies, in Africa, Ghana Police Force have its roots in the colonial forces, created with a mandate dominated by the need to stifle dissent and maintain colonial rule. Professional Policing in Ghana was born in 1821. Before then public law, order and peace was maintained by traditional

authorities including chiefs and community leaders through unpaid messengers. In 1894, the passing of the Police Ordinance gave legal backing for the formation of a Civil Police Force; now known as the Ghana Police Service. The Police Service Act, 1970 [Act 350] of Ghana states the functions of the current Ghana Police Service as: apprehension [arrest] and prosecution of offenders; maintenance of law and order; due enforcement of the law and crime detection and prevention. By this mandate, the Police Service is in fact the main enforcing agent of any policy relating to the public security.

Cybercrime is a growing phenomenon globally. Research show that cybercrime is increasing at a more rapid rate in Africa (including Ghana), than in any other area of the world (Symantec Corporation, Internet Security Threat Report [SCISTR] 2013). Indeed, experts of cybersecurity estimate that 80% of personal computers in Africa are plagued with viruses and other malicious software, leaving them widely exposed to cyber-attacks (Franz-Stefan 2010). Studies further reveal that in 2012 alone, there was a 42% increase in targeted cyberattacks in Africa. (SCISTR 2013).

In Ghana, Information and Communication Technology (ICT) is becoming essential to the operations of government, corporate institutions and individuals, but the benefits accruing from the growing access is being undermined by miscreants who are exploiting its capabilities to the detriment of others through cybercrime. It means that the Police Service must be in the position to effectively fight cybercrime. This study seeks to examine some the challenges the police face in fighting cybercrime.

1.2 Problem Statement

The Ghana Police Service is confronted with challenges in its effort to fight Cybercrime. However, the advantages obtained from the growing access and use of ICT is becoming increasingly undermined by miscreants, exploiting its capabilities to breach public security through cybercrime activities. In 2010, Ghana, a country long viewed as Africa's shining light, had its reputation soured. In a report published that year, Ghana gained the terrible distinction – along with West African neighbors Nigeria and Cameroon – as one of the top ten cybercrime generating states in the world (Danquah & Longe 2018). In its aim to effectively fight the cybercrime menace as expected of the main public security policy enforcing agent, the Ghana Police Service established the Police Cybercrime Unit as a specialized division. In spite of some success in fighting cybercrime, the service is faced with huge challenges some of which include low level of security provisions sufficient to prevent and control technological and informational risks; lack of technical know-how in terms of cybersecurity and inability to monitor and defend national networks, making the nation and individuals vulnerable to cyberespionage, as well as to incidences of cyberterrorism, inability to develop the necessary cybersecurity legal frameworks to fight cybercrime; and the fact that cyber-security concerns are broader in scope than national security concerns. This challenges jeopardized the security both at individual and national level. This study seeks to examine some the challenges the police face in fighting cybercrime.

1.3 Objectives of the Study

The study sought to achieve the following objectives:

1. Understand the socioeconomic characteristics of offenders and the victims,
2. identify the motivation that predispose the offenders to cybercrime,

3. Establish the various forms of cybercriminal activities in Ghana
4. Examine the responses and challenges of the Ghana Police Service to fight cybercrime.

1.4 Research Questions

The study would be guided by the following research questions:

1. What are the socioeconomic characteristics of offenders and the victims?
2. Which motivation predispose the offenders to cybercrime?
3. What are the various forms of cybercriminal activities in Ghana?
4. What are the responses and challenges of the Ghana Police Service to fighting cybercrime?

1.5 Justification

The consequences of unchecked cybercrime for any country can be damaging. As with the case of most crime forms, cybercrime has the potential to lower investor confidence, destroy a nation's reputation and deter foreign investment inflow.

Further, internet has become a major medium through businesses are transacted across the world. It therefore means that countries must equip themselves with the capacity to maintain a sanitized cyberspace; devoid of criminal activities.

Socially, the growth of cybercrime has the tendency to encourage more youth to drop out of school, shun the virtues of hard work, honesty and good citizenship, in unrelenting quest for quick but fraudulent gains.

In the mist of these concerns, it remains true that gathering digital evidence is fraught with several challenges, and requires special skill set and processes. This, and many other factors makes it difficult to fight some might term an unconventional crime

form, committed over the internet by rather savvy miscreants who would find it easy to outwit any untrained and ill equip security force.

The situation exposed above renders any research effort into the nature, forms, and problems of cybercrime a worthwhile academic endeavor. One way of minimizing criminal activities is when the chances of being apprehended are high, and when the cost of being found out are deterring enough. A study into the challenges of fighting cybercrime would identify lapses in the capacity to fight the crime and propose remedial measures to address the shortfalls.

1.6 Significance of the Study

A study in fighting cybercrime is significant in the following vein:

Governments across the world including Ghana are embracing e-governance, which rely heavily on ICT tools in policy implementation. This predisposes nation information systems to hackers and computer criminals. A study to examine the challenges to fighting cybercrime can deepen on understanding of the subject of cybersecurity.

Further, individual and businesses in today's world can hardly exist without using ICT. Addressing the challenges to fighting cybercrime could provide suggestions on more effective ways of protecting them from falling victims to crime.

The study of this nature would also make significant proposition which could help in fighting cybercrime in Ghana. Finally, the findings of this study add to existing literature of cyber security.

1.7 Scope and limitation

The study was carried out among personnel in the Greater Accra Region of Ghana exclusively. No data collected from any other region included. The study further limited in scope to its stated objective as indicated early on.

1.8 Organisation of the Study

This work is organized into five chapters. Chapter one discusses the background of the study, relates the problem statement, objectives of study and scope of study. The second chapter contains the literature review. This chapter outlines the conceptual and theoretical framework on the subject of public security; aspects and dynamics of crime and cybercrime prevention within the context of security policy.

Chapter three details the research methodology, the research design which was used for the study. The various sources of data are also discussed in this chapter; the instrument employed for primary data collection was further explained. Chapter further looks at the study population and sample size as well as the sample techniques. Chapter four presents an analysis of the result obtained relates these findings to prior studies to either confirm or refute the theories, concepts and propositions related in literature. Lastly, chapter five gives a summary of main findings from the analysis and the conclusions arrived at from the results. The chapter concludes with the proposition of some recommendations premised on the findings.

CHAPTER TWO

LITERATURE REVIEW

2.0 Introduction

The study sought to assess the challenges involved in fighting cybercrime in Accra. This section presents a review of literature on previous studies carried out in relation to the subject. In doing so, this section discusses thoughts on technology of crime, some contemporary views on change and crime, types of crime, consequences of crime for society and a brief history of cybercrime in Ghana.

2.1 Classical Thinkers on Technology and Crime

Academia has been inundated with a wide array of sociological thought on social order, the impact of science and technology and crime in society generally. It is prudent to highlight the various debates and viewpoints on this issue as a precursor to the review of the already existing body of knowledge on technology and crime. In making an assessment of the positivist approach to social thought, Durkheim concluded that higher rates of crime are inherently imbued in modern society. He then characterizes crime as 'functional' because it requires a standard form of societal action to find a common remedy to crime. Karl Marx reasons that the rise of crime is symptomatic of the various contradictions within capitalism. Weber views society through a lens of rationality which is built on foundations of logic and efficiency rather than a moral order or tradition. A contemporary society thus is any society which has experienced an emergence of a specialization in technology, change in its social structure and new forms of crime. It is then clear that the classical thinkers argued their positions on technology, crime and its societal implications based on concerns about the social alterations resulting from a rise in technology.

2.2 Modern Thinkers on Modernity, Technology and Crime

Merton (1968) reasons that 'anomie' is a condition occurring when there is an inconsistency or discord between societal goals and the means of attaining such goals. This then results in inconsistency between the ends and means that produce the various forms of behavior in the acceptance or rejection of the means and goals which can also be seen as innovations. Despite the fact that the rapid growth of technology has some very relevant functions, it has also invariably culminated into some regrettably undesirable ramifications such as cybercrime.

Giddens (1991) brings a whole new dimension of modernity by referring to it as a 'Juggernaut Engine', which totally collapses with no effective and efficient human control over it. Both the trust mechanisms (symbolic tokens and expert system) that have a close association with modernity and its distinctive 'risk profile' are always a threat to our trust and leads to insecurity.

Beck (1992) describes the modern society as being made up of both industrial and risk elements. The unrestrained use of technology has its risks associated which are yet not readily identifiable. Owing to the complex nature of society and technological advancement, newer forms of crime especially cybercrime have brought forth new types of risk for persons, organizations and the entire human society.

Castells (1996) emphasizes the importance of technology to human society when he stated that "Technology is neither good nor bad, nor is it neutral, it is a force". Technology has led to a once industrial social structure to one that is network in nature. Network Society is premised on a series of intercommunication among people globally. It has however also caused an ever increasing incidence of 'Organized global crime'. It has worn away the complexities associated with organized crime that

existed in earlier times. Wall (2001) discusses a modern form of technology that generates great anxiety. He views the internet as a concept that has its roots from the media. It is therefore the responsibility of criminologists to fully have a grasp of the behavior that it describes and to assist the understanding of others. The internet holds influence over the criminal and crime in three main ways; first, the internet is a medium of communication which shores up existing patterns of harmful activity such as drug trafficking. Second, the internet has created an environment that fosters criminal activity across borders providing new opportunity for criminals in the process and finally, is the nature of the virtual environment particularly with regard to the way that it merged time and space. Wall highlights the negative use of technology but fails to provide possible measures of fighting the ills of it.

