UNIVERSITY OF GHANA

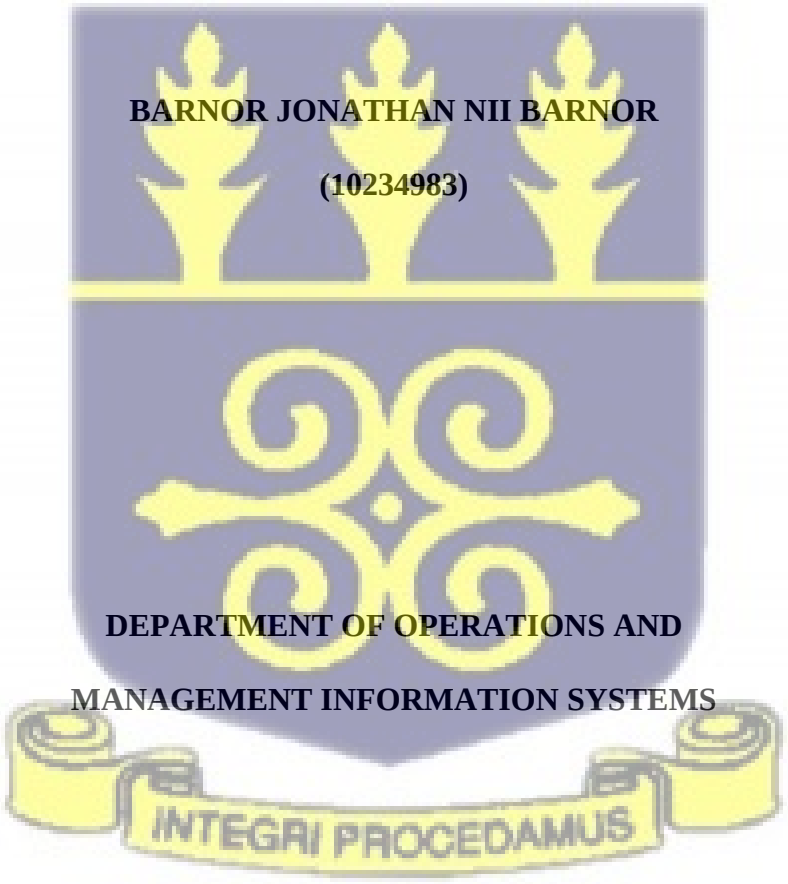
COLLEGE OF HUMANITIES

UNDERSTANDING ABILITY, OPPORTUNITY, AND MOTIVATION RATIONALISATION IN ONLINE ROMANCE SCAMS

BARNOR JONATHAN NII BARNOR

(10234983)

DEPARTMENT OF OPERATIONS AND MANAGEMENT INFORMATION SYSTEMS



FEBRUARY 2023

UNIVERSITY OF GHANA

COLLEGE OF HUMANITIES

UNIVERSITY OF GHANA BUSINESS SCHOOL

UNDERSTANDING ABILITY, OPPORTUNITY, AND MOTIVATION RATIONALISATION IN ONLINE ROMANCE SCAMS

BARNOR JONATHAN NII BARNOR

(10234983)

THIS THESIS IS SUBMITTED TO THE UNIVERSITY OF GHANA, LEGON, IN PARTIAL FULFILMENT OF THE REQUIREMENT FOR THE AWARD OF A DOCTOR OF PHILOSOPHY IN INFORMATION SYSTEMS DEGREE

DEPARTMENT OF OPERATIONS AND MANAGEMENT INFORMATION SYSTEMS

FEBRUARY 2023

DECLARATION

I do hereby declare that this thesis is my own work produced from research I carried out under supervision. This thesis has not been presented by anyone for any academic award in this or any other institution. All references made to work done by other people have been duly acknowledged.

Barnor Jonathan Nii Barnor
(10234983)

16th February 2023
Date

..RICHARD BOATENG
(Lead Supervisor)

16th February 2023
Date

Dr Emmanuel Awuni Kolog
(Co-Supervisor)

16th February 2023
Date

Prof. Anthony Afful-Dadzie
(Co-Supervisor)

16th February 2023
Date

ABSTRACT

Advancements in information and communication technology (ICT) have made it easier for various public and private sectors to perform effectively. However, the growth in ICTs is accompanied by new and emerging challenges for people and countries to contend with, notably cybercrime. Cybercrime is described as the use of computers and computer-related technologies, which includes the internet, to commit crimes such as fraud, child pornography, identity theft, and invasion of privacy. Despite the borderless nature of these crimes, one type of crime reverberates in West Africa; online romance scams – a scheme in which scammers pretend to have genuine affection for victims in order to acquire their love and then use that goodwill to persuade the victims in order to exploit them.

While cyberspace in relation to cybercrimes is made up of three players – attackers, defence, and victims, extensive evaluation of literature shows a paucity of studies that consolidate evidence from the attackers' perspectives. It is, therefore, essential to investigate the triggers of attackers' behaviours in order to understand the mechanisms that unite to cause cybercrime to occur. The dearth of studies that take the perpetrators' dimension into perspective implies a lack of studies that explore their behavioural dynamics as well as the strategies they employ in exploiting their victims. As a result, this study developed three research objectives to fill these gaps. The first objective is to unearth the mechanisms that trigger cybercriminal behaviours. The second is to explore the dynamics of cybercriminal behaviours, and the third is to explore the strategies that online romance scammers employ in finding, priming, and defrauding their victims.

To achieve the study's objectives, this research consolidates three theories: Routine Activity Theory (RAT), Motivation-Opportunity-Ability (MOA) framework, and Neutralisation Theory (NT). The combination of these theories was in an effort to address their weaknesses in relation

to cybercrime studies. Based on existing fraud studies, this thesis operationalised the conditions that need to be present for a crime to take effect, leading to the development of a conceptual framework. To put this into perspective, the study draws on the tenets of critical realism and uses a qualitative single case study approach to investigate the activities of a cybercrime syndicate in Ghana. The choice for this approach was informed by the fact that using a single case study allows the researcher to question old theoretical relationships and investigate new ones, resulting in a more thorough study. As a site for such research, Ghana is not out of place, as sufficient anecdotal evidence indicates that the country, along with Nigeria, is one of the main hubs for West African scams.

The first research objective sought *to unearth the mechanisms that trigger cybercriminal behaviour*s. In this regard, four mechanisms were elicited through theoretical re-description and retroduction. These are motivation, opportunity, ability, and neutralisation. Concerning motivation, the study revealed an interplay of various socio-economic factors, including unemployment, low-level income, low-level education, and quick money syndrome, as the primary driving forces behind the commission of online romance scams. Regarding opportunity, the research found that online romance scam perpetrators take advantage of weaknesses in regulatory laws to commit romance scams. Concerning ability, the study pointed out two forms: social and technical abilities. A representational finding from this dimension indicated that scammers hold a high level of interactional social ability that aids them in keeping their victims believing seemingly legitimate truths, which turn out to be lies. Whereas ability is a trigger on its own, a leveraged ability becomes an opportunity when a technical ability is outsourced. Lastly, concerning their neutralisation strategies, this research suggested that perpetrators moderate the severity of their offences by engaging in selective social comparisons.

The second objective sought *to explore the behavioural dynamics of cybercriminal behaviours*. Findings in this regard brought to the fore three-stage behavioural dynamics: creation, maturation, and decline. The creation stage was noted in the study as the starting stage of an individual's ingress into the commission of online crimes. The research found that at this stage, cybercriminals possess little to no skills in committing cybercrimes and have no clear sense of direction. Perpetrators further graduate to the maturation stage when they begin to engage in carefully calculated multiplicity of internet crimes. While the maturation stage may last for a while, the decline stage sets in when perpetrators are unsuccessful in their fraud attempts due to an interplay of various factors, including security upgrades on dating and e-commerce platforms. Traditional and other forms of depravities also become attractive at this stage. These findings' uniqueness stems from the fact that cybercriminal behavioural dynamics in relation to romance scam seems unclear in prior literature, making this research perhaps one of the first.

The results of the third objective revealed two approaches that *cybercrime perpetrators employ in finding, priming, and defrauding their victims*. These included scammer-led and victim-led strategies. The scammer-led strategy involves instances where scammers pose as men and lead their victims (mostly females) into presumably romantic relationships that later turn out to be fake. While this approach has been featured in prior literature from the victims' point of view, this study exposed some key elements worthy of note. Such include the use of tests to ascertain the legitimacy of the relationships and the use of victims' addresses as a transit for shipping items obtained through e-commerce frauds. In the victim-led strategy, scammers pose as young ladies and allow victims (mostly males) to make demands in the form of naked photographs and webcam videos in exchange for money. Scammers who use this strategy sting their victims by blackmailing them. Again, this finding is unique because the victim-led approach in the

scammers' persuasive techniques has arguably not been documented in previous studies, making this study a pioneering one in that regard.

This research makes the following contributions in terms of research, theory, methodology, practice, and policy. The study contributes to research by expanding the romance scam persuasive techniques, which has hitherto been developed using data from victims and dating platforms. The study further contributes to theory by developing and empirically testing a conceptual framework on how romance scam perpetrators rationalise their motivation, opportunities, and abilities. This was done by combining the RAT, MOA, and NT. This was a necessary move in that it contributes to addressing the debate surrounding the RAT for its inability to comprehensively address online crimes and also its inability to explain why offenders become motivated to commit crimes. The development of the framework is not limited to romance scams, as it may serve as a reference framework for studying other forms of online crimes (e.g., cyberbullying, hacking, pharming, digital piracy, etc.). Concerning the study's contribution to methodology, this thesis aggregated primary evidence directly from romance scam perpetrators in an effort to ostensibly fill the gap in the lack of offender-side data representation in cybercrime literature. Regarding practice, this study presents rich information to developers and managers of dating platforms on the strategies online crime perpetrators employ to circumvent security features. Concerning policy, the study provides adequate information for law enforcement agencies and ISPs on the need for collaboration to combat cybercrime in Ghana and perhaps, West Africa. Notable outputs from this thesis are publications in two conference proceedings and two book chapter publications. One of the conference publications titled *"Rationalising Online Romance Fraud: In the Eyes of the Offender"* was nominated for the best paper award at the 2020 Americas Conference on Information Systems.

DEDICATION

To
My Wife & Daughters

ACKNOWLEDGMENT

All glory to God for every blessing and every trial, for they mould us into the people we were created to be. For us not to walk through this life alone, He brings good people our way. People like these have a variety of effects on our lives, and some of them are mentioned below.

I would like to acknowledge my indebtedness and render my warmest appreciation to my lead supervisor, Prof. Richard Boateng, whose guidance made this work possible. I am particularly appreciative of your unique approach to supervision. I value your comments and advice during our interactions for the completion of this thesis – ***you are a bundle of wonder—a marvel of surprises and a heart of preciousness beyond diamonds***. I am also extremely grateful to my co-supervisors, Dr Anthony Afful-Dadzie and Dr Emmanuel Awuni Kolog. Your in-depth and insightful feedback significantly improved the study.

I am particularly grateful to my family for the prayers, support, inspiration and encouragement for me to get this far. I am thankful to everyone who has helped me achieve this goal in various ways, especially Dr Sheena Lovia Boateng, for your constant motivation, unwavering support, and guidance during the study. To Edward Entee and my year group, God bless you all.

I appreciate the time and effort put in by my data respondents and everyone else who reviewed and validated the interview guide for this project. Among those who helped me out were DSP Freeman Tettey, who was instrumental when I needed access to the Ghana Police Service so I could collect data and ACP Dr Herbert Yankson, who was very kind to me as a respondent for this study. I also appreciate the efforts of lawyers at Kuenyehia and Nutsukpui, Labone in helping collect data in the firm. I am unable to mention all names, but to all who read portions of this work and made corrections, your efforts have not gone unnoticed.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

ACCC	-	Australian Competition and Consumer Commission
AFF	-	Advance Fee Fraud
BNI	-	Bureau of National Investigations
COC	-	Convention on Cybercrime
CR	-	Critical Realism
DDOS	-	Distributed Denial of Service
ECOWAS	-	Economic Community of West African States
FIC	-	Financial Intelligence Centre
ICT	-	Information and Communications Technology
IS	-	Information Systems
ISP	-	Internet Service Providers
IT	-	Information Technology
MISQ	-	Management Information Systems Quarterly
MOA	-	Motivation-Opportunity-Ability
NAM	-	Norm Activation Model
ORS	-	Online Romance Scam
OTP	-	One-Time Password
RAT	-	Routine Activity Theory
RSP	-	Romance Scam Pathway
SCARS	-	Society of Citizens Against Relationship Scams
TPB	-	Theory of Planned Behaviour
UK	-	United Kingdom
USA	-	United States of America
VPN	-	Virtual Private Network

CHAPTER ONE

INTRODUCTION

1.1 Research Background

Computers and computer-related technologies have become essential tools that have significantly affected various aspects of personal and social lives, ranging from education and business to cultural and leisure activities (Bankole & Bankole, 2017; Moon et al., 2010). Despite the enormous benefits of ICTs, there exist a myriad of cases of inappropriate use of these technologies, which translate into financial loss to individuals, organisations, and states. Unmistakably, cybercrime poses one of the biggest threats to the digital society (van de Weijer & Leukfeldt, 2017). Cybersecurity Ventures (2017) valued the cost of cybercrime in 2015 at $3 trillion, while Forbes (2017) conjectured that this figure would double to approximately $6 trillion per year on average through 2021.

Cybercrimes are considered global crimes; they transcend geographical boundaries and can be perpetuated from anywhere against any individual and technology (Donalds & Osei-Bryson, 2019). Such crimes may include but are not limited to hacking, cyberbullying, identity theft, online romance fraud and advance fee fraud. Riek and Böhme (2018) posit that losses resulting from cybercrime are driven mainly by scams and extortion in Germany and identity thefts in the UK. On the other hand, Italian, Estonian, and Polish consumers lose considerably less money to cybercriminals, even though they spend less money and time on protection. Whereas this development pertains to western countries, Africa's situation is not entirely different. Cross (2018), for instance, asserts that Nigeria has become synonymous with online scams, with advance fee fraud (AFF) and romance scams dominating in recent decades. Consequently, Nigeria is ranked as the leading country in the region for the commission of malicious internet activities (Aransiola & Asindemade, 2011; Longe & Chiemeke, 2008; Quarshie & Martin-

Odoom, 2012). That notwithstanding, many countries in the continent have developed legislation to fight cyber threats, strengthened enforcement measures, and engaged private-sector efforts to enhance cybersecurity (Kshetri, 2017). For example, in East Africa, a task force comprising government, industry, and civic groups has been set up to deal with cybersecurity at the three levels of legal, policy, and regulation, while in West Africa, the Economic Community of West African States (ECOWAS) has initiated policies in capacity-building, prioritising cybercrime issues and developing networks across the borders to fight cybercrime (Quarshie & Martin-Odoom, 2012).

In Ghana, Internet penetration has, for the past few years, been on the ascendancy. Hootsuite (2018), for instance, reports that about 10.11 million, representing 35% of the population, are active internet users, with 32% being active phone internet users. As Ghana's internet infrastructure continues to expand, more widespread, cheaper and faster internet connectivity gives cybercriminals more considerable resources to engage in illegal activities, including providing them with access to more potential victims (Barfi et al., 2018). It would not be out of place to contend that cybercrime cases will escalate as more people get access to data (National Communications Authority, 2017). With the preceding discussion as the backbone for this study, it has become necessary to understand the underlying mechanisms behind the commission of internet crimes, focusing on online romance scams. It is not out of place to use Ghana as a site for such research, as sufficient anecdotal evidence indicates that the country, along with Nigeria, is one of the main hubs for West African scams.

1.2 Research Problem

A review of existing literature for this study indicated an appreciable number of studies on cybercrime and its attendant effects on countries and the social stigmatisation that accompany them (see Chapter 2). These literature cover a number of relevant themes, which include but are not limited to the fight against cybercrime (Adomi & Igun, 2008; Cassim, 2011; Huey et al., 2013; Jamil, 2012; Malgwi, 2005), credit card fraud and financial crimes (Barker et al., 2008; Gottschalk, 2010; Salu, 2005; Yogi Prabowo, 2012), law enforcement (Davis, 2012), romance and dating fraud (Cross, 2020a; Fair et al., 2009; Whitty, 2019) and technical crimes (Baruah, 2019; Hui et al., 2017; Santanna et al., 2015; Soliman & Azer, 2018; Van der Wagen & Pieters, 2015).

The review further classified cybercrime using Wall's (2003) four-category cybercrime typology: cyber-trespass, cyber-deception/theft, cyber-porn and obscenity, and cyber-violence. Cyber-trespass refers to digital crimes that verge on crossing boundaries into computer systems and spaces where rights of ownership or title have already been established, example, hacking, defacement and viruses (Ngo & Jaishankar, 2017; Wall, 2015). Cyber-deception/theft refers to the theft of material and immaterial resources through piracy and credit card fraud via the internet (Dobovšek et al., 2013; Laue, 2011). Cyber porn is an act of using cyberspace to create, display, distribute and publish pornography and obscene material (Hillman et al., 2014; Mthembu, 2012; Puspitosari & Bidari, 2017). Cyberviolence refers to online crimes which thrive on the various ways that individuals can cause harm in real or virtual environments (Hua & Bapna, 2013; JiYoung Park et al., 2018).

Despite the growing body of studies on cybercrime, there seem to be a number of issues that can influence future research. To begin with, the disparities in the literature show that research

on various aspects of cybercrime from various fields and perspectives seems to dominate. However, research on the dynamics of cybercriminal behaviours appears to be a grey area in which further scholarship is needed (Venkatraman et al., 2018). Second, the literature indicates that most studies that have attempted to address why and how cybercriminals commit online crimes have done so primarily from the perspective of victims, dating platforms or defence, arguably omitting that of the attackers (Hui et al., 2017). Third, despite the fact that cybercrime has received recent research attention, there appears to be a dearth of studies that examine criminals' tactics on dating sites and the violent ways in which they aim to exploit vulnerable victims (Cross & Holt, 2021). Lastly, there is arguably a lack of theorisation in cybercrime studies. In that regard, there is the need to explore theories that can unearth the mechanisms that underly the commission of cyber offences (Boateng et al., 2011; Holt & Bossler, 2014; Jaishankar, 2008; Venkatraman et al., 2018). This doctoral research, therefore, seeks to address these gaps, as elaborated in the ensuing paragraphs.