Yar (2006) provides a concise view of cybercrime. Newer forms of crime are increasing at a rapid pace and old crimes disappear or are modified in terms of operation and what counts as a crime is relative to the social context within which it happens. As Majid Yar highlights, 'academic criminology has been slow to reorient itself to developments arising in the cyber world'. Having discussed at length the rise and growth of the internet and its role in everyday activities, the degree of its influence on cybercriminal activities and the challenges associated with quantifying these activities, the author then identifies numerous ways in which cybercrime negatively affects society. Several types of cybercrime such as hacking, pornography, piracy, and online hate speech, e-frauds, identity theft etc. are discussed at large. One of the salient points raised by the author is that there cannot always be a clear line of distinction between crime and deviance in criminal inquiry. Cybercrime has presented new challenges for policing and criminal justice as it is not confined by territorial boundaries. Besides this, new problems arise because of resource constraints and

inadequate expertise. A very critical yet unanswered question by the author is whether information and communications technologies are conditions that either "enable" or "enhance" crime.

Jaishankar (2011) emphasizes the fact that several criminal justice systems lack a comprehensive and up-to-date knowledge on the modern realities of cybercrime. The author's 'Space Transition Theory' is important to understand cybercrime. Anonymity has further caused or likely to cause criminal behavior in virtual space. It has worsened to Deviance and Criminal Subculture within the internet space. Victimization in social networks especially adolescent victimization has been associated with the Routine Activity Theory and Lifestyle Theory. Teenagers explore new technologies because of the freedom associated with these technologies but it also makes them vulnerable to online crime. Although cyber bullying is discussed, it is done within a psychological framework and its social implications are not stated.

2.3 Typology of Cyber crime

Some authors such as Hawthorne and Klein (1999) have analyzed the growth of use of women in establishing a cyber-culture that portray females as cyber-sex objects. The authors discuss Pornography in depth as a social trauma. Pornography as an e-commerce product has been identified as the foremost crime on the internet. However, Klien and Hawthrone neglected other types of cybercrime. They just focused on the objectification of women and their use in cyber porn and neglect other issues related to cybercrime specially the abuse of social networks.

Other writers caution the use of pornography on the internet (Philip, 2001). According to him, so much emphasis has been placed on quite innocuous forms of adult content while issues as dangerous and vile as child pornography is circulated without

difficulty. While agencies and agents such as the media, politicians and law enforcers have responded rightly to the growing obscenity in internet use, these institutions have terribly failed at grasping the more serious form of the cyber market for child porn. The writer highlights the modern history of child porn, which dates from the 1960s with regard to breach in censorship law in this period. After examining various laws relating to pornography, he questioned the "democratization" of pornography and argues that policies outlined on pornography are incomprehensive and make room for a policy bypass on legal grounds and may rather do more harm than good. Even the more traditional ways and means for deterrence had little impact in this area. The author had little insight on how to eliminate child porn and rather left it at the mercy of society. While the role of society in the elimination of child porn is very crucial, the author neglects the relevance of the issue. High prejudice is rather conferred on technical and legal but not social aspects.

Clarke and Knake (2010) draws attention to Cyber terrorism. He warns that computer is an effective tool for 'Net War' as malicious software may be installed into a user's system from a distance without approval from the said user. Cyber terrorism goes beyond the physical scope or dimension of destruction but also leads to destruction of giant electrical generators, derailing of trains, burning of high power transmission lines, explosion of gas pipelines, crash of aircrafts, and malfunctioning of weapons. Cyber war has the potential to launch attack in any part of the world within electronic medium. Large-scale attacks are carried out from a distance due to the technological misuse in modern times. The author, though providing warning for this abuse was unable to provide probable solutions to cyber-attacks.

Observing the use of computers and the change in technology due to new advancements, Morris and Higgins (2010) caution the security of internet users and

relates this to rise of cybercrime. He also examines pornography which is very much rampant. He also develops a contextual framework on information flow on the international stage. He discusses hacking as based on technical virtuosity. He identifies the introduction of computer networking and the ever increasing popularity of the internet as the cause of hacking. Privacy is also an issue because of online transactions. Higgins suggests that efforts should be made in the future to safeguard information stored frequently in electronic media should be thoroughly analyzed. An education on technology usage and its abuse is very much essential in combating the recent increase in online related offenses.

Four major types of cybercrimes namely cyber deception/ theft, cyber violence, cyber porn and obscenity and cyber violence are identified by Holt and Bossler (2011). He discussed various theories of criminology in the light of changing patterns of crime. He examined hacking in its various forms. He also evaluated child pornography in the light of recent legal developments. In addition, he evaluates the laws which address cyber bullying, and cyber stalking. In his views, and for creating 'awareness' among the ordinary people, more research work is needed to educate those who frequently use the internet.

2.4 Effects of Technology and Cybercrime on Society

Kraut et al (1998), examines the socio-psychological effect of the Internet. He argued that the frequent use of Internet is directly related to a decline in interaction among family members and further decline in social association. Many scholars further argue that, social networking makes individuals introverts and drift them apart from genuine real life social interaction. Conversely, another school of thought argue that internet and social networking ensure better social association. Kraut does a comparison of the Internet and the television. He stated that though both are primarily tools of

entertainment and information that enhance the development of new skills and confidence, the excessive use of the internet inversely reduces real interaction during leisure time with family since it is mostly time consuming. The findings of his study highlight that teenagers comparatively use the Internet for more hours than adults do. According to Kraut 'Greater use of the net shows a decline in social involvement'. Finally, he discusses the need of policy and technology interventions at individual and social level for better interpersonal communication.

People are increasingly relying on the internet because it is fast and easy to maintain contacts with others across borders (Mckenna and Bargh 2000). The authors point out the difference in interaction on the Internet from that in real life. Mckena and Bargh highlight four reasons for this; first, the possibility of staying anonymous on the Internet, second, the possibility of communicating across borders, third, the unimportance of physical appearance and visual cues and, fourth, the irrelevance of time on the Internet. They further make an assessment of the negative effects of the internet in conjunction the above stated. They asserted that anonymity of internet communication is an issue of great since researchers have found that people are more unrestricted about personal issues on the Internet than in face-to-face communication. Hate groups and racists use anonymity over the Internet as a tool for harassing minority groups by sending threatening e-mails and hateful messages. Looking at it from a different perspective, the internet provides the opportunity to engage in new roles and identity construction than is possible in the physical environment. Introverts turn to the internet as a means to develop and enhance social connections

Heuven et al (2003) opine that internet frauds and identity thefts have caused financial loss globally and is a challenge for a nation's infrastructure and security. Further, cyber criminals are using modern forms of technology to commit traditional crimes

online such as child pornography and pirated software. Counteractive laws and effective enforcement of those laws are needed to combat the attack viruses, hackers and terrorists. However, the authors failed to discuss the effects of cybercrime on society. They limited themselves to technical issues.

Brenner (2010) highlights the fact that individuals have limited knowledge about cyberspace crime. In modern times, cybercrime has direct implications on the lives of individuals, groups and the society at large. Cybercrime according Brenner argues is not a new form of crime. Online interaction leaves us exposed to cybercrime due to the fact that personal information is freely given out on the internet. Most importantly, the lack of effective legislation, law enforcement and security experts in the field of cybercrime makes us really vulnerable to cyber-attacks. However, the techniques which are employed to forestall computer intrusions are relatively ineffective as compared to the techniques used by cyber criminals. The author criticizes law enforcement agencies and neglects the possible use of technology to control cybercrime.

The history and growth of the information society and the internet is examined by Furnell (2002). He highlights various tools and skills employed in hacking and characterizes malware viruses and malware incidents. The author makes an observation of social, political and commercial impacts of hacking. He describes hackers as the members of an emerging subculture in modern society. He further points out the causes of the emergence of negative stereotypes of hackers. But Furnell failed to discuss the means and measures to control hacking.

Rege's (2009) paints a different picture of the internet that offers an alternative venue for romantic relationships. He examines online relationship because of four reasons;

first, people do not necessarily have to leave their homes or workplaces to be involved in a relationship. Secondly, the anonymous nature of the internet makes it possible for individuals to date privately. He further adds that people experience new forms of online dating such as chatting live and instant messaging like Yahoo chat. Finally, he is of the belief that internet usage for romantic relationships serves as perfect match because it leaves people with options to choose partners of their interest. There has been a proliferation of online dating sites since 1990s and it has emerged as the fourth highest earning industry on the internet after online gambling, digital music and video games. However, this successful industry is mutually exclusive from cyber-crimes. This article explains Romance Scams on the Internet in detail due to the fact that its breeds false obsession among victims. This does not only result in emotional distress but also costs lots of millions of dollars annually. Russian and Nigeria are renowned in this phenomenon due to their ability to manage fake and non-existent internet identities in luring victims. Victims experience a wide range of negative emotional and psychological harms such as anger, resentment, fear and depression. He concludes that if no effective measure is taken against cyber romance, it could be perpetuated, inevitably affecting the fabric of society. It therefore becomes necessary that control measures are devised to curb them.

Kluver and Qiu (2003) point out that the 'Net' has empowered communities and individuals to continually revise their identity. He posits that besides its technical functions, social and psychological functions are fulfilled via the internet. Asian countries are progressively using the internet for economic reasons. This has given rise to unanticipated consequences such as an ever increasing divide amongst social classes and nations simply because while a certain segment of society has access to digital resources, others are cut off from this. Those who do not have access to

technology see the people who have access to Internet and latest technologies as superior. And vice versa. The International Labor Organization recognizes the widening digital divide between and within countries.

2.5 Theoretical Review

Criminal behavior is a complex phenomenon. The factors responsible for criminal acts are not any simple in any instance. Criminologists in their quest to finding reasons why crime occurs, how it may be controlled or prevented have come up with several theories.

Around the nineteenth century, Cesare Lombroso, drawing heavily on earlier propositions by Charles Darwin, noted that those who commit regularly crime are primarily "atavistic" in their nature. In his view, Atavistic describes an individual who suffer from any form of mental retardation or under development.

Working as a prison psychologist in Italy, Cesare Lombroso asserted that criminals are criminals because it inherent or biological in their nature, that they are born that way; as some group of evolutionary throwbacks with distinctive features in their physical appearance including sloping foreheads, receding chins, tall and with square jaws.

Lambroso came to this conclusion after continually observing body types of prisoners with specific trait or features. Lambroso concluded that crime is a result of innate biological characteristic. Lambroso therefore conclude that criminals are born criminals.

His theory attracts several criticisms mainly because it paints a rather dismal picture of humans with specific physical characteristics. Furthermore, Lombroso's theory of

Biological Positivism in seeking to ascribe the cause of criminal behavior implies an observable distinction between non-offenders and offenders.

Several researches conducted to validate Lambroso's conclusions have failed to support the fact that it could be easy to identify individuals who may commit crime and those who do not (Travis Hirschi (1969; Richard Cloward and Lloyd Ohlin 1960; Lawrence Cohen and Marcus Felson 1979).

Subsequent theories after Lombroso rather analyze crime rather from social and environments circumstance and conditions (example the opportunity diffencial theory of Albert Cohen (1955); Anomie/Strain Theory by Robert Merton (1957); and the Social Disorganization Theory propounded by Clifford R. Shaw and Henry D. McKay (1942). However, a more adaptable theory to the examining the challenges in fighting cybercrime is the Routine Activity theory.

2.5.1 Routine Activity Theory

The present study is guided by the Routine Activity Theory (RAT), put forth by Lawrence Cohen and Marcus Felson in 1979. This is because beyond how and why crime occurs, RAT explains how crime can be combatted, fought or prevented.

In essence, the theory suggests that crime occurs when certain factors converge at the same place and space in time. According to the theory, crime occurs when there is an offender with the zeal to commit a criminal act, where there simultaneously exist an exposed and suitable prey or target, in the absence deterring factor (a police presence, a cctv camera, or a neighbor other persons) to interfere with the completion of the criminal act.

RAT theory assumes that the motivation to commit crime could result from variety of circumstances (for example when offender considers time as appropriate to engage in the criminal, or that the target is vulnerable or defenseless because there is no deterring factor to dissuade and prevent the crime from being completed). The suitability of a target is dependent upon the value to be acquired from robbing or killing weighted against the easy accessibility of the target and how visible the target is.

The theory further explained that, visibility as a conception made by the criminal to measure the gains (value) that may be acquired from carrying out the criminal activity whiles accessibility of target is an estimation of the vulnerability of the victim perceived by the offender. Cohen and Felson also introduced in their theory the third variable termed "Guardian" or Guardianship, which describes the presence of a deterring element or factor. For example, the presence of a law enforcement agent, applicable and effective laws to prosecute offenders, the installation of a crime surveillance system, or the presence of people in the neighborhood.

The reason for using this theory stems from its suitability to the subject of this study. RAT provides solution to the very tittle of the present research on what challenges there may be to the fight against cybercrime in all three composing factors, (a motivated cybercriminal; the absence of police guardianship on the web space and a cybercrime victim who has or finds himself so exposed by his own presence online).

Additionally, the theory was employed in the study of how people are victimized be cyber-fraudsters. Reyns, Henson and Fisher (2011) found that vulnerability of victims is heightened when they spend ample time on the internet by signing up to more social networks as well as frequently updating their social network accounts. In other

words, when people make themselves easily accessible on the internet, they are render themselves liable valuable target largely due to the absence of the deterrent element (Ghana Police Service) on national cyberspace.

2.6 Conceptual Framework

This section examines the conceptualization of the challenges of the Ghana police service and their ability to promote effective policing.

2.6.1 Cybercrime in Ghana

The following section discuss particular socio-cultural phenomena which include Ghanaians'; the rise of Sakawa; and the underlying philosophies of social justice used to justify cyber-fraud – which have till this point, gone unconsidered. While these by no means constitute a complete list of the numerous realities that promote cybercrime in Ghana, they however are a useful initial point of investigation.

2.7 Cybercrime in Ghana: History, Trends, Nature, and Responses

In 2010, Ghana, having had a reputation for not being caught up in the throes of, had its reputation tarnished. In 2010 report, Ghana gained the bad image– along with Nigeria and Cameroon – as one of the top ten cybercrime generating states globally (Ghana, Nigeria cited, 2010). In addition, a prior report had revealed that Ghana was the second-most frequently blocked location by U.S. online retailers due to mistrust of fake orders from Internet scammers (Kwablah, 2009). To better understand just how one of the continent's flawless states fell victim to this menace, this section offers a broad representation of cybercrime activities in Ghana. It begins with a brief history of cybercrime in Ghana, it then details the three most common scamming activities, offers the profile of any typical scammer, and finally examines the ways in which the

Ghanaian state is attempting to fight this new development. Ultimately, this section gives a brief overview of the phenomenon.

Warner (2011) observes that as compared to other parts of the West African sub-region, cybercrime is a relatively new phenomenon in Ghana. Cyber-fraud was on the rise in the country between the years 1999 and 2000. During this period the nature of cybercrime was largely about credit card fraud, which was basically facilitated by porters at hotels who share Western visitors' credit card details with fraudsters. In these instances, Ghanaian scammers would access the number of Western credit cards, purchase items via the internet, and then have them shipped to Ghana. After 2004 however, credit card purchases over the internet have dropped significantly with new forms of internet fraud emerging through the use of "social engineering tactics" to hypnotize the potential victims.

Burrell (2008) avers that internet fraud/cybercrime otherwise known as scamming in Ghana emanate from a more harmless practice which involved writing to foreign "pen pals" via post. Some of the young people involved in this practice valued these relationships essentially as a strategy for realizing material gain. Consequently, the fraud that was in place from the pen pal exchanges at the time reflected how fraudsters drew on established patterns of communications to framing their operational strategies for economic gain. This practice continued until it was eventually replaced with the modern day internet fraud.

2.8 Forms of Cybercrime in Ghana

According to Warner (2011), there are three primary types of cybercrimes practised in Ghana. The first of these being identity theft. In this instance, Ghanaian fraudsters establish contact with their Western victims often via social networking sites like

Facebook or dating websites such as Badoo.com or eLove.com and communicate under the pretense of a false identity. This is the most usual case of fraud in identity fraud known as "romance fraud".

Close linked to the same tactic of false identity is the second form of cyber-fraud mostly perpetrated in Ghana- fake gold dealers. Having gained the reputation as the "Gold Coast" as a result of its colonial past, Ghana is well-known for its abundance of the ornament. The fraudsters advertise gold samples on the internet, they then offer highly competitive prices which are far below the selling price on the world market. According to Obiri-Yeboah (2013), the fraudsters generate fake licenses from the Geological Survey Department, Minerals Commission, Precious Mineral Market Company (PMMC), Affidavits and other documentation to lure their unsuspecting victims. In some instances, they are able to convince their victims into the country and then exhibit samples of genuine gold. They afterwards draft sale and purchase agreement to provide some form of legitimacy to their transaction.

The third type of cybercrime rife in Ghana is that of estate fraud. In such cases, the victims are not typically Westerners, but rather, Ghanaians resident in the Diaspora. Upon return to Ghana usually after retirement, these returnees usually require accommodation. As a result, new enterprises have emerged on the internet to cater for these wealthy Ghanaians' real estate needs. Several cases of fake construction firms have been reported whereby Ghanaians create advertisement on the internet purportedly specializing in housing for retirees returning to the country. Pictures of houses are displayed on the websites and the blueprints of the buildings sold to would-be retirees. Plots of land on which these houses would be built are then shown to the retirees. Later, building materials such as bags of cement and sand are shown to the retirees as proof of construction. After extorting a huge sum of money from these

distant clients, the company disappears, the website is shut down and the scammers nowhere to be found.

2.9 Policy and Legislative Responses to Cybercrime in Ghana

The emergence of technology and online communication has not only resulted in a dramatic increase in crime but has also culminated invariably in the emergence of what seems to be new varieties of criminal activities and these pose a great difficulty for legal systems, as well as for law enforcement agencies (Brenner, 2007). These new types of crime have left governments and the law enforcement agencies with many difficult questions. For instance, how does one draw a line of distinction between which cybercrime legal or illegal. How can cybercrime laws be enforced seeing as the relationship between the victim and perpetrator is largely virtual? The internet makes room for individuals to interact with each other across borders raising issues or questions of jurisdiction in administering justice. This section reviewed some laws that have been adopted to deal with cybercrime Ghana.

With cybercrime posing a real threat to the state and a total of $97 million lost annually to internet fraud and its related activities[1], the Ministry of Communication introduced some ccts to regulate the conduct of individuals in the cyber space. These Acts consist of Electronic Transactions Act, 2008 (Act 772), National Information Technology Agency Act, 2008 (Act 771), Data Protection Act, 2012 (Act 843), and some other provisions in the Criminal Code. The subsections that follow hint on the spirits and limitations of these acts.

[1] https://www.myjoyonline.com/business/2018/October-11th/ghana-loses-97m-to-cybercrime-in-2018.php

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

In December, 2008, The Parliament of Ghana passed the Electronic Transaction Bill into law. The main objective of this law was to secure the cyber space as a means of reducing crime incidence that may affect the ability of the citizens to create wealth.