The four gaps listed above are of particular interest to this research. First, in terms of cybercriminal behaviours, current literature has identified different methods used by cybercriminals to circumvent existing national and transnational laws (Bande, 2018; Croasdell & Palustre, 2019). Wall (2017) envisages that in the future, society will be forced to respond to a wide variety of networked crimes that will increase both the complexity of crime investigation and prevention whilst also intensifying the regulative challenges. It is worth pointing out that these advancements in criminal behaviours are often guided by the evolution of platforms and technologies (Venkatraman et al., 2018) or, to a large extent, the lack of organised social responses to prevent internet crimes (Paquet-Clouston et al., 2018). Concerning platform evolutions and cyberdeviance behaviours, a recent study by Venkatraman et al. (2018), published in the *Journal of Management Information Systems*, offers some

pointers for further studies. The study, which focussed on the intentional use of information technology in the workplace that is contrary to the explicit and implicit norms of the organisation, developed a typology of cyberdeviance with three dimensions: First, minor versus serious cyberdeviant behaviours; second, behaviours that target individuals versus organisations and third, cyberdeviant behaviours that require low versus high technical skills. The dimensions were further streamlined along four categories of crime in existing literature, namely cyberslacking, computer abuse, unauthorised access and use of IT, and cyberaggression. Considering the rate at which technologies continue to evolve in modern times, Venkatraman et al. (2018) accentuated the need for future research to continue to explore the triggers of cybercriminal behaviours and how unlawful cyber behaviours change over time. They perceive that the changes in behaviours may be triggered in various ways, including through platform evolutions.

Concerning attacker-side data, a review of literature for this study indicated three principal players in cyberspace: the offender, victim and deterrence agents (See section 2.4). Cybercrime perpetrators are people who have been exposed to one form of traditional crime or another (Ngafeeson, 2010) or government-sponsored agents who are engaged in cyberwars (Kshetri, 2013b; Liu, 2013). The victim refers to the targets of cyber-offences who can be individuals, computers or organisations, while deterrence agents are agents who manipulate an adversary's cost/benefit calculations to prevent offenders from committing offences (Goldman & McCoy, 2016). Whereas all these three actors are vital in cyberspace, extensive evaluation of literature indicates that there has arguably been less attention given to studies with data from perpetrators and that most studies have probed offender-data from the victims' perspective (Kopp et al., 2015; Whitty & Buchanan, 2012). To this effect, a recent study by Hui, Kim and Wang (2017), published in the *MIS Quarterly*, pointed out a direction for future studies. The quantitative

study estimated the impact of enforcing the Convention on Cybercrime (COC) on deterring distributed denial of service (DDOS) attacks. The study's findings suggested that attackers in cyberspace are rational, motivated by economic incentives, and strategic in choosing attack targets. Aside from the inconclusive results, the study focused on single-sided data to infer crime deterrence effectiveness, that is, from the victim's side. Such inference may be insufficient in expressing first-hand experiences of cybercriminals. The current study departs from this literature in that it empirically examines the modus operandi of cyber-offenders from a developing economy's perspective (see Chapter 6). Hui et al. (2017) emphasised the need to establish direct, complementary evidence from attacker-side data.

As previously noted, there appears to be a void in the literature about offender side data regarding perpetrator techniques for identifying and manipulating their victims. This gap in the literature is ostensibly due to the difficulties involved in collecting data from offenders (Hutchings & Holt, 2018). Despite the apparent scarcity of first-hand offender research, studies that have attempted to address this issue have relied on victim data to profile the tactics perpetrators use to exploit their victims (Buchanan & Whitty, 2014; Cross & Holt, 2021; Whitty, 2018b). To this effect, a recent study by Cross and Holt (2021) pointed out a gap that future studies should consider. The study, which focused on how often criminals use profiles and narratives built on military profiles to deceive victims through romance scam schemes and how they do it, found that although the military identity and narrative could be used to generate specific justifications for demanding money, there was no proof that it could be considered a separate type of romance scam. Despite the circumstantial indications of the approaches that cybercriminals use in their operations around the world, there has been hardly any empirical research on the strategies they employ in exploiting unsuspecting victims, particularly from the perpetrator's perspective. In light of this, Cross and Holt (2021) emphasised the importance of

future research into the tactics used by criminals on dating websites, as well as the cruel ways in which they continue to exploit vulnerable victims.

Regarding theorisation in cybercrime research, there seem to be a number of criminological and social theories that have been postulated to explain criminal activities and the behaviour of conventional criminals. However, empirical research to validate these theories in the context of cyber-activities and their application to cybercrime are sparse in the literature (Wada et al., 2012). Again, Venkatraman et al. (2018) emphasise that existing theories or prior research could be most helpful in investigating the motivating factors or consequences of cyberdeviant behaviours. Existing theories in cybercriminal literature include but not limited to Routine Activity Theory (RAT) (Cox et al., 2009; Jansen & Leukfeldt, 2015; Olayemi, 2014; Reyns, 2013), space transition theory (Danquah & Longe, 2011; Jaishankar, 2008) and protection motivation theory (Jansen & Leukfeldt, 2015). Even though these theories are relevant to cybercrime studies, there have been calls for future studies to explore how these existing theories can assist in understanding the behaviour and intention of both the victim and perpetrators in cybercrime (Boateng et al., 2011; Holt & Bossler, 2014; Jaishankar, 2008; Venkatraman et al., 2018).

1.3 Research Purpose

This study seeks to unearth the mechanisms that underlie the commission of online romance scams from the perpetrators' point of view and to develop an online dating scam pathway. The romance scam pathway, known in the literature as the scammers' persuasive techniques (Edwards et al., 2017; Kopp et al., 2015; Whitty, 2013b), consists of a blend of various forms of internet crimes. Each step in the pathway and the complementing internet crime are discussed in chapters five and six of this study. This thesis goes beyond developing a

comprehensive online romance scam pathway to also explore offender-behaviour dynamics. This is geared towards understanding the technological and environmental dynamics that cause cyber-offenders to change over time.

1.4 Research Objectives

Consequent to section 1.3, the following are the outlined objectives geared towards achieving the study's purpose.

a. *To unearth the mechanisms that trigger cybercriminal behaviours.*
b. *To explore the dynamics of cybercriminal behaviours.*
c. *To explore the strategies that online romance scammers employ in finding, priming and defrauding their victims.*

The first research objective responds to calls by scholars on the need for future research to explore the mechanisms that converge to trigger cybercriminal behaviours (Venkatraman et al., 2018; Arora, 2016). To achieve this objective, this study, after a review of literature to ascertain some factors that ignite the commission of crimes (see sections 3.3.1 to 3.4), dwelt on primary data collected from active cybercrime perpetrators. The analysis of the data revealed four mechanisms that are believed to instigate the commission of crimes (i.e., motivation, opportunity, ability, and rationalisation).

The second research objective is in response to the call for future studies to explore the triggers of cybercriminal behaviours and how these behaviours change over time (Venkatraman et al., 2018). Based on a longitudinal data collection, these objectives rely on the routine activity theory, the motivation-opportunity-ability framework and the neutralisation theory to understudy a romance scam syndicate, six self-identified independent scammers and a former

romance scam perpetrator to ascertain the critical technological and environmental dynamics that trigger the instigation and transformations of offender-behaviours. The change processes involved in such behaviours can be understood in three constituents: creation, maturation, and decline (See section 6.4).

The third research objective responds to the call for future studies to examine the tactics used by criminals on dating websites, as well as the ways in which they continue to exploit vulnerable victims (Cross & Holt, 2021; Whitty, 2013b, 2013a). Even though there exist numerous romance scam studies, a careful evaluation of the studies points to the fact that most studies consolidate data from either the dating platforms (Koon & Yoong, 2013) or the victims'(Kopp et al., 2015; Whitty, 2013b), thereby omitting the perpetrators' perspectives. To achieve this objective, this study draws on Whitty's (2013b) Scammers Persuasive Techniques (see section 2.5.1), and by obtaining evidence from ten self-identified romance scam perpetrators through interviews, observations, and content analysis, a romance scam pathway was developed (see section 6.5). The quest to fill this gap using first-hand perpetrator-data is backed by the call for future studies to establish direct, complementary evidence from offender-side (Hui et al., 2017).

1.5 Research Questions

Pursuant to the above objectives, the research questions are as follows:

a. What mechanisms trigger cybercriminal behaviours?
   i. *What are the motivational factors of these cyberdeviant behaviours?*
   ii. *Which environmental forces (opportunities) enable the work performance of cyber-offenders?*

iii. *What abilities do cybercrime perpetrators possess that aid them in committing online crimes?*

iv. *What neutralisation strategies do romance scam perpetrators employ to justify their unlawful behaviours?*

b. How do cybercrime behaviours change over time?

c. Which strategies do online dating romance scammers employ in finding, priming, and defrauding their victims?

1.6 Significance of the Study

The significance of this research can broadly be measured along three strands: Research, Practice, and Policy.

Regarding research, this study arguably is one of the first in information systems research to apply the MOA framework to study cybercriminal behaviours. Again, it is arguably the first study to employ a multi-dimensional perspective for understanding criminal actions. Thus, previous studies that have attempted to understand cybercrime triggers have often done so from one dimension or a combination of two. This study combines four dimensions of crime that is, motivation, opportunity, ability and neutralisation, and applies them to online activities, thereby developing a framework that future researchers can apply to other internet offences. This significance cannot be overlooked as the study aims to add to the existing body of knowledge regarding cybercrime studies.

Concerning policy and practice, this study forms a solid basis to banks, internet service providers, and shipping and clearing agencies to collaborate with the police to crack-down on cybercriminals. This research will also provide adequate findings for the Government of Ghana and law enforcement agencies responsible for enacting laws to expedite ongoing processes in

formulating policies and regulations to govern the internet's irresponsible use among some Ghanaian youth.

1.7 Chapter Outline

Chapter One is the introduction of the research. Contained in this chapter are the background of the study, research problem, research purpose, objectives of the study, research questions, and the research organisation. **Chapter Two** presents a review of relevant literature on cybercrime as well as defines key concepts. The gaps in existing research have also been highlighted in this chapter. This study's theoretical foundation is discussed in **Chapter Three** with the justification for using the selected theories. The chapter also highlights the assumptions, revisions, and criticisms of the theories/framework and expounds the framework chosen in relation to this study and how it addresses the research questions and objectives. **Chapter Four** discusses the methodological approach, highlighting the research strategy, paradigm, and design. The instrument for data collection and method used as well as data processing and analysis, are dealt with in the chapter. **Chapter Five** projects an overview of cybercrime in Ghana and presents the findings of the selected case for this study. **Chapter Six** deals with the analysis of data to unearth dominant themes arising from the findings in chapter five. **Chapter Seven** discusses the findings and analysis in chapters five and six respectively to answer the research questions posed in chapter one in relation to the literature discussed in chapter two. **Chapter Eight** presents the summary of the research, implications to research, theory, methodology, practice and policy, and future research directions.

CHAPTER TWO

LITERATURE REVIEW

2.1 Chapter Overview

Chapter one presented an introduction to this research by providing the background of the study, the research problem, research purpose, objectives and questions, significance of the study and a chapter-by-chapter synopsis of the thesis. Building on the first chapter, this chapter presents an overview of cyberspace with respect to online crimes. The concept of cybercrime and its constituents are also presented by way of definitions in this chapter. This is followed by a systematic review of cybercrime literature, taking into consideration the economic distribution of articles in cybercrime research, previous attempts to address issues in research as well as theories and frameworks that have been employed in existing studies. The chapter concludes by presenting gaps for future studies.

2.2 Definition/Overview of Key Concepts

Cybercrime has been a critical issue of discussion in recent times. For this reason, it has been studied in various disciplines such as criminology (Holt & Bossler, 2014), sociology (Odumesi, 2014), and information systems (Alagarsamy, 2021). However, despite an apparent acceptance of and familiarity with the term, there exist dramatically varied views of what cybercrime is (Gordon & Ford, 2006). Wall (2015), for instance, contends that the constituents of cybercrime are very contentious because whilst everybody agrees it is what exists, not everybody agrees as to what it is. Therefore, there is no catchall term for the tools and software used to commit certain online crimes (Gordon & Ford, 2006). In this regard, this section of the chapter will attempt to define the concept of cybercrime by consolidating some existing definitions. In so doing, the section will also present definitions of the various constituents of cybercrime.

Donn Parker, one of the first researchers in computer crime studies, defined computer abuse as any intentional act in which one or more victims suffered or could have suffered a loss, and one or more perpetrators made or could have made a gain (Parker, 1976). It is, however, worth noting that Parker (1976) did not use the term cybercrime. Instead, he used computer abuse. The use of abuse in the author's definition can largely be attributed to the fact that the study considered a number of computer crimes. These included vandalism, information and property fraud or theft, financial fraud and unauthorised use or sale of service. This stance was, however, critiqued by succeeding researchers (Kling, 1980; Nycum, 1976). Kling (1980), for instance, cautions that the definition of computer abuse or crime becomes problematic when a computer is tangentially associated with victimisation.

Goodman (1997) points out that there is disagreement globally as to what exactly constitutes computer crime. Goodman (1997) proposes three general categories of cybercrime: computer-targeted crimes, computer-mediated crimes and crimes where the computer is incidental. Computer-targeted crimes involve situations where a criminal computer intruder attacks an innocent party's computer system. Examples include hacking, malware circulation, denial of service attacks and eavesdropping (Marcum et al., 2014; Mohurle & Patil, 2017; Yan et al., 2016). Computer-mediated crimes consist of criminal activities that use computers as tools in the commission of internet crimes such as internet fraud, child pornography and cyberbullying (Bai & Koong, 2017; Vazsonyi et al., 2012; Salu, 2005; Jansen & Leukfeldt, 2015). Lastly, a computer is incidental to the crime if the computer itself is not required for committing the crime but is used in some way and thereby becomes connected to the criminal activity. Examples include financial records on a drug dealer's machine, an inculpatory bomb recipe discovered on a computer hard drive after an explosion in the neighbouring town among others.

(Goodman, 1997). Such crimes may go unnoticed without forensic investigations and discovery.

As noted by Parthasarathi (n.d.), the term cybercrime is a misnomer as it is broadly used to refer to all criminal activities conducted by the use of the internet and computer-related devices. The turn of the 21st century, therefore, came with its convention of definitions of cyber offences. This may largely be attributed to the diverse ways in which cybercrimes are perpetrated. In this regard, scholars began to specify the various crimes that their definitions encompass. Table 2.1 outlines some of these definitions and their corresponding crimes identified in the respective studies.

Table 2.1 Cybercrime Definitions and Factors Considered

Author (s)	Definition/characteristics of cybercrime	Internet fraud	Computer hacking	Cyber piracy	Spreading of malicious code	Others
Adomi and Igun (2008)	Any unlawful conduct carried out using computers, electronic and ancillary devices.	✓	✓		✓	✓
Loader and Thomas (2013)	Computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks.	✓	✓	✓	✓	✓
Chung et al. (2006)	Illegal computer-mediated activities that often take place in the global electronic networks.	✓	✓	✓	✓	✓
Longe et al. (2009)	Cybercrime refers to misconducts in cyberspace as well as the wrongful use of the internet for criminal purposes	✓			✓	✓
Gordon and Ford (2006)	Any crime that is facilitated or committed using a computer, network, or hardware device.	✓	✓		✓	✓
Kshetri (2009)	Criminal activities in which computers or	✓	✓			✓

Author (s)	Definition/characteristics of cybercrime	Internet fraud	Computer hacking	Cyber piracy	Spreading of malicious code	Others
	computer networks are the principal means of committing an offence.					
ITU (2012)	A range of offences including traditional computer crimes, as well as network crimes.	✓	✓	✓	✓	✓

Source: Literature synthesis

As can be deduced from the foregoing discussion, the conceptualisation of computer crimes covers a broad range of deviances, some of which are technical (Type I) (e.g., hacking, denial of service, malware distribution) or socio-technical (Type II) (e.g., confidence romance scams, advance fee fraud) in nature. This thesis is concerned with the latter: Type II internet crimes. Consequently, the study adopts the components from Barn and Barn (2016) that:

> An agent is motivated by either an intrinsic desire or an extrinsic need to commit an action. Actions are perceived as crimes depending upon a receiver agent's viewpoint. If an action is a cybercrime, then the cybercrime must be mediated through a technology. An action must have a target, and the target must endure some impact. An impact is the effect of a crime on a target and can be economic, psychological or geo-political. (p.6)

2.3 Cybercrime Categorisation

Cybercrime as a phenomenon can be perceived in several forms. Wall (2015), for instance, contends that the constituents of cybercrime are very contentious because while everybody agrees it exists, not everybody agrees as to what it is. Further, Donalds and Osei-Bryson (2019)