The Act is divided into 12 clauses. These are electronic transactions, electronic government services, the certifying agency, consumer protection, protected computers and critical database, domain name registry, and appeal tribunal. Other clauses mentioned are: industry forum, the liability of service providers and intermediaries, cyber inspectors, cyber offences, and miscellaneous matters.

The law enforcement component of the law can be found in the tenth group of clauses which gives security agencies the power to, in the course of the execution of court warrants, seize a computer, electronic record, programme, information document or any item should they reasonably believe that an offence has been or is about to be committed (ETA 2008, Act 772, clause 98). The presentation of evidence by providers of wire or electronic communication services or a remote computing services may also be requested by law enforcement agencies pending the issuance of a Court Order (ETA 2008, Act 772, clause100). The Judiciary is also empowered, upon application by a law enforcement agency, "to order an electronic communication service provider to disclose the contents of an electronic communication, that is in transit, held, maintained or that has been in electronic storage in an electronic communications system, if the disclosure is relevant for the investigative purposes in the interest of national security" (ETA 2008, Act 772, clause 101). The scope of the enforcement of the Act is however limited by the area of jurisdiction as it is contained in clause 142 (2):

This Act applies if, for the offence in question:

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

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

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

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

By tradition, the legal jurisdiction involves territories within the scope of a country being defined by the limit of its boundaries. This territorial notion is ineffective to prosecute cybercriminals. To determine where cybercrime has been committed can be difficult since the perpetrators and the victim can be located in different countries. The offenders may also employ computer systems in different countries to target their victims.

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

The National Information Agency is a Ghanaian public institution established by Act 771 in 2008, as the ICT policy implementing arm of the Ministry of Communications. It has as its mandate the regulation and monitoring of activities of companies in the electronic industry to ensure quality information delivery and standard of efficiency. The agency is further empowered to offer accreditation to individuals who want to conduct legitimate businesses online.

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

a) Perform the functions of the certifying Agency established under the ETA, 2008 (Act 772).
b) Issue licences and ensure fair competition among licence holders in the cyber space.
c) Monitor, enforce and ensure effective compliance with the conditions contained in licences and tariffs; (National Information Technology Agency Act, NITA 2008:3).
d) Maintain registers for approval given for equipment used under the ETA, 2008 (772)
e) Establish quality of service indicators and reporting requirements that apply to the licence holders under the ETA.

It is worthy of note that fake websites are being created everyday by the internet and hackers continue to dupe innocent people without NITA detection or apprehension. This could be attributed to the inadequacy of skilled manpower or technically enabling environment to track perpetrators.

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

The Data Protection Act is a legislation in improving transparency in the cyberspace. The Data Protection Act 2012 (Act 843) was passed by parliament in 2012, to protect privacy of individual and personal data (Data Protection Act 843, 2012:5).

2.9.4 Criminal Offences Act, 1960 (Act, 29)

The growing usage of the internet in Ghana has opened up the country for new cyber-trading platforms which has given Ghanaians an opportunity to transact various

business operations. Despite the fact that the online portal serves as a medium for exchanging goods and services, most transactions take place offline. Consequently, certain sections of the Criminal Offences Act (29/30) are again mentioned in the Electronic Transactions Act (Act 772) in preferring charges against suspects of cybercrime. These Sections include: 20, 21, 23, 122, 124, 133, 137 among others.

Crimes captured under these Sections of the Criminal Offences Act 29 (60) which have been again metioned in the Electronic Transactions Act (Act 772) are offences which can at best be described as bailable and attract midler punishment which fails at deterring fraudsters.

Besides, Danquah and Longe (2011) opine that the laws under which individuals suspected of cybercrime are currently prosecuted have existed under the fraud laws established since 1960 which makes it possible for defense attorneys to often win and acquit their clients because some of the facts do not support the prosecutor's claims of evidence.

CHAPTER THREE

METHODOLOGY

3.0 Introduction

This study examines the various Challenges to Fighting Cyber-Crime in Greater Accra Region of Ghana. This chapter provides an explanation of the procedure followed in conducting the research. The section looks at the research designs and describes the population from which the sample was taken. Other headings discussed in this chapter include: the instruments used in collecting first hand data and the procedure employed to this end; the sampling techniques and sampling procedure; source from which data was gathered from and how the data was finally analysed to arrive at the research outcome.

3.1 Research design

In the view of Weidenborner and Caruso (2007), the research design primarily aims to ensure that evidences derived from a research work allows the researcher to address the research problem in an effective manner; without any ambiguity. Gathering data which is relevant to a social science research involve specifying the kind of proof required to evaluate a theory, test a program or to describe and assess the significance of an observed phenomenon (Sydney & Mugenda 2001). Weidenborner and Caruso (2007) refer to research design as the blueprint for the collection of relevant information relating to the research question and the measurement and examination of the same.

The research design therefore is a description of the plan chosen by the researcher to seamlessly merge the various steps and parts of research methodology in order to provide confidence that the research question will be adequately addressed. Sydney &

Mugenda (2001), notes that the research design dictates how the various components of the study methodology are pieced together and integrated to address the study objectives. The research design is determined by the nature of the research problem being investigated.

In the current study, a survey method is proposed. The rational for this method lies in the fact that surveys methods are suitable for describing the characteristics and views of a population (Baxter & Babbie, 2004 ;); in this the challenges as faced by Police Personnel responsible for fighting the menace of cybercrime.

3.2 Study Population

In the opinion of Persaud, (2010), a research population is an appropriate description of the group of items, individuals or phenomenon in whom the researcher is interested; and suggests the group from which samples may be drawn. According to Ghauri & Gronhaug (2008), the population of any study is the actual focus of the scientific enquiry, and represent the group to which the conclusion obtained from any research work can be generalized. As far as the present study is concerned, the population consisted of all Police Service Personnel in the Cybercrime Unit in Accra. A total of 1,279 servicemen form the cybercrime unit (Ghana Police Service Official Record 2017).

3.3 Sample and sampling method

Fraenkel & Wallen, (2006) notes that a sample is that finite part of a statistical population whose properties may be studied in order to obtain accurate and relevant information about the whole population. A sample must be selected in such a way that it represents and reflect the various characteristic of the population from which it is drawn. Ghauri & Gronhaug (2008), argue that when all factors are held equal, the

larger a sample size the more accurately it will reflect the population which is being studied. In fact, Fraenkel & Wallen, (2006) propose that sample size may be increased to make it more representative of the population from which it was drawn. However, sampling technique frequently used is to reduce sampling error is the Yamane sampling techniques. This study used this method in order to benefit from the benefit minimizing sampling error.

Thus: **n = N / (1 + Ne^2)**

Where

n= corrected sample size, N = population size, and e = Margin of error (MoE), e = 0.05.

Therefore:

1279 / (1 + 1279 (0.05^2)

= 1279 /4.3 = 297.44 ~ 298

The current study selects a sample size of 298 Police Personnel; conveniently sampled from the Cybercrime division of the Ghana Police Service in Accra.

Galvan (2013) indicates that the method is convenient in saving cost and time, and allows the researcher to focus on and select those elements in the population who are willing and available to provide responses needed to achieve the aims or objectives of the study. Further, convenient sampling may provide suitable means of carrying out preliminary studies as observed in Galvan (2013); Persaud (2010); and Weidenborner, & Caruso (2007).

3.4 Data Sources

In this study, two main sources of data were used. This is made up Primary Data and Secondary data. The term primary source is used broadly to embody all sources that are originally obtained first hand from the responses of participants included in the sample of the study. According to Sydney and Mugenda (2001), primary sources provide firsthand information that is closest to the object of study. This was sourced in the present study to collect views of what the challenges of fighting cybercrime in the Police Service are. Original reports of research found in academic journals detailing the methodology used in the research, in-depth descriptions, and discussions of the findings are considered primary sources of information. Primary data was gathered by means of survey type questionnaires administered to sampled of respondents as proposed in Sydney and Mugenda (2001). Weidenborner, & Caruso (2007) defines secondary data as information produce through the studies carried by researchers other than the present researcher. Weidenborner, & Caruso (2007) list census information, other information gathered by state institutions or government departments, records obtained from organisational archives and any other **data** that was originally collected for other research purposes or produced from other research endevours as secondary data. Secondary data was obtained by reviewing relevant literature on the subject of the study from articles from peer review journals, books, organizational records and other publicly available materials on the subject of cyber security.

3.5 Data Collection Instrument

Questionnaires made up of open-ended and close ended questions were designed to address the research questions of this study. As per Sydney and Mugenda (2001), open ended questions in a questionnaire provides room for participants to add further

information regarding their feeling, assessment and understanding of the subject of the study. By including open ended questions the study obtained in-depth information relating to the challenges faced by the Police Service in combating cyber-crime.

The inclusion of both open-ended and close-ended questions in the questionnaire was meant to allow respondents to both focus on specific research questions as well as provide respondents with opportunities to provide explanations to deep lying issues on the challenges posed to combatting cybercrime.

3.6 Data Collection Procedure

Designed questionnaires were pilot tested to identify and correct ambiguous questions. Subsequently, the questionnaire was administered to respondents, after their agreement is sought to include them in the study. The questionnaire was administered by multiple means: by email, and in –person. In view of the time constrains, the researcher obtained some assistance from friends and colleagues in administering the questionnaires in order to fast-track the data collection process. The multiple means of administration was to ensure a high return rate since this method would allow respondents to select the mean most convenient to them.

3.7 Method of Data Analysis

To ensure that the accuracy of the processed data, the researcher edited and cleanse the collected data before subjecting the data to analysis. Analysis was done electronically. Because of that it was important to first codify collected data from the field in order to facilitate imputing it into the data processing system. Although several electronic means of analyzing data are available, the researcher employed the use Statistical Package for Social Sciences (SPSS) for purposes of this analysis. Data was analyzed using both descriptive and inferential statistics where inferences were

drawn and descriptive statistics like frequencies of responses were used to give the results of the analysis. Open-ended responses were grouped according to themes, corresponding themes to the research objectives, they were subsequently coded and fed into data tool.