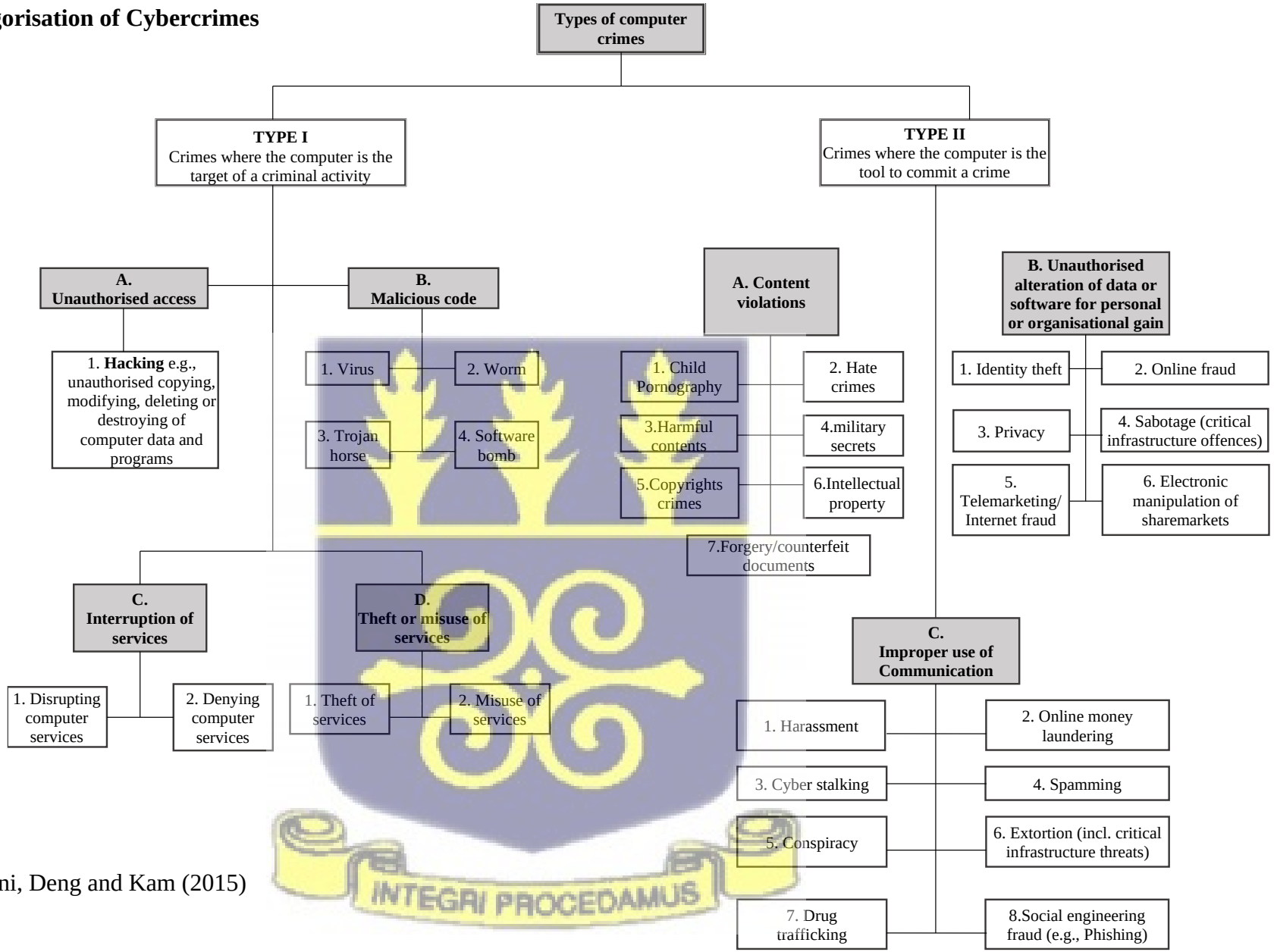
emphasised that while there is no single definition of "cybercrime", the term is generally used to cover/describe a wide variety of crimes or what is considered illicit conduct in cyberspace. Such crimes may include those committed by individuals or groups against computers, computer-related and other devices, information technology networks, or traditional crimes, as well as actions targeting individuals supported by the use of the internet and technology. Similarly, Gordon and Ford (2006) posit that cybercrimes differ depending on the perception of both observer/protector and victim and are partly a function of computer-related crimes' geographic evolution. This projection has also been endorsed by other scholars who believe computer crimes can be looked at in the three broad forms mentioned. Sukhai (2004), for example, breaks the categorisation further into financial – crimes that disrupt a company's ability to conduct e-business; piracy – crimes of copying copyrighted material without explicit permission; and hacking – crimes of gaining unauthorised access to a computer system or network and in some cases making unauthorised use of this access. According to Sukhai (2004), cyber-terrorism can be considered a type of hacking designed to cause terror, violence against persons or property, or at least enough harm to generate fear. Online pornography, possessing or distributing child pornography is against federal law and distributing pornography of any form to a minor is illegal.

Contrary to this categorisation, another group of researchers believe that cybercrime can be categorised into Type I and Type II cybercrimes. For instance, Gordon and Ford (2006), in their categorisation of the two, specifically stated that Type I cybercrimes are mostly technical in nature while Type II cybercrimes have a more pronounced human element. For example, a computer penetration or a denial-of-service attack can be categorised as a Type I cybercrime since it relies almost entirely on technology. On the other hand, cybercrime can also be almost entirely people-centric when the role of technology in the commission of the crime is minimal.

Consider, for instance, an e-commerce fraud where a fake product is advertised online, and a gullible customer pays for the item but does not receive it.

Inasmuch as these categorisations are essential in the definition and classification of cybercrime studies, prevention and the formulation of policies and frameworks, there is one key component that plays a critical role in the commission of internet crimes: technology. In that respect, Alkaabi, Mohay, McCullagh and Chantler (2010) claim that for a crime to be considered cybercrime, the computer, a network, or a digital device must have a central role in the crime, i.e., as a target or tool. This claim by the authors tends to serve as an arbitral ground for both schools of thought.

Figure 2.1 Categorisation of Cybercrimes



Source: AlKalbani, Deng and Kam (2015)

2.4 Actors in Cyberspace: Attackers, Defenders and Victims

A clear understanding of cybercrime from an individual to a societal level involves identifying and comprehending cybercrime stakeholders, who are classified according to their roles in cybercrime incidents (Arief & Adzmi, 2015). Regarding the stakeholders of cybercrime, studies have been conducted by various researchers on the interrelationship between people and technology to commit crime – perpetrators (Leukfeldt, 2014a; Marcum et al., 2014; Soudijn & Zegers, 2012); the interrelationship between people and technology to prevent crime – defence/preventions (Arief & Adzmi, 2015; Rotich et al., 2014); and the interrelationship between people and technology in the suffering of crime – victimisation (Leukfeldt & Yar, 2016; Ngo & Paternoster, 2011; Pereira, Spitzberg, & Matos, 2016). Therefore, this section seeks to synthesise studies that have been done concerning the various actors in cyberspace.

2.4.1 Attackers/Perpetrators

Discussions on cybercrime studies in the past have hinged on the forms of crimes committed, much to the neglect of the offenders. This is not to say that no studies have been conducted on the perpetrators and their motivations. Nonetheless, only a few studies (Aransiola & Asindemade, 2011; Ngafeeson, 2010) have taken into consideration the subject of perpetrator and offender motivations. In a broad sense, cybercrime perpetration may be categorised into two levels; Institutional and Individual (Näsi et al., 2015): Institutional cybercrimes are mainly related to crimes that target governments and large multinational institutions. Such crimes may be initiated by cyber-gangs, cyber terrorists or hackers whose targets are electronic networks, computers and data (Holt & Schell, 2011). On the other hand, cybercrime at the individual level often reflects victimisation through known assailants or where the victim is a specific target (Näsi et al., 2015).

According to Ngafeeson (2010), cybercrime perpetrators are people who have been exposed to one form of traditional crime or another. He argues that without predisposing factors (determinants of crime), some people may only stay as latent potential candidates and may never really get to commit a cybercrime. A study by Aransiola and Asindemade (2011) in Nigeria revealed that cybercrime perpetrators cut across youth from different social backgrounds, with half of the respondents in their study being between 22 and 25 years, whereas another 40 per cent were between 26 and 29 years. The findings of the foregoing study are in line with that of Boateng et al. (2011), which pointed out that cybercrime perpetrators are young and have some degree of technical competence to commit computer-related crimes. While these studies are relevant to understanding cybercriminals' demographics and behaviours, both studies overlooked some critical aspects of committing internet crimes. For example, the perpetrators' motivations and their opportunities were not addressed. In that regard, Warikoo (2014) posits that cybercriminals are driven by financial gains and consequently target consumers and businesses. Similar to Boateng et al.'s (2011) findings on the competence of cybercriminals, Warikoo (2014) discovered that cybercriminals are not organised, and their skill level ranges from basic to intermediate.

2.4.2 Defence/Deterrence

Cybercrime deterrence is one of the most venerable concepts in the national security lexicon. It refers to manipulating an adversary's cost/benefit calculations to prevent an action that one does not want to occur (Goldman & McCoy, 2016). Cybercrime deterrence and defence can also be viewed in two ways: Digital defence (Bowles, 2012; Choi, 2008; Holt & Bossler, 2014) and physical defence (Tseloni et al., 2004). Whereas digital defence has to do with utilising antivirus and firewalls in the prevention of cyberattacks, physical defence encompasses the presence of the police, CCTV cameras, parental monitoring, and the presence of people

standing by, among others, in the prevention of cybercrime. This study's focus shall be on the latter since the forms of cybercrime being studied do not fall into the category of Type I crimes.

While the police were originally tasked to deal with social disorder (Wall, 2007), their mandate has been made more sophisticated with the prevalence of technology and for that matter cybercrime. Wall (2007) claims that a long-standing complaint made by members of police and law enforcement agencies is that they do not have the facilities to keep up with criminals, especially with regard to offences that require a high policing response. Similarly, Olayemi (2014) avers that the Nigerian law enforcement agencies are not computer literate and lack computer forensic laboratory facilities within any branch of the Nigerian Police or other law enforcement agencies to investigate and analyse cybercrime-related issues.

2.4.3 Victims

Victims are the targets of cyber offences. Victims of cyber offences can also either be organisations or individuals. Arief and Adzmi (2015) argue that in an attack on an individual, the defender is likely to be the victim as well. This actor in the cybercrime space has been studied from the point of view of the value, inertia, visibility and accessibility (VIVA) of the victim (Leukfeldt, 2014b; Yar, 2005) as well as the awareness, proficiency level, attractiveness and the cost impact on the victim (Arief & Adzmi, 2015).

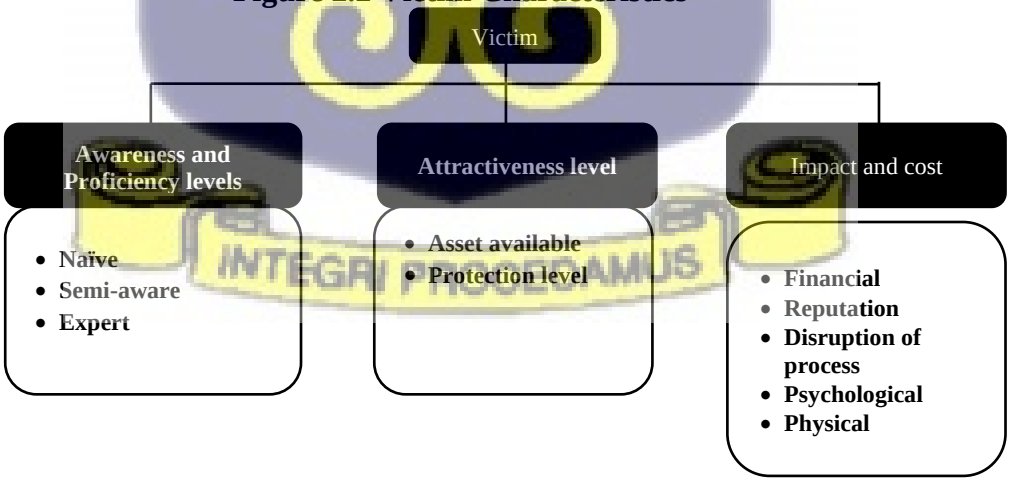
Many of the crimes that are reported online are a result of the victims' inability to identify the crime being committed. In instances where organisations have been hacked, it may be due to their weak firewalls or other security systems. Likewise, unaware individuals are also caught in the web of scams when scammers identify them to have low IT proficiency levels. According

to Arief and Adzmi (2015), however, very knowledgeable individuals or organisations can still become victims, often as a result of identity theft, insider threat or cyberwarfare.

On the other hand, attractiveness is similar to the operationalisation of the *value* advanced by Leukfeldt (2014a) and Yar (2005). Attractiveness is the financial value of the target. Whereas the offender does not have access to the would-be victim's financial records, his/her social media profile is equally valuable to the offender. For e-commerce fraud, for instance, the attractiveness of the organisation will stem from the site's traffic and their inability to detect credit card fraud.

Arief and Adzmi (2015) argue that the impact and cost of cybercrime to the victim could be equated to the level of its attractiveness. For example, suppose a cybercriminal targets an attractive amount of $2,000.00 in a victim's account and is subsequently successful in obtaining and using the said amount. In that case, the cost of this venture to the victim is the criminal's targeted amount. The authors further divided the cost into five categories (Financial, Reputation, Disruption of process, Psychological and physical), as evident in Figure 2.2.

Figure 2.2 Victim Characteristics



Source: Arief and Adzmi (2015)

2.5 Forms of Cybercrime

As discussed, cybercrime has been divided in the literature into three broad categories: Computer as the target, computer-mediated and computer as an incidental instrument. However, it is worth noting that while some researchers agree to the three-layer categorisation, others subscribe to the two-layer categorisation (see Figure 2.1). That notwithstanding, this research's interest lies in computer-mediated crimes (Type II). Against this backdrop, this section will delve into some of the crimes identified in the literature as computer-mediated crimes.

Existing literature has pointed out quite an appreciable number of online crimes which can be considered computer-mediated. Some of these include advance fee fraud (Alli et al., 2018; Edwards et al., 2017; Webster & Drew, 2017), Confidence Romance Scams (Huang et al., 2015; Tan & David, 2017; Whitty, 2013a; Whitty & Buchanan, 2016), Identity Theft (Almerdas, 2014; Reyns & Henson, 2016; Williams, 2015) and credit card fraud (Bai & Chen, 2013; Papadopoulos & Brooks, 2011; Prabowo, 2012).

2.5.1 Online Dating Romance Scam

Online dating romance scams, otherwise known as sweetheart swindles, have been thought to have the *spirit* of advance fee fraud (Huang et al., 2015). According to Whitty (2015), the portrayed end goal for the victims is that they will be in a committed relationship rather than simply in receipt of large sums of money.

While extant studies in cybercrime have provided insights into the motivations and techniques of romance scams (Whitty, 2013b), only a few have considered the complexities involved in the commission of the crime. To date, most existing romance scam studies have concentrated

on the perpetrators' grooming and persuasion techniques (Cross et al., 2018), much to the neglect of the motivations and rationalisations to which the offenders attribute their unlawful behaviours. Again, while these studies are valuable, only a few have arguably critically examined evidence from the offenders' stance; a large amount of the literature sourced evidence from romance scam victims (Kopp et al., 2015), dating platforms or law enforcement agents (Koon & Yoong, 2013). For instance, Kopp et al. (2015) conducted an exploratory study using a qualitative analysis of fraudulent profiles from an international dating website with the assumption that the success factors found in normal relationships contribute to the success of romance scams. The results of the study indicated that "personal affinities related to personal romantic imaginations, which are described by personal love stories, play an important role in the success of a romance scam" (Kopp et al., 2015).

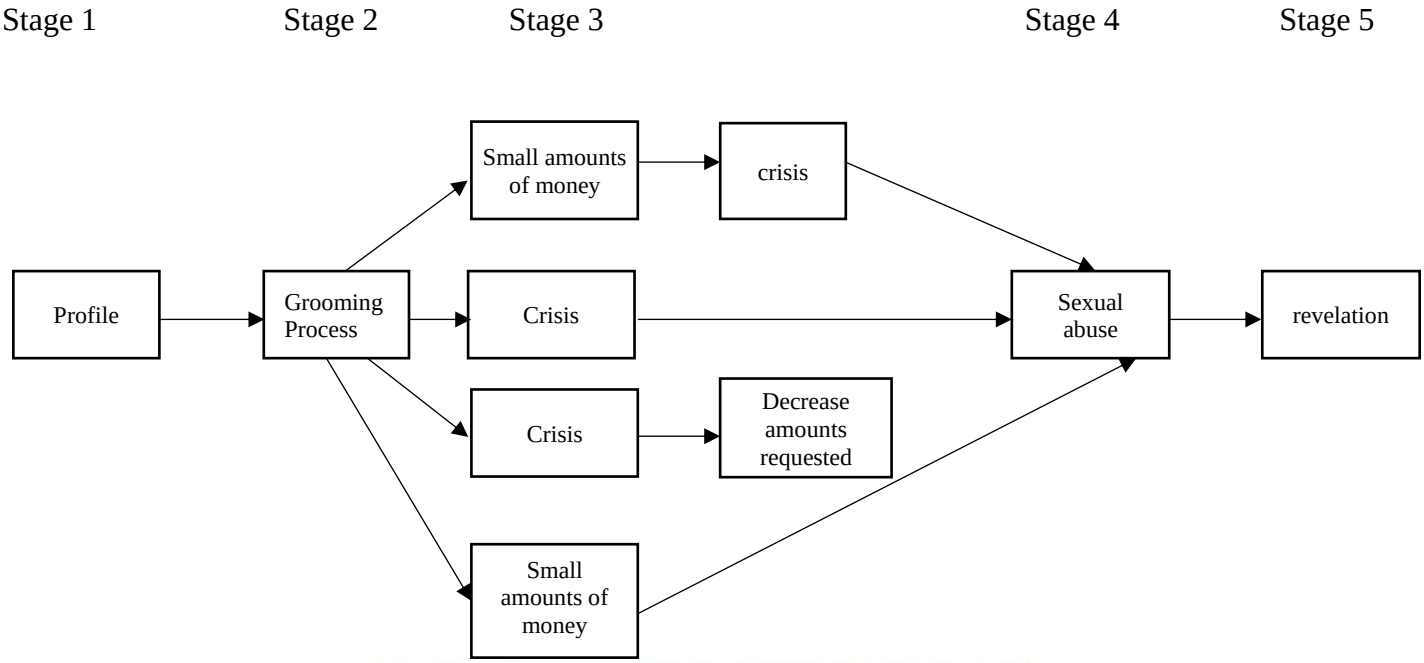
Similarly, a study by Cross et al. (2018) towards the understanding of how romance scam works in relation to other forms of online scams and non-physical forms of abuse used semi-structured face-to-face interviews with 21 Australian romance fraud victims who had reported online dating scams to the Australian Competition and Consumer Commission (ACCC) scamwatch website. The study's findings revealed considerable overlap in the types of psychological maltreatment in romance fraud and domestic violence, despite the differences in the presence or absence of a physical relationship.

In a three-layer structured study, Whitty (2013) analysed posts from a public online support group, conducted in-depth interviews with victims of romance scams and also interviewed a Serious Organised Crime Agency officer to outline the anatomy of online romance fraud. The results of the study identified four main trajectories of the scam and five distinct stages.

In this type of scam, criminals create fake social network site profiles to attract the trust of persons into relationships with the aim of financially defrauding them (Budd & Anderson, 2011; Whitty, 2019; Whitty & Buchanan, 2016). They then upload photographs ranging from low-quality to heavily pixilated ones of the same crafty socially engineered person to strengthen the scammer's credibility. The second stage is to maintain consistent contact with the would-be victim. This requires establishing a strong bond with the target through constant contact to engender trust, confidence and romantic connections (Rege, 2009). Cross, Dragiewicz and Richards (2018) contend that once trust is proven, offenders resort to various modes of communication, including email, telephone, and text messaging, to maintain the ruse. According to Whitty (2015), stage three is the sting stage, where scammers attempt to con the victim out of money. If they failed in the first instance, they go back to the grooming stage (stage two). In some instances, in stage three, criminals craft tragic stories such as theft of personal documents during travel and unexpected hospital expenses resulting from sudden accidents or illnesses (Rege, 2009).

Furthermore, victims are sometimes unable to identify such scams considering the length of period it takes to create a relationship and build trust in these scams. Rege (2009) posits that such relationships take as long as six to eight months until trust is built. At the fourth stage of the trajectory, when so much money has been taken from the victim, in very few instances, scammers embarrassed their victims by requesting naked live webcam videos from them. The final (fifth) stage is the revelation stage, where victims realise that they have been scammed. Whitty (2015) opines that some financial victims realise the scams themselves and seek out evidence to support their premonitions, while victims who fairly quickly identify the scam exit at stage 3. The stages outlined in the above discussion are represented in Figure 2.3.

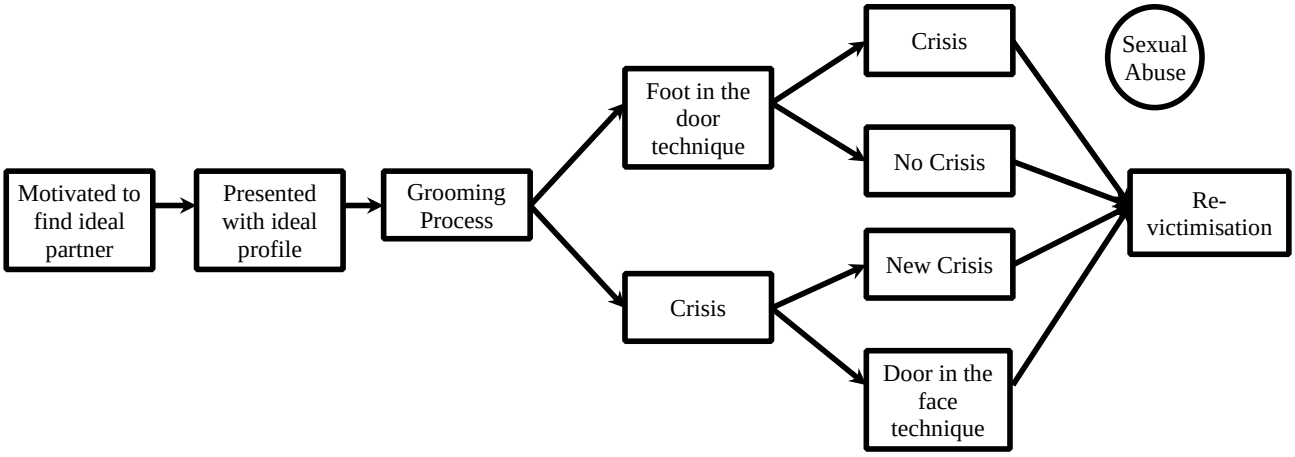
Figure 2.3 Romance Fraud Trajectories



Source: Whitty (2013)

In another research aimed at examining the persuasive techniques that scammers employ and whether previous theories on persuasion are adequate in explaining why victims are conned by romance fraud, Whitty (2013b) extended the romance scam trajectories from five to seven stages as presented in Figure 2.4. By extension, Whitty (2013b) suggests that the first step of the model entails the victim being motivated to find an ideal lover online. The victim is then presented with an enticing profile of the "ideal lover" who tends to be the offender. The grooming process and the sting stage, as described in the earlier model, then follow. The scam process continues in stages five and six. According to the author, in just a few cases, victims are requested to perform sexual gestures before a live webcam under the guise of distance relationships which the offender then uses to blackmail them. The final stage, according to Whitty (2013b), is the re-victimisation stage, where victims, even when informed by law enforcement agencies, revert to the scam, either to the same person or a different person.

Figure 2.4 The Scammers' Persuasive Technique



Source: Whitty (2013b)

2.5.2 Advance Fee Fraud

Advance fee fraud involves an offender using deceit to secure a financial benefit from the victim with the promise of a future 'pay-off' for the victim (Whitty & Buchanan, 2012). According to Ofulue (2010), advance fee fraud is the most frequently encountered and successful type of fraud in history. The modus operandi for advance fee fraudsters involves requesting unsuspecting victims for upfront payments for products, services or materials that do not exist with a promise of a pay-off. The promised pay-off can be a financial reward or, in the case of romance scams, a romantic relationship (Webster & Drew, 2017). According to Whitty (2015), advance fee fraud began in the 1970s with postal mail and faxes. It manifested through enticing victims via postal letters to commit huge sums of monies for one venture or the other. The schemes come in multiple forms, such as agreements to pay ransoms for kidnapped citizens from Africa or to redeem family properties.

Another form is the estate property redemption scheme, in which scammers charge victims fees to assist them in demanding family properties and millions of dollars from the central

bank. Scammers often draft fake wills of rich and famous Nigerians and mail them to victims to legitimise the scammer's position. However, the advent of computers and the internet did not only enhance positive development on the continent but also opened up avenues for the hitherto postal mail scammers to upgrade their skills to internet scammers. This, simply put, brought scammers closer to their victims. Offenders now have the opportunity to connect with massive populations within a short timeframe and at a meagre cost (Webster & Drew, 2017). Likewise, the accessories and the time spent in the commission of advance fee crime reduced significantly to a computer, internet connection and an email address (Holt & Bossler, 2014). As pointed out in the literature, the targets for this crime are rich people, the elderly, vulnerable and uneducated, and greedy individuals whose contact addresses are obtained from newspapers, commercial directories, and trade journals (Alli et al., 2018; Glickman, 2005). Existing research also indicates the interplay of two or more kinds of scams, including romance scams, identity theft and phishing (Edelson, 2003).

2.5.3 Identity Fraud/Theft

The term identity theft is widely used today among law enforcement agencies, organisations and scholars; however, its definition has been an issue of academic contention as the term is not consistently used (Almerdas, 2014). This is because the term has been used synonymously with identity fraud in the literature for some time. Berg (2009) and Finch (2013) determined that identity fraud involves the impersonation of another person for a particular purpose, after which the imposter resumes his/her identity. However, with identity theft, a person will not incur criminal liability for the assumption of another's identity or the abandonment of their own identity unless they do something under this assumed identity which amounts to a criminal offence (Finch, 2013). This study consequently uses the two terms (identity theft and identity fraud) synonymously. It adopts McQuade III's (2008) definition that identity theft/fraud is the

illegal possession and use of another person's financial account details in order to obtain goods and services. The risk of one falling prey to identity fraud is the provision of one's financial records at a point-of-sale (POS) terminal where cybercriminals plant allies unknown to the victim. Again, McQuade (2006) suggested that cybercriminals create websites that appear to be legitimate but are actually set up to socially engineer people to give out confidential information.

2.5.4 Credit Card Fraud

Credit card fraud is described in the literature as the use of another person's credit card for personal purposes without the card owner's or issuer's permission (Chaudhary et al., 2012). Existing literature on this form of crime has studied it from various perspectives, including but not limited to credit card data mining, credit card fraud detection and prevention(Bhattacharyya et al., 2011; Carlson, 2014; Raj & Portia, 2011). For instance, a study by Barker et al. (2008) on credit card fraud reviewed literature and information from internet websites to provide corroboration and details of how fraudsters use credit cards to steal monies every year. The study found that credit card fraud is a healthy and growing means of stealing billions of dollars from credit card companies, merchants, and consumers. The paper concluded that although credit card companies and merchants have implemented various ways to deter credit card fraud, it is still a concern. Prabowo (2012) further studied credit card fraud prevention by assessing the efficacy of Indonesia's credit card fraud prevention from a strategic point of view. The study made use of a qualitative method by way of a literature review and in-depth interviews with payment system professionals. The study revealed that credit card fraud prevention practice in Indonesia is still at a lower level of robustness than those in the USA, the UK and Australia. The author recommended that deficiencies and weaknesses in the system should be

identified and actions taken to make it more consistent with credit card fraud prevention practices of other countries.

2.6 Cybercrime Research: The Past, the Present and the Future

Cybercrime issues have enjoyed a fair share of research conceivably because it is perceived to be equally climbing into the categories of traditional crimes. Some of the scholarly works in this field include literature that underscores the need for laws, policies and regulatory frameworks to counter the cybercrime menace (Eboibi, 2017; Gerry & Moore, 2015; Hunton, 2011; Ju et al., 2016; Sun et al., 2015; Yilma, 2014), literature that highlights financial crimes and strategies for combatting them; ICT aided banking crimes, digital currency crimes and credit card fraud (Bai & Koong, 2017; Bay et al., 2014; Bolimos & Choo, 2017; Hunton, 2012; Vahdati & Yasini, 2015). There are also studies that focus on stakeholders' engagement in the fight against cybercrime (Levi & Leighton Williams, 2013; Martin & Rice, 2011; Tehrani et al., 2013) and security awareness and prevention (McGee & Byington, 2013; Singleton, 2013; Vlachos et al., 2011). However, it is worth noting that though these sources and others not cited above provide insights into cybercrime, there are some knowledge gaps that call for extensive review of cybercrime.

Regardless of the rapid interest in the literature, there seems to be a lack of concentration on cybercrime in information systems research. Therefore, cybercrime research in information systems needs a systematic approach to classify the various contributions of scholars in the field. The following sections seek to answer this call.

2.6.1 Methodology for Review

2.6.1.1 Identification and Collection of the Literature

In conducting this review, only peer-reviewed articles were considered. Peer review, according to Solomon (2007), is generally seen as vital for the roles of establishing an archive of knowledge and distributing rewards. Peer review also plays a crucial role in validating the quality of research in a field. In that regard, the study was conducted at two levels: first, by searching for articles published in the Senior Scholars' Basket of Information Systems Journals and thence to exploring high-ranking journal databases. Details of the processes have been delineated in the ensuing sections.

2.6.1.2 Data Collection and Search Process

The articles considered for this review were articles published between 2010 and 2018[1]. As earlier indicated, of the publications on cybercrime within the period under consideration, only peer-reviewed articles were considered. The articles reviewed were accessed in two phases: first, the senior scholars' basket of information systems research was searched to cumulate cybercrime research journal articles from the field of information systems. The returns indicated that very few studies had been done concerning cybercrime in information systems journals. The second set of downloads were done using JSTOR, Emerald, WILEY, Science Direct, and Taylor and Francis databases. These databases were selected because of their supply of prime journals they provide in information systems research.

In order to ensure relevance to the focus of this research, the researcher examined each article regarding its title, abstract and, where applicable, the full text. After removing duplicate articles from the filtering, 109 articles remained for review.

[1] The literature review was conducted in 2018 during the researcher's second year of the PhD programme.

2.6.1.3 Inclusion and Exclusion Criteria

In searching for the articles, the descriptors used were *cybercrime, cyber crime, cyber fraud and internet fraud*. The downloaded articles were subjected to filtering. Editorials and reports were eliminated because, as earlier stated, the study set out to include only peer-reviewed articles in the review. Further, publications that had only full-body text in English were considered for this review. Studies that were deemed duplicates were also excluded.

2.6.2 Article Categorisation

A total of 109 articles across 40 journals were analysed in this review. These articles were further categorised into themes, geographical areas of focus, methodology, research framework and publication outlets. The classification in terms of methodology was done according to the methods used by researchers in conducting their studies, be it qualitative, quantitative, mixed-methods and studies that did not explicitly state their methodologies. For instance, studies that emphasise objective measurements and statistical, mathematical, or numerical analysis of data collected through polls, questionnaires, and surveys, or by manipulating pre-existing statistical data using computational techniques, were categorised under quantitative. On the other hand, the qualitative category involved articles that used case studies as a research method and data collected through interviews and observations. The mixed-method category consolidated articles that combined both the quantitative and the qualitative methodologies. Lastly, studies that did not make use of any of the methodologies mentioned above were grouped under the 'not mentioned' category.

With regard to categorising the literature under geographical focus, the selected articles were grouped under the seven continents: Asia, Africa, North America, South America, Antarctica,

Europe and Australia. Articles that concentrated on more than one country were categorised as cross-country, while those that did not have a particular country in scope were categorised as "no region." With Ghana being the focus of this study, a brief review of cybercrime studies in Ghana and Nigeria was presented in this section.

Articles were further classified under level of analysis. Four levels of analysis exist in information systems research. The micro-level studies relate to articles which focus on individuals and organisations while the meso level consolidated industry-level studies (Senyo, 2018). Macro studies relate to nationally focused studies, while meta studies relate to studies that go beyond the national level — for example, regional level or cross-country studies. Lastly, the review categorised the selected articles according to their publication outlets.

2.6.3 Publication Outlets

As indicated, a total of 109 articles across 40 journals were considered for this review. Computer Law & Security Review published the highest number of articles in cybercrime studies (17). Journal of Financial Crime followed with a total of 11 and Journal of Money Laundering Control with 10. Computers and Security recorded 15, while Journal of Association of Information Systems featured 4 of the articles published during the period. Journal of Management Information Systems, International Journal of Law, Crime and Justice and Digital Investigation all recorded 3 each. Policing: An International Journal of Police Strategies & Management, Information Systems Research, Information Management & Computer Security and Digital Policy, Regulation and Governance all recorded 2 each, while Procedia Computer Science, Journal of Criminal Justice, Journal of Corporate Accounting & Finance, International Journal of Social Economics, Info Systems Journal and Information and Computer Security featured 1 each. Third World Quarterly, The Journal of Risk Finance, The Electronic Library,

The Comparative and International Law Journal of Southern Africa, Technological Forecasting & Social Change, Security and Communication Networks, Procedia Engineering, Procedia Economics and Finance, Perspectives in Science, MIS Quarterly, Journal of Strategic Information Systems, Journal of Investment Compliance, International Review of Law, Computers & Technology, International Journal of Web Information Systems, International Journal of Accounting & Information Management, Information Security Journal: A Global Perspective Information & Communications Technology Law, Foresight, Computers and Human Behaviour, Computers & Security, Computer Networks, Advances in Autism, and Accounting Perspectives also recorded 1 each. Table 2.2 shows the distribution of articles per publication outlet.

Table 2.2 Publication Outlets of Reviewed Articles

Journals	**Publication**
Computer Law & Security Review	17
Computers and security	15
Journal of Financial Crime	11
Journal of Money Laundering Control	10
Computers in Human Behaviour	4
Journal of Association of Information Systems	4
Digital Investigation	3
International Journal of Law, Crime and Justice	3
Journal of Management Information Systems	3
Digital Policy, Regulation and Governance	3
Information Management & Computer Security	3
Information Systems Research	3
Policing: An International Journal of Police Strategies & Management	3
Info Systems Journal	2
Information & Computer Security	2
International Journal of Social Economics	2
Journal of Corporate Accounting & Finance	2
Journal of Criminal Justice	2
Procedia Computer Science	2
Accounting Perspectives	1
Advances in Autism	1
Computer Networks	1

Journals	Publication
Foresight	1
Information & Communications Technology Law	1
information Security journal: A Global Perspective	1
International Journal of Accounting & Information Management	1
International Journal of Web Information Systems	1
International Review of Law, Computers & Technology	1
Journal of Investment Compliance,	1
Journal of Strategic Information Systems	1
MIS Quarterly	1
Perspectives in Science	1
Procedia Economics and Finance	1
Procedia Engineering	1
Security and Communication Networks	1
Technological Forecasting & Social Change	1
The Comparative and International Law Journal of Southern Africa	1
The Electronic Library	1
The Journal of Risk Finance	1
Third World Quarterly	1
Total	109

Source: Literature Synthesis

2.6.4 Classification Framework

Cybercrime has been an issue of contention in recent times, thereby attracting attention from different disciplines. It is against this backdrop that this review categorised the literature into themes and their sub-themes. In that regard, the review categorised existing literature on various forms of technology-enabled crimes using Wall's (2003) four-category cybercrime typology: cyber-trespass, cyber-deception/theft, cyber-porn and obscenity, and cyber-violence. According to Holt and Bossler (2014), this is considered one of the most comprehensive frameworks for understanding the incorporation of technology into various forms of offences.

The cyber-trespass category puts together studies that bordered on crossing invisible yet salient boundaries of ownership online (Holt & Bossler, 2014). Such crimes include hacking, cracking, ransomware, botnet distribution of viruses, among others (e.g. Bartholomae, 2018; Smith,

2015; Jeong et al., 2011). The cyber-deception/theft categorisation recognises the different types of acquisitive harm that can take place within cyberspace (Wall, 2003). This crime category includes e-banking fraud, advance fee fraud, piracy, credit card fraud and consumer fraud.

The third typology is cyber-pornography and obscenity, which encompasses the range of sexual expressions enabled by computer-mediated communications and the distribution of sexually explicit materials online (Holt & Bossler, 2014). Literature categorised under this section includes cyber-pornography and child pornography (e.g. Hillman et al., 2014; Mthembu, 2012; Verma, 2012; Prichard et al., 2011). The cyber-violence category comprises various ways that individuals can cause harm in real or virtual environments (Holt & Bossler, 2014). These crimes include cyber-terrorism, cyber bullying, cyber stalking and money laundering and terrorism financing.