CHAPTER FOUR

ANALYSIS OF RESULT

4.0 Introduction

This study aimed to examine the challenges to fighting cybercrime by the Ghana Police Service. To achieve this aim, 298 Service Men from the Cybercrime Unit of the Ghana Police in the Greater Accra Region were sampled and made to respond to questionnaire. This section presents the result obtained from analyzing the data collected from respondents.

4.1 Response Rate

Table 4.1 Response Rate

Number of Questionnaire Administered	Number of questionnaire returned	Response Rate
298	198	66. 4 %

Source Field Data 2018

Of the 298 questionnaire administered, 198 was returned, giving a response rate of 66.4%. The data was therefore analyzed base on the data collected. It must be noted that while many of the service could not return their questionnaire in time, Fraenkel & Wallen, (2006) suggest that a 66.4% return rate was sufficient to answer the research questions.

4.2 Demographic Information of Servicemen

Table 4.2 Gender of Service personnel

Gender	Frequency	Percentage
Male	117	59.0%
Female	81	41.0%
Total	198	100%

Of the 198 respondents, 117 were men; representing 59% and 81 were women. This shows that there about 1.4 men to 1 woman in the cybercrime unit of the Ghana Police Service.

Table 4.3 Age of Service personnel

Age Group	Frequency	Percentage
30-35	57	28.8
36-40	74	37.4
41-45	26	13.1
46-50	27	13.6
51-55	5	2.5%
56-60	9	4.5%
Total	198	100

As could be seen in table 4.3, 28.8% of service personnel are between the ages of 30-35, 37.4% are between the ages of 36-40, and 13.1% are between the ages 41-45. Also 13.6% are between the age range of 46-50. Those in the age bracket of 51-55 formed 2.5% while 4.5% are between the ages of 56-60. The result show that over 66% of the servicemen in the cybercrime unit are below the age of 40. This shows a fairly youthful force in the cybercrime unit. This may prove beneficial for training and retraining purposes, as younger generation are often more amenable to changes than older persons.

Table 4.4 Educational Background of Personnel

Educational Achievement	**Frequency**	**Percentage**
SHS	21	10.6%
Technical/Vocational	8	4.0%
First Degree/HND	116	58.6%
Post Graduate/Master's Degree	51	25.8%
Doctorate Degree	2	1.0%
Total	**198**	**100%**

The educational background of service personnel in the cybercrime unit was also analyzed. It was found that 10.6% had completed Senior High School, 4.0% had

obtained either a technical or vocational qualification after Senior High School, 58.6% hold either a first degree or a National Higher Diploma, 25.8% hold some form of a postgraduate qualification, (either a postgraduate certificate or a postgraduate diploma) or a master's degree. Only 1% had a doctorate degree. It could be seen from the analysis that majority of the servicemen are well educated. About 80% are educated up to tertiary level, thus are well-placed to understand the nature of the cybercrime.

4.3 Responses and challenges of the Ghana Police Service to fight cybercrime

The cybercrime unit of the Ghana Police Service has served, since it was formed to fight the menace of cybercrime. Being the state agency most visible in the fight against crime, and the maintenance of law and order, the Ghana Police has the authority according to the Police Service Act (350) and 1992 constitution, article 200. The Police Service has the right to protect citizens and residents from loss of valuable and lives by detecting and preventing crime of any form, arresting and detaining suspects and conducting investigation which must lead to the conviction of guilty suspect and acquittal of suspect found to be innocent.

The challenge with this mandate is that cybercrime has introduced a new dimension to criminal activities in that it is not only local it has international dimension. A young man sitting in the comfort of his room in Nigeria, South Africa or the UK can defraud an unsuspecting young lady who is doing her business to put food on the table for her family.

In the advent of cybercrime, the police had not specially trained unit to deal with cybercrime. As a result, cybercrime had to be handled by a multiple Units within the Police Service such as the Visa Fraud Unit, the Commercial Crime Unit, the Legal

and Prosecution Unit and the Intelligent Unit. This situation of making several unit take charge for cybercrime although helped in many ways to fight the menace, the police service felt that cybercrime although has many of the characteristics of other crime forms, was peculiar in many respects. As a result a new unit, specifically dedicated to fighting cybercrime was created in response to the growing menace.

Some of the special features of the unit include specialized training and periodic refresher courses for the service men in the dynamics of fighting cybercrime. Also special training in online and internet scam is also provided periodically.

Out of the 198 police personnel of the cybercrime unit who responded to the questionnaire, 196 were of the view that the creation of a special unit was a good response to more effectively dealing with the menace. This figure represents 98.9%. It is therefore is an endorsement of what the police have done so far in the fight against cybercrime.

Number of respondents	Creation of a cybercrime Unit is Good Decision	Not a necessary Decision	Endorsement from Service personnel
198	196	2	98.9%

Summary

The menace of cybercrime is on the rise. Within its constitutional mandate, and the resources available for its operation, the Ghana Police has created the Cybercrime Unit of the service to combat the growing phenomenon. While some may see this responses as inadequate, a careful appreciation of the resource limitation of the Police Service provide some understanding that their effort has made some strides in the fight against cybercrime the existing challenges notwithstanding.

4.4 Challenges of fighting Cybercrime

In spite of the huge endorsement of the creation of special unit within the service, dedicated to fighting cybercrime, the unit is not without some major challenges. Below is a table showing some of the challenges identified by respondents from the Cybercrime Unit of the Police Service.

Table 4.5 Challenges of fighting Cybercrime

Challenge	Frequency	Ranking
Not enough Police Personnel	172	3rd
Absence of Internet facilities and computers to track and apprehend Offenders	181	1st
Absence of cybercrime-specific laws	103	5th
Inadequate training for Unit Personnel	178	2nd
Lack of technical know-how on the part of investigators of Cybercrime	120	6th
Difficulty in obtaining Collaboration from Telecom organization	162	4th

Challenges identified by personnel sampled from the cybercrime unit of the police service as main impediments to more efficiently combatting cybercrime in the region include: the small number of personnel within the cybercrime unit, the absence of internet facilities and computers to track offenders' activities online, absence or inadequacy of cybercrime specific laws, lack of technical know-how on the part of investigators, inadequate training and difficulty in obtaining information from collaborative organizations such as the telecommunication companies .

4.4.1 Absence of Internet facilities and computers to track and apprehend Offenders

Of all the challenges enumerated above, absence of internet facilities and related equipment has the most mention and therefore is seen as the most important challenge. Cybercrime is carried out mainly by use of internet. While it may be impossible to pre-empt criminal activities on the internet, an online presence by the unit is necessary to monitor the activities of fraudsters who use the internet as a mean to defraud others. The absence of equipment needed to track IP addresses of computers used in cyber-fraud in-order to detect their location and illegal activities carried with these computers is crucial in fighting the crime. 181 out of the 198 respondents identified this as a major challenge.

4.4.2 Inadequate training for Cybercrime Unit Personnel

Training is one important mean of improving the knowledge, skills and capacity of employees. Even though some training has been organized for unit in the past personnel are of the view that more training could have helped the unit in it crime fighting disposition. From the responses obtained from the sampled responding personnel of the unit, inadequate training ranked as the second most important challenge to fighting cybercrime in the country.

4.4.3 Not enough Police Personnel

As indicated earlier, cybercrime is growing exponentially. This means that if more service men are not enlisted into the unit, there will come a time where offenders will outnumber the personnel charged with combatting cybercrime. This concern reflect what was carried in the Ghana Police Annual Report of (2013), that the current population-police ration 847 to 1 police serviceman instead of the UN prescribed ratio of 500 persons to 1 policeman. The concern among personnel of the unit is that if

more personals are not recruited, the tendency for the unit to be overwhelmed by the sheer number of cases could create a slow pace in prosecution and serve as a disincentive to victims who wants to report crimes against them. With the rapid expansion in population and the growth in cybercrime, this challenge was seen by respondent as the third most important with 172 out of 189 mentioning it as a challenge faced in the fight against cybercrime.

4.4.4 Difficulty in obtaining Collaboration from Telecom Organization

Noted among the challenges, respondents also mentioned the difficulty they encounter in obtaining relevant information of evidential value from the telecommunication operators who when the need to do arise in investigating a cybercrime case. Under the current laws, police officers must first file an ex-parte motion in a court of competent jurisdiction specifying his intention to obtain such information from a telecommunication operator. This is followed by a swearing of affidavit by the investigator to back the motion. It is only after these two processes are completed that a court can order the telecommunication operator to make such information available. The whole procedure can take days, several weeks or even months before information is obtained. This makes cases lag in the courts and therefore frustrating for victims who must be encouraged by quick dispatch of justice. Respondents sited this as the 4th most important challenge facing the fight against cybercrime.

4.4.5 Absence of cybercrime-specific laws

Legal frameworks ought to dynamic. This is because they constitute the major tools with which criminals are penalized. Officers and men of the cybercrime unit intimated that when prosecuting cybercrime offenders sometimes there are not enough legal provision to base their prosecution on. This absence of specific legal bases, sufficient to prosecute cybercriminals makes it difficult to fight the crime. The over reliance by

the court system of conventional trial procedure where there must be a complainant, an accused and a prosecutor provides grounds for the judge to strike out a case in the absence of any party to the proceedings leaves many cyber-fraudsters of the legal hook. This is because, while the current criminal code can be interpreted to cover various crime forms, exact definition and provision for cybercrime is lacking. Respondent view this as the 5th most important challenge facing the fight against cybercrime.

4.4.6 Lack of technical know-how on the part of investigators of Cybercrime

The technical knowledge of how to investigate cybercrime by detecting, analyzing and retrieving finalized documentary evidence from personal digital assistants is extremely important for cybercrime investigating officer. However, training in such crucial skills is still below the level of sophistication exhibited by some cybercrime offenders. The recent update in the training content of the Ghana Police College is a welcome development and a credit to the hard work of police administrators in the country giving the level of resource availability. However, cybercrime is not covered in the update. Meanwhile, the complexity of the security threat posed by cybercrime calls for corresponding response from law enforcement agents especially in high-tech crime such as cybercrime where information can be altered by criminal in split seconds. Surprisingly, respondent rank this challenge as the least most important.

Summary

The study sought to assess the challenges hindering the fight against cybercrime. To achieve this objective, questionnaires were administered to 189 policemen of the newly created cybercrime unit of the police service. Participants identified challenges in a descending order of importance: absence of internet facilities and computers to

track and apprehend offenders, inadequate training for unit personnel, not enough police personnel, and difficulty in obtaining collaboration from telecom organization, absence of cybercrime-specific laws and lack of technical know-how on the part of investigators of cybercrime.

4.5 Socio Economic Characteristics Cybercrime offenders

Another objective of the study was to understand the socioeconomic characteristics of cybercrime offenders. The study is of the view that one good way of developing anti-crime disposition is to understand the background of offenders. The study therefore sought to collect information from Service personnel form the various divisional headquarters on the socioeconomic background of cybercrime offenders.

4.5.1 Age Group of Cybercrime Offernders

Table 4.6 Age Groups of Cybercrime Offenders (2013-2018)

Age Group	16-20	20-25	26-30	31-35	36-40	41-45	46-50	50 +	total
Number of Cases	103	159	161	132	87	59	43	18	762
Percentage	13.5 %	20.9%	21.1%	17.3%	11.4%	7.7%	5.6%	2.4%	100%

Source: Police Cybercrime Unit (2018)

From Table 4.6 above it can be observed that 13.5% of Cybercrime offenders fall within the age bracket of 16-20, 20.9% fall within the 20-25age group, 21.1% fall within the 26-30 age category, 17.3% are between the ages of 31-35, 11.4% fall within the age of 36-40, 7.7% are of the ages between 41-45, while only 5.6% are aged between 45-50. Finally, only 2.4% are fifty years old and above. It would appear that majority of cybercrime offenders are between the ages of 16-35. This age group accounts for 72.8% of all cybercrime offenders. This finding resonates with Smith (2011)'s position that cybercrime is mostly committed by the youth especially people between 18 to 24 years of age. One explanation could be that people in these age range are more internet savvy. Secondly it could be that Ghana's youth unemployment figure which stands at about

43% according to the Ghana Statistical Service (2010), could have lead many of these youths into cybercrime. From observation many of the youth find cybercrime a less risky crime to commit because the crime can be carried out in the hiding of their homes as compared to other crime forms which exposes them more to be caught by the law agents.

4.5.2 Marital Status of Cybercrime Offenders

Table 4.7 Marital Status of Cybercrime Offenders (2013-2018)

Status	Married	Single	Separated	Divorced	Total
Number	41	678	33	10	762
Percentage	5.4%	89.0%	4.3%	1.3%	100%

(Source: Cybercrime Unit 2018)

Results from Table 4.7 show that of the 762 cybercriminal cases reported, 678 representing 89% were single. 33 of them representing 4.3% have been married before but are separated, 41 representing 5.4% are married while 10 of them representing 1.3% are divorced. From the analysis, it can therefore be concluded that majority of cybercriminals are young and unmarried individuals.

4.5.3 Gender Distribution of Cybercrime Offenders

Table 4.8 Gender Distribution of Cybercrime Offenders

Gender	Male	Female	Total
Number	735	27	762
Percentage	96.5 %	3.5%	100%

(Source: Cybercrime Unit 2018)

From Table 4.8, the result indicates that majority of cybercrime offenders are males. From the total number of 762 cases, 735 representing 96.5% were males while 27 representing only 3.5% were females. This shows that young male adults are more likely to engage in cybercrime than their female counterparts. From observation it was realized that male are more subjected to the societal pressure of *"making it in life"* (a colloquial

term which indicate to became materially successful and affluent), than their female colleagues. This may have motivated young men who thought of cybercrime as an easy means of making money to indulge in this form of crime.

4.5.4 Educational Achievement of cybercrime Offenders

Table 4.9 Educational Achievement of Cybercrime Offenders

Highest Educational Level	Primary	JHS	SHS	HND/1st Degree/ Diploma	Post Graduate	No Formal Education	Total
Number	94	183	298	120	11	56	762
Percentage	12.3%	24.0%	39.1%	15.7%	1.4%	7.3%	100%

(Source: Cybercrime Unit 2018)

From the Table 4.9, it can be observed that majority of individual perpetrators of cybercrime are educated up to SHS level. They represent 298 out of the total reported cases of 762 constituting 39.1%. Those educated up to primary school form 12.3% of all cybercriminals while those schooled up to JHS level form 24.0%. Degree holders, Diploma or HND leavers form 15.7% of reported cybercrime offenders. Only 1.4% have postgraduate education while 7.3% had no formal education. Nukunya (1992) argues that formal education is not only an essential vehicle for the acquisition of wealth and power but also for prestige. Therefore, higher education gives market value which invariably put the person on a pedestal to earn a good income which in turn is a prerequisite for respectable life style and family. An interesting observation here is that those whose educational achievement is below tertiary level are more likely to indulge in cybercriminal activities. In all, they are involved in more than 80% of all cybercrime cases reported within Accra alone. It is also worthy to note that involvement turns to decrease with advancement in education only 1.4% of people educated beyond graduate level have been found to be involved in cybercrime activities. What this could suggest is

that with the right educational policies in place to encourage school going, cybercrime could be party minimized.

4.5.5 Religious affiliation of Cybercrime Offenders

Table 5.0 |Religious Affiliation of Cybercrime Offenders

Religious affiliation	Christian Orthodox	Christian Charismatic Pentecostal	Muslims	Traditional religious	Others	Total
Number	265	209	241	39	8	762
Percentage	34.8%	27.4%	31.6%	5.1%	1.0%	100%

Source: Cybercrime unit 2018

Form the result related in table 5.0 above, it was found that of 762 offenders, 265 said they belong to Orthodox Christian faith. The figure represents 34.8% of all cybercrime offenders. 209 representing 27.4 % noted that they belong to Christian Charismatic/Pentecostal religious faith. 241 representing 31.6% are Muslims, while 39 offenders representing 5.1% said they profess traditional religious faith. All other religions were categorized as others form only 1.0%. it is therefore safe to argue, at the risk of sounding controversial that more than 61% of cybercrime offenders are Christian or at least worship at a Christian religious center. Sadly some do not see cybercrime which they sometimes refer to as 419, a reference to the Bible verse in Philippians Chapter 4: 19 which reads " my God shall supply all your needs according to His riches in Glory" alluding to the supposition that many of them see cybercrime as a way for God to supply their need. However, it could be seen that the religious representation of cybercrime offenders reflect to large extent the religious affiliation distribution in the population of the country (Ghana Statistical Service 2010). Therefore to deduce that crime has no colour and no religions orientation is therefore a plausible proposition to make.

4.5.6 Employment Status of Cybercrime Offenders

Table 5.1 Employment Status of Cybercrime Offenders

Employmen Status	Unemployed	Self Employed	Business Owners	Private Sector Employee	Government Sector employee	Others	Total
Number	391	111	92	97	42	29	762
Percentage	51.3%	14.6%	12.0%	12.7%	5.5%	3.8%	100%

Source: Cybercrime Unit 2018

From the Table 5.1 above the employment status of cybercrime offenders was analysed. This was to provide information on their economic activities and earning potential. The study revealed that more than half of all cybercrime offenders are unemployed. By unemployed we mean that these offenders are not engaged in any other legitimate means of earing income. They rely solely on their criminal activities as means of subsistence. It was further observed that self-employed constitute the second largest groups of cybercrime offenders. They form close to 15% of all cybercrime offenders in the Greater Accra Region.

The results also show that government sector workers are less likely to indulge in cybercriminal activities. They are responsible for only 5.5% of reported cybercrime offenses as compared with the private 24.7%, and 65.9% for the informal sector. The results indicate that largely, poor or precarious employment situation could be a major motivator for engaging in cybercrime offenses.

Summary

With respect to the first objective of this study, which was to find the socioeconomic background of cybercrime offenders it was observed, majority of cybercrime offenders fall between the ages of 16-35. This age group is responsible for 72.8% of all cybercrime offenses reported within the greater Accra Region. Secondly, the tendency to commit cybercrime is greater for those whose educational attainment is below the tertiary degree

level. Over 80% of those involved in cybercrime offenses are in these categories. People who claim affiliation to Christian religious beliefs were more than half of all cybercrime offenders. A little over 30% said they were Muslims whiles traditional religious believers form just over 5% of reported cybercrime cases. The study also found that government sector employees are less likely to engage in cybercriminal activities, 5.5% as against 24.7% for private sector employees, 14.6% for self-employed and 51.3% unemployed persons.

4.6 Motivation which predispose the offenders to cybercrime

The second object of this study was to find what motivates cybercrime offender to commit the crime.