Table 2.3 Cybercrime Literature Classification Framework

Theme	Sub-themes	Sources
Cyber-Trespass	Hacking, Cracking, Ransomware, Botnet virus attacks.	Bartholomae (2018) Ngo and Jaishankar (2017) Wall (2015) Smith (2015)
Cyber-deception/Theft	E-Banking Fraud, Advanced Fee Fraud, Piracy, Credit Card Fraud, Consumer Fraud.	Li, Yin, et al. (2016) Carminati et al. (2015) van der Meulen (2013) Yogi Prabowo(2012) Laue (2011) Papadopoulos and Brooks (2011)
Cyber-Pornography and Obscenity	Cyber-pornography and child pornography.	Hillman et al. (2014) Mthembu (2012) Verma (2012) Prichard et al. (2011)
Cyber-Violence	Cyber-terrorism, Cyber bullying, Cyber Stalking and money laundering and terrorism financing.	Gross et al. (2016) Salleh et al. (2016) Irwin et al. (2014) Hua and Bapna (2013)

Source: Literature Synthesis

2.6.4.1 Cyber-Trespass

Classification of literature under this category encompassed crimes that verge on crossing boundaries into computer systems and spaces where rights of ownership or title have already been established e.g. hacking, defacement and viruses (Ngo & Jaishankar, 2017; Wall, 2015). Sampled papers on this typology indicated that hackers are motivated by a number of factors that may include perceived cost benefits and psychological benefits. Bartholomae (2018) pointed out that there are three types of hackers: the good, the bad and the greedy. Good hackers have decent aims of making the world a better place by hacking systems to identify challenges and informing the systems' owners about the loopholes. The main interest of the bad hackers is fame among their communities. Such hackers may later transform into greedy hackers who aim to earn income from their activities. Such people hack into banking systems to steal credit card details which they sell at the credit card black-market. Studies sampled under this category also proposed that the hacking community could be grouped into lone hackers and cybergangs (organised) (Smith, 2015). Lone hackers have the least complex organisational structures, mostly one person in one geographical location. The literature recognises that there are easy prosecutions of lone hackers because their attacks less sophisticated than those of the cybergangs who implement a sophisticated level of operation. Smith (2015) surmises that in the future, governments that do not have the resources or time to develop their own cyber-attack centres, such as the Chinese or the USA, will hire these cybergangs on a project-by-project basis.

2.6.4.2 Cyber-Deception/Theft

This classification dwelt on articles that discussed theft of materials and immaterial resources through piracy and credit card fraud via the Internet (Laue, 2011). Issues discussed in papers

under this theme included advance fee fraud (Dobovšek et al., 2013), banking fraud (Carminati et al., 2015; van der Meulen, 2013) and credit card fraud (Chen et al., 2016; Papadopoulos & Brooks, 2011; Yogi Prabowo, 2011, 2012).

Regarding advance fee fraud, papers analysed pointed out that AFFs are not declining in occurrence. Instead, they constantly develop and use bulk sending and narrower targeting (Dobovšek et al., 2013). However, this form of crime tends to advance into other forms of crimes (e.g., phishing, email spoofing and pilfering). In relation to credit card fraud, there were mixed concerns about whether the phenomenon can be mitigated entirely. For instance, Papadopoulos and Brooks (2011) suggest that a far more co-ordinated approach is needed to tackle credit card fraud, with a lack of specialised knowledge of fraud being a major drawback. Prabowo (2011) established a common approach to preventing credit card fraud which the author believes is reducing offenders' opportunities to commit offences. This often requires a significant amount of resources, and thus, a sound strategy needs to be properly formulated and executed. In that regard, Prabowo (2011) suggests that resources should be allocated mainly to six key areas of fraud prevention: understanding of the real problems, fraud prevention policy, fraud awareness, technology-based protection, identity management and legal deterrence. These are supported in principle by four main groups in a payments system: user, institution, network, and government and industry.

It is, therefore, worth noting that these types of frauds are global and no country is immune to them nor can any country be excluded from hosting the perpetrators (Dobovšek et al., 2013). It has, for that matter, become a necessity to research on mitigating initiatives to combatting credit card fraud.

2.6.4.3 Cyber-Porn and Obscenity

Categorisation of papers for this typology was on two themes: cyber-pornography (Verma, 2012) and child pornography (Hillman et al., 2014; Mthembu, 2012; Prichard et al., 2011). Cyberspace facilitates access to child exploitation materials that were once difficult to locate, thereby providing instant access to children from all over the world or within a country (Choo, 2008). Cyber pornography is an increasingly visible problem in society today (Schell et al., 2007). Evidence from the literature reviewed indicates that although legislation and prosecution are essential tools in the fight against online child exploitation, there is also the need to investigate alternative approaches to child exploitation. Further, other studies found that loopholes in legal and regulatory frameworks account for states' and governments' inability to adequately deal with online child pornography. In that regard, Mthembu (2012) suggests that an additional tool for combating online child pornography should be industry self-regulation, whereby industry codes of conduct and hotlines are developed, and ISPs work collaboratively. ISPs are believed to be in a pivotal position to assist with combating not just child pornography but also other forms of internet crimes. Lastly, an emphasis on prevention and education is more likely to shield children from such exploitation, whether committed by perpetrators or victims (e.g. sexting and in cases where victims were 'directed' by the offender to perform sexual acts on themselves in front of a webcam) (Simon & Choo, 2014).

2.6.4.4 Cyberviolence

The final typology deals with crimes which include a number of ways in which people can harm others in actual or virtual environments. Some of these crimes can be attributed to the high-rate of smartphones and smart devices penetration and social media subscriptions. In some instances, unassuming people take on certain attitudes which translate into bullying online. Committed by an individual or a group of users, cyberbullying refers to the use of

information and communication technology to harass others. Papers reviewed seem to acknowledge that cyberbullying has become a major problem along with the development of online communication and social media. Studies on cyber terrorism, on the other hand, have considered the subject of cyberviolence from various perspectives. Some of these viewpoints include economic impact (Hua & Bapna, 2013; Park et al., 2018), behaviours of cyber-terrorists (Gross et al., 2016; Salleh et al., 2016), governance and mitigation (Mohamed et al., 2018) and financing cyberterrorism (Irwin, Slay, Raymond Choo, & Lui, 2014).

These studies acknowledge that the internet has become a fertile ground for terrorists to obtain funds to support their operations by participating in activities ranging from credit card theft using phishing, to hacking and key logging attacks and money laundering. As such, the studies advocated that organisations that comprise the national critical infrastructure need to invest more heavily in information security than other organisations. The studies also challenged governments to consider mitigating strategies such as subsidising IS security investments, crafting ‘‘cyber terrorism intrusion compliance’’ policies, certifying such compliance, periodic IS security auditing of firms that comprise the critical national infrastructure and sharing lessons learned.

2.6.5 Economic Distribution of Articles

Articles considered for this study were further categorised under countries of focus. Evidence from the review suggested that studies that generally focussed on the issues of cybercrime without being country or regional specific accounted for 47 of the articles reviewed. The distribution of articles with regional specifications are as follows: North America 15, Cross-Country 15, Asia 12, Europe 8, Africa 7 and Australia 5.

The outcome suggested that most of the studies conducted were globally focused. Such studies did not particularly use data sources from any of the continents but discussed the issue of cybercrime generally. This finding suggests that cybercrime articles published during the period did not have a specific geographical focus in that they sought to provide a general understanding of the phenomenon. Nonetheless, the findings also pointed to the fact that studies in cybercrime did not disregard the various continents. Thus, a significant number of papers were published with respect to Asia, Africa, Australia, North America, and Europe. For instance, papers published with Africa in focus concentrated on Nigeria, Ghana, Ethiopia, and South Africa. Asian papers focused on Korea, Cambodia, Taiwan, Malaysia, India, Iran, and Kyrgyz Republic, and European papers focused on the United Kingdom, Greece, Cyprus, and the Netherlands. As is evident, most studies in cybercrime are not country focused. It has become imperative to conduct studies with data sources from individual countries. This will help in unveiling cybercriminal activities to the global communities on the perspectives peculiar to the individual countries.

2.6.5.1 Cybercrime Studies in Ghana and Nigeria

Several studies have been done with the Sub-Saharan region in focus. These studies follow quite a wide range of themes (some have been indicated in Table 2.4). Inasmuch as these studies are not exhaustive, there is a lack of concentration on the roles IT skills and strategies play in the commission of the crime. Aransiola and Asindemade (2011), in studying new strategies employed by cybercriminals in Nigeria, identified imperceptible aids, including the use of ladies as collaborators, collaboration with security agents and bank officials, local and international networking, and the use of voodoo.

A similar study by Warner (2011) sought to give a broad overview of Ghanaian cybercrime, focusing on its genesis, the various incarnations of national scams and the state-level reactions. The study claimed that most Ghanaians believe cybercrime was imported from Nigeria as a result of the influx of Nigerian nationals residing in Ghana. Also, like Tade (2013), Warner (2011) noted that the delayed success rates in *yahoo yahoo*, the untiring clampdown of the Economic and Financial Crimes Commission on cybercriminals, group rivalry and the activities of the media in enlightening the public accounted for the search for a more speedy way of increasing cybercrime victimisation, hence the *techno-spiritual paradigm of Sakawa*. Lastly, Warner (2011) pointed out that perpetrators of cybercrime in Ghana justified their actions with the assertion that there is nothing wrong with the acts and that the undertaking should be seen as a sort of redemptive project of social justice; as vengeance for centuries of historical injustices perpetrated by the West against Africans. Again, even though the findings by Warner (2011) provide grounds for further studies in cybercrime, especially in Ghana, the study dwelt on secondary data; the data collected did not include perpetrators of cybercrime but the views of individuals on cybercrime in Ghana.

Table 2.4 Cybercrime Studies in Ghana and Nigeria

Article	**Country and Perspective**	**Theme / Theory**	**Findings**
Tade (2013)	Nigeria Student [Cybercrime] fraudsters	Cybercrime and spirituality **Theory:** *Space transition theory*	The delayed success rates in yahoo yahoo, the untiring clampdown of the Economic and Financial Crimes Commission on cybercriminals, group rivalry, and the media's activities in enlightening the public accounted for the search for a speedier way of increasing cybercrime victimisation.
Quarshie and Martin-Odoom (2012)	East and West Africa Content Analysis	Legal and regulatory frameworks	According to the findings, Africa will benefit from the experience of developed

Article	Country and Perspective	Theme / Theory	Findings
		Theory: *Not Considered*	countries in combating cybercrime. The fight against cybercrime requires coordinated effort among all stakeholders such as government bodies, educational institutions, business organisations and law enforcement authorities.
Olayemi (2014)	Nigeria Law Enforcement Agencies, Governmental Institution	Legal and regulatory frameworks **Theories:** *Routine Activity Theory* *Structural Functionalism Theory* *Marxian Theory* *The Theory of Technology-Enabled Crime*	Laws to combat cybercrimes are useless if law enforcement agencies do not have the education and training necessary to even operate a computer. Judges must be well trained as well.
Aransiola and Asindemade (2011)	Nigeria Perpetrators	New cybercrime strategies **Theory:** *Not Considered*	Most cybercrime perpetrators in Nigeria are between the ages of 22 and 29 years who were undergraduates and have distinctive lifestyles from other youth. Their strategies include collaboration with security agents and bank officials, local and international networking, and the use of voodoo that is, traditional supernatural power. Findings also indicated most perpetrators of cybercrime were involved in online dating and buying and selling with fake identities among others.
Warner (2011)	Ghana Perpetrators*	Geopolitics Techno-spiritual paradigm (Sakawa) Justified Philosophy of Thievery	Sakawa boys justify their duping of Westerners by claiming that it is pointed retribution for centuries of historical injustices perpetrated by the West against

Article	Country and Perspective	Theme / Theory	Findings
		Theory: *Not Considered*	Africans. The rise and proliferation of the techno-religious phenomenon of Sakawa is another increasingly embedded, yet underreported, aspect of the practice of Internet fraudulence in Ghana.
Boateng, Olumide, Isabalija, and Budu (2011)	Ghana Internet Café Operators Law Enforcement agencies Lawyers Banks	Forms and implications of cybercrime **Theory:** *Not Considered*	Cybercrime is fast gaining ground in Ghana and the agencies responsible for investigating, controlling and apprehending online criminals lack the technical knowledge needed to tackle the problem. In Ghana, the perpetrators are young and have some degree of technical competence to commit computer-related crimes.
Offei et al. (2020)	Ghana Individuals with knowledge about online romance fraud.	Romance Scams Theories: Neutralisation Theory and Denial of Risk Theory	The study shows that denial of risk, a rationalisation mechanism, moderates the relationship between denial of victim, a justification technique, and intention to commit romance fraud

Source: Literature synthesis

Despite the enormous contributions of these studies, there continues to be a void in understanding cybercrime from the viewpoint of offenders in relation to law enforcement agencies and secondary stakeholders. Further, theories employed in studying computer-related crimes remain sparse, considering the dynamic nature of the phenomenon.

2.6.6 Theories/Conceptual Frameworks Used to Address Research Issue

Papers were also categorised under theories and research frameworks employed. Evidence indicated that most of the articles reviewed did not make use of theories. This category of studies unsurprisingly formed about 70% of the papers analysed (e.g. Arora, 2016; Lindsay, 2017; Menon & Guan Siew, 2012; Mueller, 2017). That notwithstanding, theories and frameworks used in the studies reviewed included Routine Activity Theory (e.g. Paek & Nalla, 2015; Prabowo, 2011; Reyns, 2015) and Self-Control Theory (Bossler & Holt, 2010; Moon et al., 2010), General Theory of Crime (Donner et al., 2014; Marcum et al., 2015). Other considerations of theory and frameworks include Game Theory, Dynamic Capabilities, Integrated Digital Forensic Process Model, Technology Threat Avoidance Theory (TTAT).

Analysis of the findings further points to the fact that traditional cybercrime theories and frameworks employed by researchers over the period under review were relatively few. This supports the claim that cybercrime is multidisciplinary. As such, the perspectives of researchers matter in the study of the phenomenon. For example, Kraemer-Mbula, Tang and Rush (2013) used dynamic capabilities theory in conjunction with other models to study the cybercrime ecosystem. Their research examined how cybercriminals innovate, what the sources of innovation are and from where they emanate. They argued that by doing so, they contribute to the broad literature on cybercriminal activity, which is mainly populated by scholars in criminology, psychology, sociology, law and information technology.

In this regard, there is the need for future studies to explore how existing theories in cybercriminal studies can help in understanding behaviour and intention of the actors in cyberspace.

2.7 Gaps for future research

The foregoing sections presented discussions on issues addressed in existing cybercrime research, the methodologies and conceptual approaches used in the identified studies. This section discusses gaps identified in the literature reviewed for the study.

First, analysis of the literature reviewed for this study indicated that there seems to be no definite classification of theories and frameworks purposely developed for cybercrime studies. A plausible reason for this can be the multifaceted manner in which cybercrime has been studied. In that regard, researchers tend to borrow theories from various disciplines to answer specific questions or to achieve peculiar research objectives. Routine activity theory, for example, appears to be the first-choice theory in a significant number of the studies examined (Olayemi, 2014; Paek & Nalla, 2015; Pratt et al., 2010). However, since the theory was postulated to solve traditional crimes, its applicability to crimes in cyberspace has been challenged by researchers in the field (Leukfeldt & Yar, 2016; Eck & Clarke, 2003), prompting calls for researchers to investigate how current theories can help in uncovering the processes that underpin internet crimes (Boateng et al., 2011; Holt & Bossler, 2014; Jaishankar, 2008; Venkatraman et al., 2018).

Second, according to the literature, there are three types of players in cyberspace when it comes to cybercrime: offenders, deterrent agents and victims. With that identified, the analysis showed an apparent lack of focus on studies from the offenders' perspectives, as most studies investigated perpetrators' behaviours through their victims and dating platforms. The apparent paucity of studies from the offenders' viewpoints may be due to the challenges of data collection in this field (Hutchings & Holt, 2018). Although it is essential to consider the impact of cybercriminal activities on victims, Cross (2020) asserts that understanding romance scams from the viewpoint of the perpetrator is equally important. Hui et al. (2018) stressed the

importance of combining attacker-side evidence in that regard. Further, a thorough analysis of the literature for this research revealed an apparent scarcity of studies on the behavioural characteristics of internet crime perpetrators. Again, the lack of evidence may be attributed to a lack of data from the offender's perspective. Venkatraman et al. (2018) emphasised the importance of research into the mechanisms that underlie cybercriminal behaviours and how these behaviours evolve over time.

2.8 Chapter Summary

The chapter reviewed literature on cybercrime research with a particular focus on the definition of the term cybercrime in previous studies. It also took into consideration the categorisation and various forms of cybercrime. In the final sections of the chapter, a systematic review was conducted highlighting issues in cybercrime research, the economic distribution of the articles reviewed, and a brief review of studies in relation to Ghana and Nigeria. Lastly, gaps for future research were emphasised.

CHAPTER THREE

THEORETICAL FOUNDATION

3.1 Chapter Overview

This chapter considers the research framework that is deemed fit to help digest the subject, having reviewed extant literature relative to cybercrime and internet romance scams in the previous chapter. This chapter reviews related literature explicitly or indirectly related to the chosen research framework to find answers to the research questions under review. In this regard, a consolidation of the routine activity theory, the motivation-opportunity-ability theory, and the neutralisation theory was conducted in light of the multifaceted nature of romance scams.

The RAT postulates three elements that must be present for a crime to take effect. First is the motivated offender, the suitable target, and the absence of a capable guardian. The Motivation-Opportunity-Ability theory is also a well-known framework that has been applied in both behavioural and management studies. The motivation dimension of the framework reflects the willingness of an individual to perform an action. The opportunity element projects the environmental enablers of the individual's action, while the ability aspect represents the individual's skills and capabilities to perform an action. Lastly, neutralisation techniques are a set of discourses used by criminals to justify or rationalise their unlawful behaviours.