4.6.1 Motivation for Indulging in cybercrime

Table 5.2 Motivation for Indulging in Cybercrime

Reasons For Crime	Frequency	Rank
Financial Gain	601	1st
To impress my peers	309	3rd
Not likely to be caught	166	6th
Lack of Parental Guidance & Control	129	
My friends said victims would not report to the police	413	2nd
It was easy to do	211	5th
I did not know it is also a crime	49	7th
To buy drugs	214	4th

Source: Cybercrime Unit 2018

Understanding what motivates cybercriminal to commit such act is useful for a number of reasons. First it exposes areas for police and security policy expert to focus on when initiating social intervention and associated preventive measures. Secondly it provides knowledge on potentially vulnerable risk that exists in a particular population to commit such criminal acts. To achieve this aim, the responses of the

cybercrime officers were grouped and categorized into various motivation factors for committing cybercrime. Their responses are illustrated in Table 4.8. From the table it could be seen that the most important motivation for committing the offense. This was followed by the thought that they could not be caught this creates some form of impunity among offenders. In reality, because of the perception that it easier to get caught when committing other crime forms than cybercrime which can be carried out in the hiding of one's home; offenders find it a "safer crime" to indulge in. A third most important motivator to committing cybercrime as indicated to the Police Personnel by the offenders is to impress one's peers. This was followed by the fact that many offenders are also illicit drug users of one kind or the order. Most prominent among the drugs they claim to use are crack cocaine and marijuana. The next most important motivator is the fact that cybercrime is easy to execute. It does not involve exposing oneself in the open and must easier to conceal. Other reasons found include lack of parental presence, guidance or control and the lack of knowledge of the implication of breaching cyber laws.

Summary

The study found that various reasons or motives are at the root of cyber offenses. These predisposing motivations can be grouped into the following categories: to obtain financial gains, impress peers, relative ease with which one can get away with the act, the absence of parental guidance, the impression that cybercrime victims often do not report the offense, and lack of knowledge of the legal implication of the act. Among these, financial gain was found to be the most important motivator of cybercrime offense while the lack of appreciation of the cybercrime laws is the least important motivators.

4.7 The various forms of cybercrime offenses committed in Accra

4.7.1 Bogus Business Proposals

In this kind of cyber-fraud, perpetrators post some seemingly extremely profitable business proposal online. The profitability of these supposed genuine proposals appear so tempting that victims initially want to keep it as a secret from others until they benefit from this proposals. Usually perpetrators in this crime will feign knowledge of the victim; who is a business man or woman. The offender will cook up a story of some product which they want to buy from the victim because their main supplier has stopped supplying them or cannot meet the offender's demand because of growth in demand of the product in a market foreign to the victim. The offenders vanish into thin air once the supplies are shipped by the victim.

4.7.2 Online Romance Fraud

Fraudsters in this kind of crime often offer romance to victims online. Through the internet the victims are engaged on social media site, online dating sites, chat rooms and other similar forum. The victims are then enticed into a supposed romantic relationship and swindled of their money and other valuables after offenders have chatted their way into the confidence and trust of their victims. One major way they do this is by asking victims to help with some part payment of some valuable item which the cybercriminal wants to purchase with the promise that the valuable will be delivered to the victims address so that the victim can help in selling them and keeping the whole or part of the money which is usually quoted to be far higher than the amount being requested from the victim. As would be expected this items are never delivered once the money transferred to the offender; who disappears and his contact number either changed or thrown away.

4.7.3 Vehicle marked “for sale” scam

In this type of cybercrime, a person selling his/her car online can be defrauded. Once the victim post his car online for sale and adds his contact number, the fraudsters will call and ask to know where the victim lives so that he can inspect the vehicle. The offender after inspecting the vehicle will direct a brother or friend who the offender will claim is living outside the country. The supposed brother will call and negotiate for the vehicle. This brother will suggest that in order to avoid payment of commission on transferring the money from abroad he has placed the money in a parcel through FedEx, DHL or any known courier service including the amount charged for dispatching the parcel and the amount for which the car is being sold for. The car owner must now pay the charges for the parcel in order to collect the parcel which the sender (who is part of the syndicate), has sent. A day or two later someone will call (also part of the gang), claiming to be a FedEx or DHL worker. The one whose vehicle is being bought will be asked by the Courier service worker to pay the amount for shipment in order to take delivery of the parcel which is supposed to contain money in payment for the vehicle he is selling plus the shipment fees which he must pay upfront. Once he pays this money all three (the buyer, his brother or friend abroad and the courier service worker)’s phone will go off.

In other cases, vehicles are posted for sale on the internet with a number to contact if you want to buy. When you call, you are likely to be told that the car is not in Accra so you must send some money through mobile money to a number registered with the identity of a dead person so they can drive the car to you in Accra because the car owner is either not having money because he has spent so much on an ailing mother or close relative at the hospital for which reason he want to sell the car. Once the money is sent the phone number goes off for good.

4.7.4 Mobile Phone Fraud

The recent number portability has created room for mobile phone users to change their network operators by porting their number. This has led to mobile phone operators to engage in aggressive marketing to retain their customer and win more customers. In this kind of fraud, a mobile phone user would receive a call from a fraudster who will claim that the recipient of his call has won a promotional award of given cash prize amount. In order to receive his prize the person must pay some amount usually less than the money won to have the prize processed. Obviously this always turns out to be a false pretender.

4.7.5 Rent apartment scam

As the use of internet grows in the country, various online trading platforms have been created by genuine business people to provide citizenry the facility to shop from the convenience of their homes including renting apartment. This help to cut the various middlemen in the chain between the tenant and the proprietors of apartments. However, this has also created opportunity for cyber-fraudsters to defraud victims who are looking form apartments to rent. Often victims who post their intention to rent an apartment with their contact details online may receive a call from a cybercriminal who will claim to have a place for rent at a rather cheap price; with the story that he the landlord (who is an offender) is urgently looking for money to pay a hospital bill or his ward's school fees. The unsuspecting victim is hurried to pay a rent advance often covering four years or more at that cheap price the victim who sees an opportunity to make a good deal pays the money only for the "landlord's" phone to become unavailable soon after.

4.7.6 US Visa Lottery Scam

Green Card Visa lottery, officially called the US Diversity Visa Lottery is a programme created by the US State Department to offer opportunity to individuals seeking to settle in US. Entrants are selected by a lottery means and given the US Green Card Resident Permit each year. Fraudster have taken advantage of Ghanaians eagerness to leave Ghana to more promising opportunity in the US to create fake US lottery sites and entice victims to pay various sums of amount to get them entered with near fail proof chances of winning the Visa Lottery.

Summary

Various types of cybercrimes are committed in Ghana. This study found that the major ones include online romance fraud, apartment rental fraud, bogus business cyber-fraud, mobile phone fraud, car sale fraud, and US visa Lottery scam.

CHAPTER FIVE

SUMMARY OF FINDINGS, CONCLUSIONS AND RECOMMENDATIONS

5.1 Summary of findings

With respect to the first objective of this study, which was to find the socioeconomic background of cybercrime offenders it was observed, majority of cybercrime offenders fall between the ages of 16-35. This age group is responsible for 72.8% of all cybercrime offenses reported within the greater Accra Region. Secondly, the tendency to commit cybercrime is greater for those whose educational attainment is below the tertiary degree level. Over 80% of those involved in cybercrime offenses are in these categories. People who claim affiliation to Christian religious beliefs form more than half of all cybercrime offenders. A little over 30% said they were Muslims whiles traditional religious believers form just over 5% of reported cybercrime cases. The study also found that government sector employees are less likely to engage in cybercriminal activities, 5.5% as against 24.7% for private sector employees, 14.6% for self-employed and 51.3% unemployed persons.

The study found that various reasons or motives are at the root of cyber offenses. These predisposing motivations can be grouped into the following categories: to obtain financial gains, impress peers, relative ease with which one can get away with the act, the absence of parental guidance, the impression that cybercrime victims often do not report the offense, and lack of knowledge of the legal implication of the act. Among these, financial gain was found to be the most important motivator of cybercrime offense while the lack of appreciation of the cybercrime laws is the least important motivators.

Various types of cybercrimes are committed in Ghana. This study found that the major ones include online romance fraud, apartment rental fraud, bogus business cyber-fraud, mobile phone fraud, car sale fraud, and US visa Lottery scam.

The menace of cybercrime is on the rise. Within its constitutional mandate, and the resources available for its operation, the Ghana Police has created the Cybercrime Unit of the service to combat the growing phenomenon. While some may see these responses as inadequate, a careful appreciation of the resource limitation of the Police Service provide some understanding that their effort has made some strides in the fight against cybercrime; the existing challenges notwithstanding.

The study sought to assess the challenges hindering the fight against cybercrime. To achieve this objective, questionnaires were administered to 198 policemen of the newly created cybercrime unit of the police service. Participants identified challenges in a descending order of importance: absence of internet facilities and computers to track and apprehend offenders, inadequate training for unit personnel, not enough police personnel, difficulty in obtaining collaboration from telecom organization, absence of cybercrime-specific laws and lack of technical know-how on the part of investigators of cybercrime.

5.2 Conclusions

Based on the findings, the study concludes 72% of cybercrime offenders in Ghana are of the age 16-35. Their educational achievements are below tertiary level, with majority being SHS leavers. The study also concludes that the higher a person's level of education, the less likely he/she is to indulge in cybercrime as people educate above graduate level constitute a small proportion of cybercrime offenders. The study also concludes that religious denomination has no significant impact on the tendency to commit cybercrime

as the proportion of each religious category reflect to a large extent the religious distribution of the country's population. The study concludes that majority of cyber fraudsters are in the informal sector where income is more unstable compared with the public sector which accounts for only 5.5% of cybercrime offenses. Finally, the study concludes that unemployment is a major cause of cybercrime involvement as the unemployed persons are involve in more than half of all cybercrime offences.

On the reasons which motivate people to commit cybercrime, the study concludes that several factors can motivate people to commit the act. Among them, financial gain was found to be the most important motivator of cybercrime offense while the lack of appreciation of the cybercrime laws is the least important motivators.

The study also concludes that the major forms of cybercrime include online romance fraud, apartment rental fraud, bogus business cyber-fraud, mobile phone fraud, car sale fraud, and US visa Lottery scam.

The study further concludes based on its finding that the Ghana Police has responded sufficiently to the cybercrime menace. Even though some challenges still persist. These challenges include: the absence of internet facilities and computers to track and apprehend offenders, inadequate training for unit personnel, not enough police personnel, and difficulty in obtaining collaboration from telecom organization, absence of cybercrime-specific laws and lack of technical know-how on the part of investigators of cybercrime.

5.3 Recommendations

Based on the conclusion reached in this study, the researcher proposes the following recommendations. The state authorities must explore opportunities for liaising with

the Attorney General to set schedules to review existing laws to address the peculiarities of cybercrime offenses as well as drawing up a legal framework to cater for the country's cyberspace. Such reviews should also address the procedural dimensions of cybercrime cases. This would make it easier for officials to prosecute offenders in court. This is necessary because part of the reason for the impunity of perpetrators of cybercrime is sometimes due to the ease with which they escape being penalized for the offense. There is also the need to develop a grand strategy to deal with the growing menace of cybercrime.

It is also recommended that the capacity of the cybercrime unit of the police service be adequately developed to empower them to fight the crime. Where necessary, the capacity building programmes should be provided for personnel of the unit. If our resources disposition can allow the government should explore programmes in advanced nations with unparalleled capacity and know-how in fighting cybercrime should be considered for members of the unit. The ICT skills of unit members should be horned and sharpen to match and exceed the sophistication of cybercriminals.

The government should seek avenues of mobilizing funding for the building ultra-modern digital forensic laboratory to address the data-management gap between the offenders and the unit.

Government must further make education accessible and affordable to the less privilege since the tendency to engage in cybercrime has been seen to diminish with higher attainment of educational standard.

Finally, the state should motivate and incentivize Non-Governmental Organizations, Religious bodies, civil society groups to go into training the youth in employable

skills. This should complement the government's effort in providing means of lively hood to the teaming youth. As seen from the study cybercrime is more prevalent among the unemployed and the youth whose major motivation for engaging in the criminal act is to gain some financial reward.

REFERENCES

Beck, U. (1992). *Risk society: Towards a new modernity*. London: Sage Publications.

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

Castells, M. (1996). *The rise of the network society*. Malden, Mass: Blackwell Publishers.

Clarke, R. A., & Knake, R. K. (2010). *Cyber war: The next threat to national security and what to do about it*. New York: Ecco.

Cohen, L., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review, 44*(4), 588-608. Retrieved from http://www.jstor.org/stable/2094589

Danquah, P., & Longe, O. B. (2011). An Empirical Test of the Space Transition Theory of Cyber Criminality: The Case of Ghana and Beyond. African Journal of Computing & ICTs. 4(2), 37-48. Retrieved Feb 14, 2018 from http://ajcict.net/uploads

Danquah, P., & Longe, O. B. (2011). An Empirical Test of the Space Transition Theory of Cyber Criminality: The Case of Ghana and Beyond. *African Journal of Computing & ICTs*. 4(2), 37-48. Retrieved August 14, 2011 from http://ajcict.net/uploads/Danquah___Longe__An_Empirical_Test_Of_The_Space_Transition_Theory_of_Cyber_Criminality_-_The_Case_of_Ghana_and_Beyond.pdf

Durkheim, E. (1951 [1897]). *Suicide: A Study in Sociology*. Trans. J.A. Spaulding & G. Simpson. New York: The Free Press.

Durkheim, E. (1984 [1893]). *The Division of Labour in Society*. Trans. W.D. Halls. New York: The Free Press.

Fowler, F.J. (2002). *Survey research methods.* Thousand Oaks, CA: Sage Publications.

Fraenkel, J.R., & Wallen, N.E. (2006). *How to design and evaluate research in education.* New York: McGraw-Hill. Popham, W.J. (1993). *Educational evaluation. Needham Heights,*

Franz-Stefan Gacy, "Foreign policy: Africa's internet threat", National Public Radio, 29 March 2010. Available from www.npr.org/templates/story/story.php?storyId=125297426

Furnell, S. (2005). Internet threats to end-users: Hunting easy prey. Network Security, 2005(7), 5-9. doi:10.1016/S1353-4858(05)70258-0

Galvan, J. L. (2013). *Writing literature reviews: A guide for students of the social and behavioral sciences.* Glendale, CA: Pyrczak.

Galvan, J. L. (2013). *Writing literature reviews: A guide for students of the social and behavioral sciences.* Glendale, CA: Pyrczak.

Ghana Police Service: 2013 Annual Report.

Ghauri, P & Gronhaug, K (2008) Research Methods in Business Studies (4th Edition) Princeton Hall, New York.

Giddens, A. (1991). *Modernity and self-identity: Self and society in the late modern age*. Cambridge, UK: Polity Press.

Hawthorne, S., & Klein, R. (1999). *Cyberfeminism: Connectivity, critique and creativity*. North Melbourne: Spinifex Press.

Heuven, M.V, Spiegeleire, S.D., Botterman, M. (2003). *Managing New Issues: Cyber Security in an Era of Technological Change* [Kindle Edition] Rand.

Holt, T., & Blossler (2009). "Examining the applicability of lifestyle-routine activities theory for cybercrime victimization". *Deviant Behavior*, 30, 1-35.

K, Jaishankar (Ed.) (2011). *Cyber Criminology: Exploring Internet Crimes and Criminal behavior.* Boca Raton, FL, USA: CRC Press, Taylor and Francis

Kluver, R., & Qiu, J. L. (2003). China, the Internet and Democracy. In I. Banerjee (Eds.), Rhetoric and Reality: The Internet Challenge for Democracy in Asia (pp. 26-60). Singapore: Eastern University Press.

Kraut, R., Patterson, M., Lundmark, V., Kiesler, S., Mukophadhyay, T., & Scherlis, W. (1998). Internet paradox: A social technology that reduces social involvement and psychological well-being? *American Psychologist, 53*(9), 1017-1031.

Kwablah, E. (2009). Cybercrime: Giving a bad name to Ghana. Ghana Business News. Retrieved 20th March 2018, from http://www.ghanabusinessnews.com/2009/02/17/cybercrime-giving-a-bad-name-toghana/.

McKenna, K. Y. A., & Bargh, J. A. (2000). Plan 9 from cyberspace: The implications of the Internet for personality and social psychology. *Personality and Social Psychology Review, 4*(1), 57-75.

Merton, R. K. (1968). *Social theory and social structure*. New York: Free Press

Morris R. G., and Higgins G. E. (2010). Criminological Theory in the Digital Age: The Case of Social Learning Theory and Digital Piracy. *Journal of Criminal Justice* 38: 470-480.

Nukunya, G. K. (1992). Tradition and Change in Ghana: An Introduction to Sociology. Accra: Ghana Universities Press.

Persaud, N. (2010). *Primary data source. In N. Salkind (Ed.), Encyclopedia of research design.* (pp. 1095-1098). Thousand Oaks, CA: SAGE Publications, Inc

Rege, A. (2009). What's Love Got to Do with It? Exploring Online Dating Scams and Identity Fraud. *International Journal of Cyber Criminology*, 3(2), 494-512.

Reyns, B. & Henson, B. & Fisher, B. (2011). Being Pursued Online: Applying Cyberlifestyle–Routine Activities Theory to Cyberstalking Victimization. Criminal Justice and Behavior - *CRIM JUSTICE BEHAV*. 38. 1149-1169. 10.1177/0093854811421448.

Secondary Source. (2005). *In W. Paul Vogt (Ed.), Dictionary of Statistics &. Methodology.* (3rd ed., p. 291). Thousand Oaks, CA: SAGE Publications, Inc

Sinrod, E.J. and Reilly W.P. (2000), *Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws*, 16 Santa Clara High Tech. L.J. 177.

Sydney, E. A. & Mugenda L.A., (2001). *Research methods: quantitative and qualitative approaches*. Aldershot: Ashgate

Symantec Corporation, Internet Security Threat Report 2013, 2012 Trends, Volume 18, accessed 13th March, 2018). Available from www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.enus.pdf.

UNODC (2013). Comprehensive Study on Cybercrime. New York: UN

Wall, D. S. (2001). *Crime and the Internet*. London: Routledge.

Weidenborner, S., & Caruso, D. (2007). *Writing research papers: A guide to the process.* New York: St. Martin's Press

Yar, M. (2006). *Cybercrime and society*. London: SAGE Publications.

Appendix I

QUESTIONNAIRE

I am a post-graduate student of the Kwame Nkrumah University of Science and Technology, undertaking an **Investigation into the Challenges of Combatting Cybercrime**. This study is part of the requirements leading to the award of a Master of Public Administration Degree. 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 ……
……

SECTION B: Forms of cybercriminal activities in Ghana

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

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. <u>What are the Socio economic background of victims of Cybercrime?</u>

a) ……

b) …….

c) ……..

d) ……..

e) ……

f) …….

g) ……

16. <u>What are the Socio economic background of perpetrators of Cybercrime?</u>

a) ……

b) …….

c) ……..

d) ……..

e) ……

f) …….

g) ……

SECTION C: The experiences of people 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: What are some of the challenges you face in combating cybercrime? **Please state all if possible.**

a) ……
b) ……
c) ……

d) ……

18. Kindly give any advice on how to fight cybercrime in **Accra**

……

……