This chapter delves deeper into the individual theories by establishing their origins and postulations as well as identifying the weaknesses that are associated with each of them. Subsequently, the chapter concludes with the research framework that serves as the roadmap for the conduct of this study.

3.2 Theories and Conceptual Frameworks in Existing Cybercrime Research

Cybercrime is an ever-growing phenomenon that has been studied from a variety of perspectives. Again, as indicated in the introductory chapter, several theories have been propounded for studying criminal activities. However, Wada, Longe and Danquah (2012) contend that empirical evidence of the application and validation of the theories in the context of cybercriminal activities is sparse. That notwithstanding, some theories and frameworks were identified while conducting the literature review for this study. Table 3.1, for example, presents a selection of studies from the literature reviewed that used theories in conducting their studies.

Table 3.1 Theories Used in Existing Cybercrime Research

Studies	Theory	Theme
Moon, McCluskey and McCluskey (2010)	Low self-control theory	Piracy/identity theft
Donner, Marcum, Jennings, Higgins and Banfield (2014)	General Theory of Crime	General deviance
Li and Qin (2018)	Theory of new sovereignty Theory of jurisdictional relativity Theory of website jurisdiction The principle of limited jurisdiction	Legal & Regulatory Framework
Ibrahim (2016)	The tripartite cybercrime framework	Motivation of offenders
Prabowo (2011)	Routine activity theory	Credit Card Fraud
Harrison (2018)	Model of Media Effects and Fraud Rationalisation	Consumer Fraud
Hua and Bapna (2013)	Game Theory	Cyber terrorism
Bossler and Holt (2010)	Self-control theory	Victimisation
Reyns (2015)	Routine activity theory	Victimisation
Marcum, Higgins, Ricketts and Wolfe (2015)	General Theory of Crime Social Learning Theory	Identity Theft
Kraemer-Mbula, Tang and Rush (2013)	Dynamic Capabilities and Business Models	Cybercrime Ecosystem
Paek and Nalla (2015)	Routine activity theory	Identity Theft

Source: Literature synthesis

3.2.1 Self-Control Theory

Gottfredson and Hirschi (1990) defined the General Theory of Crime, also known as the Self-Control Theory, as the degree to which a person is vulnerable to momentary temptations. According to Gottfredson and Hirsch (1990), motivation is invariant among all individuals, but levels of constraint differentiate criminals from non-criminals. Donner et al. (2014) also posit that once the perception of pleasure from an action outweighs the perception of pain from the action, an individual is likely to perform that action. Gottfredson and Hirsch (1990) claim that self-control, even though is the tendency to avoid acts whose long-term consequences outweigh their immediate benefits, is thought to be rooted in effective parental socialisation. Since its postulation, self-control theory has engendered a significant amount of empirical enquiry on how an individual's level of self-control interacts with environmental opportunities to foretell deviant behaviours in both adolescents and adults (Vazsonyi et al., 2016). Gottfredson and Hirsch (1990) further suggest that persons with low self-control generally lack the diligence and wherewithal to participate successfully in social institutions. According to Marcum et al. (2015), low self-control includes the inability to resist temptation when an opportunity presents itself, as the individuals do not consider the long-term consequences of their behaviour. Low self-control is believed to be the outcome of ineffective parenting and familial socialisation (Delisi, 2001).

Gottfredson and Hirsch (1990) further postulate that people who lack self-control tend to be impulsive, insensitive, physical, risk-taking, short-sighted and non-verbal. The authors, in establishing the causes of low self-control, also pointed out that the major cause of low self-control appears to be ineffective child-rearing. The minimum conditions in controlling low self-control, according to Gottfredson and Hirsch (1990), entails frequently monitoring one's behaviour while a child, recognising deviance when it starts and punishing such behaviours.

Again, one major cause of delinquent behaviours apart from criminal parenting and single parenthood, according to the theory, is family size. It is observed that the larger the number of children in the family, the greater the likelihood of each of them being delinquent. Simply put, monitoring and punishment are more difficult when the number of children in the family is greater. In effect, children in a larger family where monitoring and punishment are lax are likely to spend more time with other children outside of their families and are less likely to spend time with adults who tend to be trainers and mentors of these children. To sum it up, the theory proposes that the transmission of low self-control can be passed intergenerationally from parent to child because adults lacking self-control will more than likely be unsuccessful at properly socialising their child (Valasik, 2014).

In a study that sought to explore the association between the self-control theory and online deviance, Donner et al. (2014) utilised a large sample of 488 undergraduate students. The results of the study indicated that the theory is essential for explaining an individual's series of online deviant behaviours such as cyberbullying, hacking, digital piracy and identity theft. While the outcome of the study is valuable for future researchers to build on, the authors pointed out that their study did not consider competing criminological theories other than the self-control theory in explaining the phenomenon. They further called on future researchers to employ a similar but broad measurement strategy for online deviance and also include measures from other criminological theories when generalising the results of the study.

Similarly, a study by Marcum et al. (2015) sought to investigate identity theft behaviours of adolescents under the age of 18 and the predictors of these behaviours. With a total of 1617 participants, the study, conducted through the lens of two criminological theories: general theory of crime and social learning theory, put forward two findings. First, the authors

identified a relationship between identity theft of debit or credit cards and deviant peer association. They further aver that young people, especially males who associate with deviant peers, were more likely to engage in identity theft. The findings of the study also pointed out that persons with better academic performance are more likely to commit identity theft crimes. Although the authors acknowledged that recent research has distinctively shown that people under the age of 18 are not only vulnerable to cyber-victimisation but also have a high risk of committing cybercrime, they also acknowledged that there are gaps in theoretical literature that offers evidence for an understanding of this behaviour in this age group.

The general theory of crime has gained academic consideration for two main reasons. The first is the fact that Gottfredson and Hirsch, the originators of the theory, were ranked first and third, respectively, in terms of citation ranking in a study conducted by Cohn and Farrington (1999). Again, their book *A General Theory of Crime* was ranked second in the citation accorded to all books in the 1990s (Pratt & Cullen, 2000). Despite the positive academic feedback granted the theory and its postulates, it has also been criticised for some reasons (Akers, 1991; Marenin & Reisig, 1995). Akers (1991), for instance, questions the rigidity of the theory and asserts that self-control theory is an *untestable tautology* in that Gottfredson and Hirsch (1990) treated low self-control and the propensity to commit crime as the same issue. Another criticism of the theory is that genetic affinity can impact an individual's ability to socialise and influence criminality (Valasik, 2014).

3.2.2 Routine Activity Theory

The Routine Activity Theory, proposed by Cohen and Felson (1979), is an ecological approach to crime causation in which criminal behaviour can be predicted by the accessibility, location, and presence or absence of environmental characteristics, as well as the presence or absence of

certain types of people. It presupposes that for a crime to take effect, three required elements must be present (see Figure 3.1). First is the motivated offender, second is the suitable target (the suitable target here refers to a person, object or place) and last, the absence of capable guardians in the form of deterrents like police patrols, security guards, neighbourhood watch, door staff, vigilant staff and co-workers, friends, neighbours and CCTV systems (Wada et al., 2012).

Figure 3.1 The Routine Activity Theory of Crime

Source: Cohen and Felson (1979)

The RAT, even though originally postulated as a traditional crime theory, has been adapted and used in various cybercrime studies (e.g., Cox, Johnson, & Richards, 2009; Reyns, 2013; Xiao, Chan, Cheung, & Wong, 2016; Yar, 2005) because of its robustness. Table 3.2 illustrates the various forms of cyber offences the theory has been applied to in previous research as well

as the consideration as sole or combined theory.

Table 3.2 Routine Activity Theory in Cybercrime Studies

Studies	Forms of cybercrime	Usage	Other theories
Olayemi (2014)	General	Combined	• Structural Functionalism Theory • Marxian Theory • The Theory of Technology-Enabled Crime
Kigerl (2012)	General	Sole	N/A
Reyns (2015)	Identity Theft	Sole	N/A
Reyns, Henson and Fisher (2011)	Cyberstalking	Sole	N/A
Navarro and Jasinski (2012)	Cyberbullying	Sole	N/A
Pratt, Holtfreter and Reisig (2010)	Fraud	Sole	N/A
Leukfeldt (2014)	Phishing	Sole	N/A
Reyns and Henson (2016)	Identity Theft	Sole	N/A

Source: Literature synthesis

Bradford Reyns can arguably be counted among scholars who have extensively researched on the routine activity theory. In the article cited in Table 3.1, Reyns (2015) tested a comprehensive routine activity framework on online victimisation. In making a case for using the theory, Reyns (2015) argued that the routine activity theory had been used in studying various kinds of online victimisation. However, most of these studies have been person-based, while his study expands the existing research to examine the effects of online exposure, online target suitability and online guardianship upon phishing, hacking and malware infection victimisation. The study's findings indicated that phishing, hacking, and malware infection victimisation result from online resources for victimisation, which are aided to some extent by people's daily online activities. For example, behaviours such as online banking and

purchasing which are related to phishing targeting and malware victimisation respectively, increase victimisation risks. Nevertheless, specific factors related to banking or purchasing, such as the security of the website or the nature of the internet connection (e.g., public vs private WiFi), are most salient in understanding who is at risk of victimisation and why.

In an earlier study, Reyns (2013) sought to expand recent works aimed at applying the RAT to crimes in which the offender and the victims are not in physical immediacy. In this regard, the author examined relationships between one's online routines and identity victimisation. Conducting binary logistic regression using data from 5,985 respondents, Reyns (2013) found that persons who use the internet for banking and/or e-mailing/instant messaging are about 50 per cent more likely to be victims of identity theft than others. The findings of the study further suggested that online shopping and downloading behaviours also increase online victimisation, while male older persons with higher incomes are also more likely to experience online victimisation. Despite the study's valuable contribution, Reyns (2013) suggested that vital theoretical concepts such as guardianship and target attractiveness take on new meanings in cyberspace, which necessitates adapting the concepts to online environments.

Similarly, Paek and Nalla (2015) employed the RAT to examine how receiving phishing attempts is associated with identity theft. Drawing data from the Korea Crime Victim Survey (KCVS) 2008, the outcome of the study suggested that perceived phishing attempts was found to be a significant predictor for identity theft victimisation.

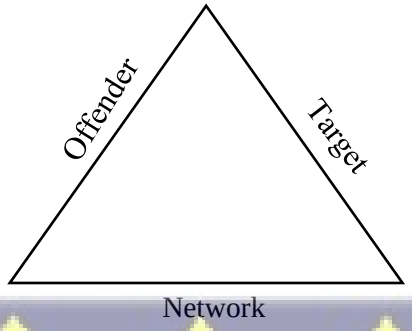
Despite these advancements in the literature, studies that focus on the RAT's technological aspect is sparse, as most scholars employ the theory as it is or combine it with other theories to answer peculiar questions. This may have prompted some researchers (e.g., Pratt et al., 2010;

Holtfreter et al., 2008; Eck & Clarke, 2003) to explore the possibilities of using the theory to explain opportunities for crimes at a distance (Reyns, 2013). For instance, Eck and Clarke (2003) argued that the traditional routine activity theory proposed by Cohen and Felson (1979) "*could be expanded by making one modification"*. In their view, if the target and the offender are part of the same geographically dispersed network, then the offender may be able to reach the target through the network. Eck and Clarke (2003) further posit that networks do not only facilitate interaction at a distance; they can also increase the speed of distant contacts. For instance, whereas traditional crimes under the routine activity theory may unfold slowly and may occur over a long period, the internet can increase the speed with which the same sorts of fraud can unfold. Tillyer and Eck (2009) advanced this argument by establishing that the RAT focusses on offenders making contact with targets at physical locations, which therefore creates a void in the study of crimes that occur at a distance. Tillyer and Eck (2009) further suggested that the routine activities theory is either limited to place-based crimes or needs revision.

These developments have arguably made it imperative to conceptualise the RAT in terms of current trends in technologies and technology-related crimes. For instance, the three elements of the RAT may exist: the motivated offender, the target and the absence of a deterring factor, but in the midst of all these, the role of technology seems to be missing. This further translates into investigating the interrelationship between technology and the constructs of the RAT. In critiquing the theory, Eck and Clarke (2003) suggested networks as represented in Figure 3.2. However, this study conceptualises the theory with the integration of Eck and Clarke's (2003) network and technologies into the original theory: motivated offender, suitable target, absence of a capable guardian and network. To this end, the study will first unveil the categories of people who fall under the offender's construct. Further, concerning the victims of cyber offences as postulated by the theory, the study will solicit the categories of victims that the

offenders target and their characteristics. This will enable the researcher to understand the victims from the perspective of the offenders. The third is to understand the role of guardianship in forestalling cyber offences. This will be done by engaging law enforcement agents and law practitioners.

Figure 3.2 Systems Problems



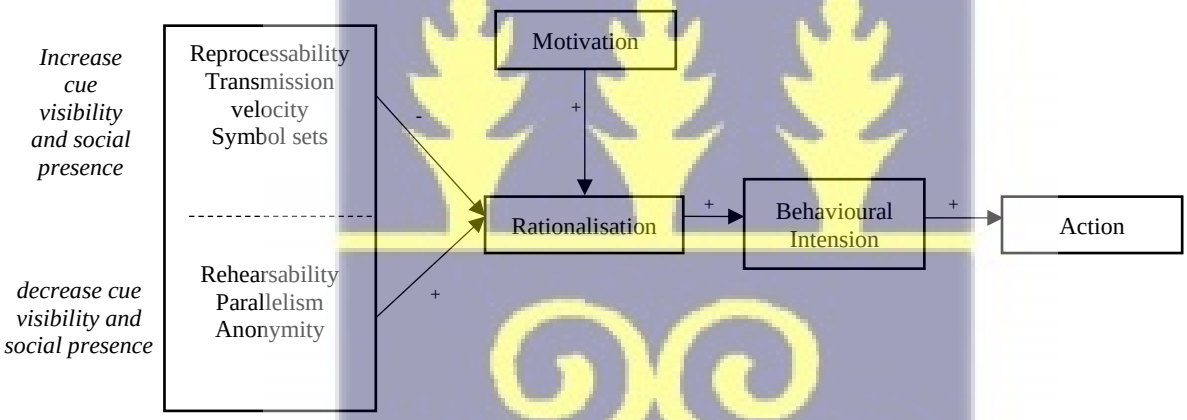
Source: Eck and Clarke (2003)

3.2.3 Model of Media Effects and Fraud Rationalisation

The model of media effects and fraud rationalisation was developed and published in the *Journal of the Association for Information Systems* by Harrison (2018) to determine how capabilities of communication technologies affect the rationalisation of fraudulent behaviours. The constructs developed by the author for the model were based on existing research about fraud rationalisation, media capabilities and computer-mediated deceptions. An analysis of 459 Facebook advertisements and 1,896 surveys among students was conducted. The results of the study which amplified the purpose of the development of the model suggested that media with greater capabilities for reprocessability and transmission velocity decrease rationalising while greater capabilities for anonymity, parallelism, and rehearsability increase rationalising. Harrison (2018) operationalised reprocessability as the extent to which the receiver may re-examine a message. According to Dennis, Fuller and Valacich (2008), individuals may hear, read, or see the message again when a message offers high capabilities for reprocessability.

Harrison (2018) also viewed parallelism as the number of communications in which participants are simultaneously engaged. In expatiating this point, the author avers that some media require a high degree of attention, as such a juggle between multiple conversations causes and obscures cues of deceit (Burgoon & Qin, 2006). Lastly, according to Harrison (2018), rehearsability provides senders with opportunities to fine-tune their messages. Media with greater capabilities for rehearsability provide potentially fraudulent actors multiple opportunities to review and revise their messages, with the goal of hiding as many of the cues of misrepresentation as possible.

Figure 3.3 Model of Media Effect and Fraud Rationalisation



Source: Harrison (2018)

Rationalisation and justification of misconduct play an important role in forming crime (Safa et al., 2019). Rationalisation serves as the vehicle by which perpetrators weigh their thoughts of committing crimes against existing values. Harrison's (2018) conceptualisation of rationalisation stems from the position that when people use media with greater capabilities for anonymity, they perceive a lesser likelihood of punishment and will be more willing to rationalise fraudulent behaviours. The model, as can be deduced in Figure 3.3 combines psychological drivers of behaviours, motivation and opportunistic contextual elements. In that

regard, the author of the model hypothesised that motivation to commit fraud would positively be related to rationalising an act of fraud. Motivation in this sense is operationalised as an important antecedent to the rationalisation of unethical decisions.

3.3 The Ability, Motivation and Opportunity Framework

The motivation-opportunity-ability framework was established to explain how consumers process information in advertisements (Clark et al., 2005). The MOA framework, which MacInnis and Jaworski (1989) postulated, posits that individuals process information based on their underlying motives, opportunities, and abilities (Parra-López et al., 2012). The framework has successfully been used in various disciplines to explain a wide array of behaviours. These include but not limited to knowledge sharing (Siemsen et al., 2008), social media (Parra-López et al., 2012), consumer choices and firm-level decision making (MacInnis et al., 1991; Wu et al., 2004). Nonetheless, the framework has also been used as a conceptualising organising framework for knowledge-management practice and research (Argote et al., 2003; Siemsen et al., 2008) and in management disciplines when discussing an individual' work performance (Siemsen et al., 2008).

As pointed out, the MOA framework was originally postulated by MacInnis and Jaworski (1989) to study the degree to which individuals process information in advertisements. The stipulation of the framework is that all three dimensions must be present for a behaviour to be enacted (Fadel & Durcikova, 2014). For example, a study by Li, Xu, Chen and Menassa (2019) suggested that motivation and opportunity have a direct positive effect on one's energy-saving behaviours. They however found the direct effect of ability on one's energy behaviour not to be significant. It is however worth noting that the study by Li et al. (2019) integrated the MOA

framework with corporate social-psychological constructs from the Norm Activation Model (NAM) and the Theory of Planned Behaviour (TPB).

A study by Leung and Bai (2013) applied the MOA framework and the concept of involvement in exploring travellers' behaviour in social media pages of hotels. The outcome of the study suggested that there are positive relationships between motivation and opportunity with travellers' involvement in hotel social media pages, and their involvement positively impacts their revisit to intended pages. However, it was observed that ability was not significantly related to travellers' social media involvement.

The adaption of the theory in the above-mentioned diverse disciplines gives an insight into the versatility of the framework. Regardless of this development, the MOA framework is arguably yet to be employed in studying any form of cybercriminal activities or behaviours.

3.3.1 Motivation

The first component of the MOA framewrok is the motivation dimension. Motivation has been identified as the driving force that pushes an individual to make a decision. In conceptualising the framework's motivation dimension, Murphy and Dacin (2011) referred to motivation as the pressures to commit fraud, which include social pressures such as how individuals wish to be seen by others. However, it is worth noting that motivation is a unitary phenomenon, as the level of motivation varies from one person to the other (Ryan & Deci, 2000). Motivation can be viewed mainly in two ways: intrinsic (e.g. pleasure and satisfaction) and extrinsic motivation (e.g. wealth) (Ryan & Deci, 2000; Vallerand, 1997). According to Ryan and Deci (2000), intrinsic motivation is the performance of an activity for the inherent satisfaction rather

than for some separable consequence, while extrinsic motivation is observed in the literature as the drive to perform a behaviour to achieve a specific reward (Deci & Ryan, 1987).

A number of existing studies have outlined some motivations towards the commission of online crimes. For instance, while establishing the particularities of cybercrime in Nigeria, Ibrahim (2016) established that cybercrime perpetrators could be motivated in three possible ways: socio-economic, psychosocial and geopolitical. The author projected socio-economic cybercrimes as financially motivated crimes where the perpetrator often has direct contact with the victim. Ibrahim (2016) cited online fraud, romance scam and e-embezzlement as examples of crimes that fall under this category of motivation. Psychosocial cybercrimes involve crimes that are psychologically driven. Unlike fraud-based cybercrimes, the injuries and the benefits of psychological crimes lie within the realm of the mind. Examples of such crimes include cyberstalking, cyber harassment and cyberbullying. On the other hand, geopolitical cybercrimes involve intrinsically motivated cybercrimes that are state-sponsored or involve agents of statecraft or industrial representation. For example, Chinese hackers have expressed patriotic and nationalistic longings in cyberwars with Taiwanese, Indonesians, Japanese and US hackers (Kshetri, 2013b).

Similarly, another study that took into consideration the motivating factors of cybercrime is Ngafeeson's (2010) which sought to develop a motivational model of cybercrime. The author conceptualised motivation as the various factors that *push* people to carry out cybercrime. This push may result from the determinants of crime: unemployment, low median income, poverty, wage inequality and social status, to mention a few. According to Ngafeeson (2010), cybercriminals indulge in cybercrimes driven by their desire to satisfy personal needs. Such needs can be psychological, safety, belonging, esteem and self-actualisation (Maslow, 1981).

In order to commit fraudulent activities online, Rodgers, Söderbom and Guiral (2015) aver that personal integrity and moral standards need to be *bendable* enough to justify the fraud, perhaps prompted by the need to feed their children or pay for a family illness. People are willing to bend their moral principles when they strongly believe that the cost benefit of their rewards are greater than the perceived punishment. Ngafeeson (2010) is of the view that the constant drop in the price of internet and computer technologies (Bakos, 1998), coupled with the high probability of remaining anonymous in the borderless crime terrain (Pocar, 2004), leaves cybercriminals with only moral cost to consider. Though economists omit moral costs in their equations for reasons of measurement difficulty, it remains a vital component in the decision to commit crimes. Moral costs include the cost of reputation and shame (Ngafeeson, 2010). Even though the model is theoretically validated and assessed, Ngafeeson (2010) maintains that it would be good to empirically test it to see its practicality. Recent studies (Barn & Barn, 2016; Donalds & Osei-Bryson, 2019) have started using the model to test its viability, as suggested by the author.

Extant research on cybercrime has studied motivation, possibly using other theories or frameworks such as the fraud triangle theory. In that regard, certain factors that contribute to the motivation of online crimes emerged. These studies and the theories, methods, and factors have been presented in Table 3.3.

Table 3.3 Motivation Dimension Studies

Studies	**Purpose**	**Theory**	**Methodology and context**	**Motivational Factors**
Murphy and Dacin (2011)	To develop a more thorough understanding of the psychological pathways to	Conceptual framework based on the ***fraud triangle***	Qualitative	***Financial*** (e.g., money) ***Pressure*** (e.g., pressure to retain their job) ***Social*** (e.g., the desire to retain

Studies	Purpose	Theory	Methodology and context	Motivational Factors
	fraud, to further fraud prevention and detection efforts.			or gain respect or enhance their self-esteem and status)
Ngafeeson (2010)	To develop a motivational framework for cybercrime classification.	- Maslow's theory of hierarchical needs - Herzberg's 1959 two-factor theory - Routine Activity Theory	Qualitative	Unemployment Low median income Poverty Wage inequality, Social status etc.
Furnell (2001)	To expose the significant variety of cybercrime classification schemes.	N/A	Qualitative	Challenge, Ego, Espionage, Ideology, Mischief, Money and Revenge.
Ibrahim (2016)	To establish the particularities of cybercrime in Nigeria and whether these suggest problems with prevailing taxonomies of cybercrime.	N/A	Qualitative Nigeria	Socioeconomic (financial motivations) Psychosocial (Psychologically motivated) Geopolitical

Source: Literature Synthesis

In considering the motivations for the commission of internet crimes, a complete explanation ultimately must consider the sociocultural environments in which people conduct their daily lives (Choo & Tan, 2007). This then leads the discussion to the configurations of the forces in a person's environment that enable the person's work performance: opportunity (Blumberg & Pringle, 1982).

3.3.2 Opportunity

Opportunity is the second dimension of the MOA framework, which is the circumstances that allow for or facilitate people to perform a behaviour (Hung & Petrick, 2012). Opportunity reflects the presence of enabling environmental mechanisms that facilitate task performance and external contextual factors that enable performance. According to Gruen, Osmonbekov and Czaplewski (2005), this dimension of the framework reflects the extent to which a situation is conducive to achieving a desired outcome. Situational factors such as the time available, attention paid, number of distractions, or number of repetitions that something is available were projected by MacInnis and Jaworski (1989) to be factors that can either impede or enhance a desired outcome.

Based on extant research on fraud and cybercrime, opportunity in relation to the commission of fraud arises when a fraudster sees a way to use his/her position of trust to solve a financial problem, knowing he/she is unlikely to be caught (Kassem & Higson, 2012). For example, in studying organisational fraud practices, Mansor (2015) pointed out that opportunity is created by ineffective control or governance systems that allow individuals to commit organisational fraud. Opportunity further becomes more attractive to perpetrators when the probability of being caught is low (Mui & Mailley, 2015). Although the foregoing discussion on the opportunities provided to fraud perpetrators is essential, there seems to be a lack of studies on this dimension of the framework in relation to cybercrime.

Among the few studies that emphasised this dimension is a study by Whitty (2018), which sought to establish how much culture could be considered as a cause and enabler of Nigerian 419 scams. In her study, Whitty (2018), through a critical review of existing literature, identified some cultural factors that are essential as far as the commission of Nigerian 419

scams are concerned. However, the author was quick to emphasise that the West African cultural explanation must not be overstated as the reason why the 419 Nigerian scam has flourished in the Sub-Saharan African country. Whitty (2018) identified gang cultures which can support and educate young criminals and low-cost crime as opportunities presented to cybercriminals in Nigeria. According to the study, internet fraud in Nigeria, also known as *Yahoo Yahoo,* is operated by young boys who often form loose groups across the world to commit internet crimes. These criminals take advantage of the weakness in the governance structure in prosecuting cybercriminals to commit the crimes.

Despite the seemingly few studies that have been conducted with the opportunity dimension in perspective, a few factors were drawn from the literature which can be viewed as opportunities for the commission of internet crimes by cybercriminals, as illustrated in Table 3.4.

Table 3.4 Opportunity Dimension Studies

Studies	**Purpose**	**Theory**	**Methodology and context**	**Factors Identified**
Aransiola and Asindemade (2011)	To investigate the operations of cybercriminals as a necessary condition for effectively combating the problem.	N/A	Qualitative *Context:* Nigeria	- Collaboration with state authorities - Access to computers and postsecondary school education.
Boateng, Olumide, Isabalija and Budu (2011)	To understand the extent of fraudulent cyber activities as well as measures put in place to address them in Ghana.	N/A	Qualitative *Context:* Ghana	- Lack of technical knowledge by state agencies in investigating, controlling and apprehending online criminals. - Lack of specific laws and policies to

Studies	Purpose	Theory	Methodology and context	Factors Identified
				deal with cyber offenses.
Whitty (2018)	To critically review existing literature to consider how much we can cite culture as a cause and enabler of cybercrime as well as West Africans, with a heavy focus on Nigerians' pathways to cyberfraud criminality.	N/A	Qualitative *Context:* Nigeria	- Gang cultures which can support and educate young criminals. - low-cost crime.

Source: Literature Synthesis

Having discussed the driving force and the environmental leverages to the commission of online criminal activities, it is imperative to delve into the behavioural decisions under the constraints of available resources and knowledge: ability.

3.3.3 Ability

Ability concerns a person's internal skills or proficiencies required to complete a task (Fadel & Durcikova, 2014). Ability is synonymous with skills and competencies and reflects individuals' beliefs about their capacity during their performance (Bigné et al., 2010). In brand information ads processing, MacInnis et al. (1991) conceptualised ability as the consumers' skills or proficiencies in interpreting brand information in an advertisement. Motivation and opportunity may not result in actions unless an individual has the *ability* to process information, make decisions, or engage in behaviours (Hoyer et al., 2012). In other words, without the necessary skills, even a motivated individual is not likely to perform an intended activity. Ability, according to the authors, is the extent to which consumers have the necessary resources (e.g., knowledge, intelligence, money) to make an outcome happen.

Relative to cybercrimes, there seems to be a lack of studies that emphasise the abilities of the perpetrators. Among the few studies reviewed is Hunton (2012), which aimed to extend an earlier research that first introduced the Cybercrime Execution Stack concept by examining in detail the underlying data objectives of the cybercriminal. In establishing why cybercriminals initiate data attacks, the author pointed out that the cybercriminal's ability to use technology and exploit the internet to directly access, manipulate and communicate electronic data is a basic feature in the commission of cybercrimes and other illicit or criminal behaviours. This assertion by Hunton (2012) was found to be an essential aid to support the ability dimension of this study.

Further, in developing a theoretical model profile of hackers, Lickiewicz (2011) also identified some traits perceived to be cybercriminals' abilities in that regard. On this dais, the author mentioned social and technical skills as the abilities that cybercriminals possess. According to the author, social skills constitute an individual's ability to function in a group and internalise social norms. On the other hand, technical skills are the general knowledge concerning programming languages, computer systems, and network functioning. Table 3.5 presents factors found in the literature that reflect the ability dimension of the framework.

Table 3.5 Ability Dimension Studies

Studies	**Purpose**	**Theory**	**Methodology and context**	**Factors Identified**
Hunton (2012)	Extend earlier research that first introduced the concept of the Cybercrime Execution Stack by examining in detail the underlying data objectives of the cybercriminal.	N/A	Qualitative *Context:* N/A	- Use of technology. - Exploit of the internet to directly access, manipulate and communicate electronic data.

Studies	Purpose	Theory	Methodology and context	Factors Identified
Lickiewicz (2011)	To study issues of applying profiling to the field of cybercrimes and to develop a theoretical model profile of hackers.	Conceptual framework based on the **Five Factor Theory**	Qualitative *Context:* N/A	- ***Social Abilities***. Social norms internalisation Relationship with other people Adapt to social norms. - ***Technical Abilities*** The ability to create own programs Knowledge of operating systems, programming languages.

Source: Literature Synthesis

3.4 Neutralisation theory

In advancing existing studies on why people commit fraud, Albrecht, Albrecht and Albrecht (2008) posit that the perceived pressure (non-sharable financial problem) does not necessarily have to be real. The perpetrator just needs to believe that he or she has pressure. Further, perceived pressure, according to Albrecht, Hill, and Albrecht (2006), is not enough to motivate one to commit fraud. Instead, there must also be perceived opportunity. Again, like pressure, opportunity does not need to be real but a perception of the perpetrator that he or she has an opportunity. Lastly, perpetrators must find ways to rationalise their actions as acceptable with personal ethics.

Research has shown that individuals rationalise that their anti-social actions or deviant behaviours are justifiable or excusable (Sharma, 2020; Sykes & Matza, 1957). The rationalisation of such behaviours is technically known as neutralisation techniques. Postulated

by Sykes and Matza (1957), neutralisation techniques can be understood as a set or classification of discourses by which criminals seek to justify or rationalise their behaviours (Enticott, 2011). Thus, individuals 'drift' back and forth between deviant and functional behaviour whilst evading any sense of guilt (Harris & Daunt, 2011).

In the development of the theory, Sykes and Matza (1957) identified five neutralisation techniques that individuals employ to justify their unlawful behaviours. These primary neutralisation techniques are denial of responsibility, denial of injury, condemnation of condemners, denial of victim, and appeal to higher loyalties. *Denial of responsibility* involves the offender rationalising his or her actions in a manner that absolves him or her of responsibility and thus avoids criticism from others (Siponen et al., 2012). *Denial of injury* involves reasonings that deny that the deviant behaviour caused anyone any harm and is, therefore, excusable (Harris & Daunt, 2011). *Condemnation of condemners* is the neutralisation strategy where an individual justifies his or her behaviour on the basis that the victims would have engaged in the same activities if they were provided with the opportunity (Moore & McMullan, 2009). *Denial of victim* is when individuals believe that the victim deserved the crime committed against him. With *appeal to higher loyalties*, offenders cite the importance of maintaining loyalty to small groups rather than society (Enticott, 2011).

While the five techniques proposed by Sykes and Matza (1957) are widely accepted and employed by researchers, there have been subsequent additions to the original five; for example, metaphor of the ledger (Klockars, 1974), defence of necessity (Minor, 1981), denial of the necessity of law and claim of entitlement (Coleman, 1994).

Table 3.6 Neutralisation Techniques

Techniques	Description	Examples	Source
Denial of responsibility	The actors engaged in corrupt behaviours perceive that they have no other choice than to participate in such activities.	*"What can I do? My arm is being twisted."* *"It is none of my business what the corporation does in overseas bribery."*	Sykes and Matza (1957)
Denial of injury	The actors are convinced that no one is harmed by their actions; hence the actions are not really corrupt.	*"No one was really harmed."* *"It could have been worse."*	Sykes and Matza (1957)
Denial of victim	The actors counter any blame for their actions by arguing that the violated party deserved whatever happened.	*"They deserved it."* *"They chose to participate."*	Sykes and Matza (1957)
Condemn the condemner	The actors assume two practices that moderate the salience of corrupt behaviours: 1. Condemn the condemner, 2. Selective social comparison.	*"You have no right to criticise us."* *"Others are worse than we are."*	Sykes and Matza (1957)
Appeal to higher loyalties	The actors argue that their violation of norms is due to their attempt to realise a higher-order value.	"*We answered to a more important cause."* *"I would not report it because of my loyalty to my boss."*	Sykes and Matza (1957)
Defense of necessity	If an act is perceived as necessary, then one need not feel guilty about its commission, even if it is considered morally wrong in the abstract.	*'I had no choice but to do it'.*	Minor (1981)
Metaphor of the ledger	The actors rationalise that they are entitled to indulge in deviant behaviours because of their accrued credits (time and effort) in their jobs.	*"We've earned the right."* *"It's all right for me to use the Internet for personal reasons at work. After all I do work overtime."*	Klockars (1974)

Source: Adopted and modified from Anand et al. (2004)

Neutralisation has been extensively examined in different areas such as digital piracy (Phau et al., 2014; Wilhelm, 2020), cyberslacking (Cheng et al., 2014; Sharma, 2020) and romance

fraud (Offei et al., 2020) to study how individuals attenuate the feeling of guilt and shame that may inhibit their criminal actions (Siponen et al., 2012). For example, Sharma (2020) used the theory to examine the role of consumerism and neutralisation on the cyberslacking behaviour of students in a classroom environment. Using a sample size of 303 students, the author found that apart from condemnation of the condemners, the rest of the neutralisation techniques were found to positively and significantly impact students' intention to engage in cyberslacking behaviours. Similarly, Van Baak et al. (2018) also used the neutralisation theory to study how offenders justify honour crimes. Using data from the United States Extremist Crime Database, they found that perpetrators used a broad variety of justifications to deny their responsibility, ranging from claiming innocence to self-defence. Their study further revealed that along with appeal to higher loyalties, denial of responsibility was also the second most common technique for justifying honour crimes.

Studies that have examined how perpetrators rationalise offences in cybercrime remain few. For instance, relative to romance fraud, Offei et al. (2020) dwelt on the neutralisation and the denial of risk theories to study how online romance scam offenders rationalise their criminal activities. In their study, the authors found that online fraudsters rationalise their crimes by considering online romance as an act that is less aggressive and dangerous compared with other crimes such as murder or burglary.

In studying the pathways to cyberfraud criminality emanating from West Africa, specifically Nigeria, Whitty (2018) identified some reasons cybercriminals attribute to why they commit internet crime as well as the justifications for the commission of those crimes. First among this justification is the fact that West African cybercriminals target Westerners they perceive to be greedy and *stupid*, popularly known in their parlance as Maga or Muga. Cybercriminals

rationalise their crimes against such people as revenge for the perceived injustices they believe were meted out by their forefathers during the era of the Transatlantic Slave Trade. Additionally, cybercriminals (not only West African Cybercriminals) tend to ride on their victims' gullibility by claiming that the onus lies on the victims to recognise when they are being scammed.

Furthermore, cybercriminals from the region rationalise other crimes to be worse than cyber offences. Tade (2013), in a paper to examine the factors that underlie the spiritual dimension to cybercrime in Nigeria, also found that perpetrators assumed that their victims were equally greedy westerners and therefore employed voodoo in luring the victims into their plots. Again, they believe their actions are vengeance missions against foreigners for exploiting Africans to build their countries. Tade (2013) concluded that even though the charms may work for some time, there are unintended consequences such as untimely death, madness and deformation.

Table 3.7 Rationalisation Dimension Studies

Study	Rationalisation	Rationalisation Strategy
Longe et al. (2009)	Criminals take great pride in how much they can exploit victims (usually from the western world) and make a fortune from the greed of some individuals that want to "make quick money." Payback for what the "Whiteman" has done to Africa. They believe that scamming is just a game with a winner and a loser.	Denial of Victim
Tade (2013)	Cyber fraud is a vengeance mission against foreigners. Those being defrauded as equally greedy.	Denial of Victim
Whitty (2018)	Cybercriminals rationalise the legitimacy of their crimes against such people as a revenge for the perceived injustices they believe	Denial of Victim

	were meted out to their forefathers during the era of Transatlantic slave trade. Cybercriminals from the region rationalise other crimes to be worse than cyber offenses.	
Warner (2011)	The perpetration of internet fraud against the state, wealthy Ghanaians or greedy Westerners is not a crime, but a sort of redemptive project of social justice. Sakawa boys justify their activities as the only way to survive in a country where the state is not doing enough to offer social protection to ensure their livelihoods.	i. Denial of Victim ii. Denial of Injury.

Source: Literature Synthesis

3.5 Conceptual Framework

With particular reference to the previous sections on the RAT, MOA and the neutralisation theories, the review points out that each of the dimensions of the theories has its designated factors (See Table 3.8). This section aims to deconstruct the variables into their different aspects and show how they are conceptualised in this study.

While the original MOA framework requires three conditions to enable an individual to perform an activity, this study, based on extant literature and a combination of the RAT, MOA framework and neutralisation theory, requires four conditions for an individual to commit online romance scams. Again, as illustrated in Table 3.8, this study operationalised the dimensions against other studies. The operationalisation of the various dimensions was necessary to align them with this study's focus, that is, online romance scam.

In this study, motivation has been operationalised as the socio-economic conditions that drive individuals to commit internet romance fraud. This conceptualisation of the dimension stems from the fact that factors identified in the literature to have been the motivations for why people commit fraud could loosely be grouped as a socio-economic condition. Financial pressure, for instance, has been studied in relation to fraud from fairly several perspectives. For example, in relating the issue of financial motivation to fraud, Bressler (2009) posits that motivation to commit fraud may be necessitated by the pressure to earn extra money, gambling debt or even drug addiction. Other factors that were found to be contributing to motivation include unemployment, poverty and low median income. It is against this backdrop that questions pertaining to family size, occupational profiles and incomes were included in the interview guide.

As can be deduced from Table 3.8, the opportunity dimension represents the forces in a person's environment that enable him/her to engage in the commission of online romance scams. Existing studies have conceptualised this dimension as ineffective control or governance systems that allow individuals to commit organisational fraud. While this assertion is valid, the current study deals particularly with online romance scams. For that matter, it will not be out of place to accede that the governance systems have well been captured as an environmental force in the operationalisation of the dimension. Offenders' collaboration with state authorities, a lack of clear laws and policies to deal with cybercrimes, and a lack of technological expertise by state agencies in investigating, monitoring, and apprehending online offenders, among other factors, were found to provide fertile ground for online romance scam activities (Boateng, et al., 2011; Aransiola & Asindemade, 2011). To test these factors against the context within which this study is conducted, questions about law enforcement capabilities and third-party collaborations were used to guide the interview process.

Even though the ability dimension has been the least studied, especially in relation to fraud, extensive evaluation of the literature found that cyber romance fraudsters need to possess some skills to take advantage of the opportunities present. In other words, without the ability to engage in cyber offensive activities, motivation and opportunity may not lead to actions. In this study, ability is conceptualised as the social and technological qualities that an individual possesses to perform online romance scams. Among the various factors found under this dimension is the perpetrators' ability to decode and internalise social norms. Principal among the technological factors includes the basic computer skills they possess. While some criminals may possess basic IT skills, others may be sophisticated in their operations.

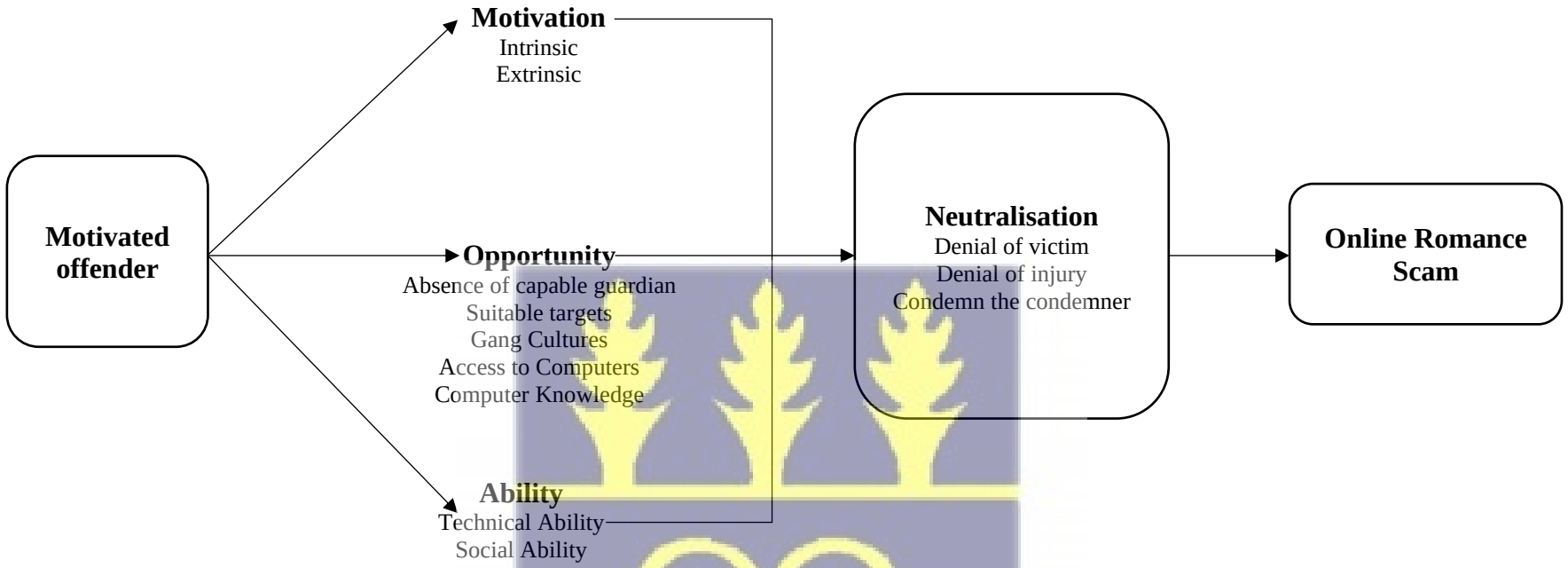
The final dimension studied as far as the model development for this study is concerned is neutralisation. In previous studies, neutralisation has been identified as one's justification for one's fraudulent behaviour due to lack of personal integrity or other moral reasoning. In this case, neutralisation may be viewed as finding non-existent reasons to commit online romance scams (Offei et al., 2020). In this study, however, this dimension has been conceptualised as the justification for one's unlawful behaviour. Extant literature has identified this dimension to have a link to ancestral history and slavery paybacks. While this is relevant in studying the reasons online romance fraudsters assign to their fraudulent acts, most of the studies posit that criminals believe their targets are greedy individuals and are sometimes unintelligent and slow at identifying fraudulent schemes.

It is worth noting that while the MOA framework has been extensively used in past studies, it has arguably not been applied in studying online criminal activities. This study may be one of the first to use the model in this sense. Again, studies that have attempted studying the drive

for criminal activities online have arguably done so only with one dimension or a combination of two.

In light of the preceding discussion, it is critical to note that for a crime to occur, a perpetrator must be inspired (intrinsically or extrinsically), take advantage of the configurations in his or her setting, possess a certain degree of technological or social skills, and find reasons to justify his or her unlawful conduct. The convergence of these theories distinguishes this study in that it goes beyond examining the RAT or the MOA constructs to find the justifications cyber romance fraudsters attribute to their unlawful behaviour.

Figure 3.4 Conceptual Framework of Romance Scam Rationalisation



Source: Modified RAT (Cohen & Felson, 1979), MOA framework (MacInnis & Jaworski, 1989), and Neutralisation Theory (Sykes & Matza, 1957).

Table 3.8 Operationalisation of Constructs and Factors Identified in Literature

Construct/Studies	Operationalisation		Factors
	Previous literature	**Current Study**	
Motivated Offender (RQ2)			
Harbinson and Selzer (2019) Leukfeldt (2017) Choo and Smith (2008)	An individual with a motive to commit an internet crime and with the capacity to do so. Organised perpetrators are groups comprised of like-minded individuals working collectively towards a common goal. Politically-motivated or ideological offenders are largely government sponsored and are known to carry out activities against governments and large corporations.	Individuals with a propensity to commit internet crimes given any favourable opportunity.	• Higher level of education • Higher intellectual capabilities • Basic to sophisticate IT skills • Mostly males
Motivation (RQ1a)			
Murphy and Dacin (2011)	The pressures to commit fraud which include social pressures such as how individuals wish to be seen by others.	Socio-economic conditions that drive individuals to commit internet romance scams.	• Social status (e.g., the desire to retain or gain respect or enhance self-esteem and status) • Unemployment • Low median income • Poverty • Challenge • Ego • Mischief • Socioeconomic (financial motivations) • Psychosocial (Psychologically motivated) • Geopolitical
Ngafeeson (2010)	The various factors that *push* people to carry out cybercrime.		
Opportunity (RQ1b)			

Kassem and Higson (2012)	Chances that arise when a fraudster sees a way to use his/her position of trust to solve a financial problem, knowing he/she is unlikely to be caught.	The forces in the environment of a person that enables the person to engage in the commission of online romance scams.	• Collaboration with state authorities • Access to computers and postsecondary school education. • Lack of technical knowledge by state agencies in investigating, controlling, and apprehending online criminals. • Lack of specific laws and policies to deal with cyber offenses. • Gang cultures which support and educate young criminals • low-cost crime • Routine Activities of victims
Mansor (2015)	Ineffective control or governance systems that allow individuals to commit organisational fraud.		
Ability (RQ1c)			
Fadel and Durcikova (2014)	Ability concerns a person's internal skills or proficiencies that are required to complete a task.	Social and technological qualities that an individual possesses to perform online romance scams.	• Use of technology • Exploitation of the internet to directly access, manipulate, and communicate electronic data • Social norms internalisation • Relationship with other people • Adapt to social norms • The ability to create own programs • Knowledge of operating systems, programming languages.
Neutralisation (RQ1d)			
Kassem and Higson (2012).	Justification for one's fraudulent behaviour. This may be as a result of lack of personal integrity or other moral reasoning	The justification for one's unlawful behaviour.	• Revenge/Vengeance • Greedy westerners • Unintelligent victims
Dellaportas (2013)	Individuals' reconciled contradictions between their intended actions and general attitudes.		
Romance Fraud (RQ3)			
Button and Cross (2017) Carter (2021)	A form of internet crime where criminals pretend to initiate a	A scheme in which the scammer pretends to have genuine affection for a victim in order to acquire	• Military profiles • Sexual abuse

Sorell and Whitty (2019) Cross and Holt (2021)	relationship via an online dating site or social networking site with the intention to defraud their victims".	their love and then uses that goodwill to persuade the victim in order to exploit the victim.	• Crisis • Extortion • Medical and flight document forgery

Source: Literature Synthesis

3.6 Chapter Summary

The chapter began by discussing some theories that have been employed in previous cybercrime studies. It then proceeded to discuss the Routine Activity Theory and how it has also been applied in previous literature, thereby making a case for its adoption in the study. The chapter also discussed the Motivation-Opportunity-Ability framework and how it had been utilised in existing studies. It was observed that even though the framework has been extensively used, it has arguably not been employed in cybercrime studies. While suggesting the usage of the framework in cybercrime studies, the chapter also proposes the need to find out how online romance fraudsters justify their unlawful behaviour. In view of this, a conceptual framework was developed, combining the RAT, MOA, and the neutralisation theory to aid in answering the research questions as well as satisfying the objectives and purpose of this study.

CHAPTER FOUR

METHODOLOGY

4.1 Chapter Overview

The previous chapter focused on the theoretical foundations of the study by reviewing theories used in cybercrime research in existing studies. Based on this, a conceptual framework was developed to guide the carrying out of this research. In light of this, this chapter explains the methods used in this study as well as the rationale for the methodological approach chosen.

The chapter begins by discussing the dominant paradigms in information systems research, leading to choosing a suitable paradigm to carry out this study. This is accompanied by a discussion of the different methodologies and methods used to conduct the research. The data analysis methods used for each research question are discussed at the end of the chapter.

4.2 Research Paradigms

There are variations in research because of how various researchers view the world and interact with the setting around them. These are practically based on the set of beliefs researchers have concerning a phenomenon. According to Kuhn (1970), research paradigms are the entire constellation of beliefs, values, and techniques shared by members of a scientific community. In effect, paradigms are a set of beliefs, values and techniques which are shared by members of a scientific community, and which acts as a guide or map, dictating the kind of problems scientists should address and the types of explanations that are acceptable to them. Kuhn (1970) further emphasises that scholars whose research is based on shared paradigms are committed to the same rules and standards for scientific practice. Guba and Lincoln (1994) viewed research paradigms as a set of fundamental beliefs that deal with ultimate or first principles. Further, paradigms represent a worldview that defines for its holder the nature of the world,

the individual's place in it and the range of possible relationships to that world and its parts. Creswell (2009) also refers to this as worldview – a researcher's overall perspective of the world and the essence of research. Although these beliefs usually remain implicit in most research, they affect the practice of the research. Many scholars in various fields of social science have attempted to analyse research philosophies (paradigms) that underpin their disciplines (Astley & de Ven, 1983; Burrell & Morgan, 1979; Eckberg & Hill, 1979; Guba & Lincoln, 1994; Morgan, 1996; Reingold, 1980).

4.3 Philosophical Assumptions

Burrell and Morgan (1979) postulate that it is convenient to conceptualise social science in terms of four sets of assumptions related to ontology, epistemology, human nature and methodology. The ensuing sections delve into the various taxonomies aforementioned.

4.3.1 Ontology

In research, assumptions are made about "the very essence of the phenomena under study". This, according to Hassard (1995), is known as ontology. Scotland (2012) further posits that ontological assumptions are concerned with what constitutes reality, in other words, *what is.* As such, researchers need to take a position regarding their perceptions of how things really are and how things work. Burrel and Morgan (2006) further argue that all social scientists implicitly or explicitly approach their disciplines via assumptions about the nature of the social world and how it should be researched. Crotty (1998) simplifies the definition of ontology as the study of being; the study of what exists and can be studied; for example, that which a researcher and his/her research community believes to have an existence and for that matter could be studied. Sauders, Lewis and Thornhill (2003) identify two aspects of ontology: objectivism and subjectivism. Objectivism portrays the position that social entities exist in

reality external to social actors concerned with their existence. On the other hand, subjectivism holds that social phenomena are created from the perceptions and consequent actions of those social actors concerned with their existence (Saunders et al., 2003).

Deriving from ontology is epistemology, which concerns the theory of knowledge, its nature and limits (Blackburn, 2005) and how people acquire and accept knowledge about the world (Bisman, 2010).

4.3.2 Epistemology

The epistemological assumption provides a philosophical background for deciding what kinds of knowledge are legitimate and adequate and tries to understand what it means to know (Gray, 2013). Epistemology poses the following questions: *What is the relationship between the knower and what is known? How do we know what we know? What counts as knowledge?* This underpinning is intimately related to ontology and methodology, as ontology involves the philosophy of reality and the view of how one perceives reality (Krauss, 2005; Wahyuni, 2012), whether it is external or a construct of our mind (Jonker & Pennink, 2010). Guba and Lincoln (1994:108) contend that the question of epistemology is "What is the nature of the relationship between the knower or would-be knower and what can be known".

4.3.3 Methodology

Methodology refers to the process and procedures of the research. Naturally, research method flows from one's position on ontology, epistemology, and axiology (Ponterotto, 2005; Wahyuni, 2012). In simple terms, Krauss (2005) posits that methodology identifies the particular practices used to attain knowledge of a phenomenon. Further, Dobson (2002) suggests that the researcher's theoretical lens also plays a vital role in the choice of methods

because the underlying belief system of the researcher largely defines the choice of method. For example, Trauth (2001) posits that in many cases, the choice of lens is often driven by a desire to avoid the shortcomings of positivism.

4.3.4 Axiology

Axiology remains the least discussed philosophical assumption. This is because various literature on paradigms had touted ontology, epistemology and methodology as the three main foci of discussion. For example, Guba and Lincoln's earlier work had been silent on the dimension of axiology in discussing philosophical assumptions of the various paradigms. However, Guba and Lincoln (1995) added it to their set of basic beliefs associated with paradigms (Teddlie & Tashakkori, 2010). In critiquing Guba and Lincoln (1994), Heron and Reason (1997) contend that omitting axiology was a serious issue, and as such; it gives a superficial account of the relation of values to an enquiry paradigm.

Axiology concerns the role of researcher values in the scientific process (Mertens, 2007; Ponterotto, 2005). According to Wahyuni (2012), axiology is concerned with ethics, encompassing the roles of values in the research and the researcher's stance concerning the subject studied. Saunders, Lewis and Thornhill (2003) illustrates: "To conduct a study where you place great importance on data collected through interview work suggests that you value personal interaction with your respondents more highly than their anonymous views expressed through a questionnaire". (p.116)

4.4 Philosophical Debates in Information Systems Research

Since the inception of the field of information systems (IS) in the 1960s, researchers have drawn upon a bewildering variety of theoretical traditions and employed a vast number of specific methods to address a widening range of applied issues (Robey, 1996). As the

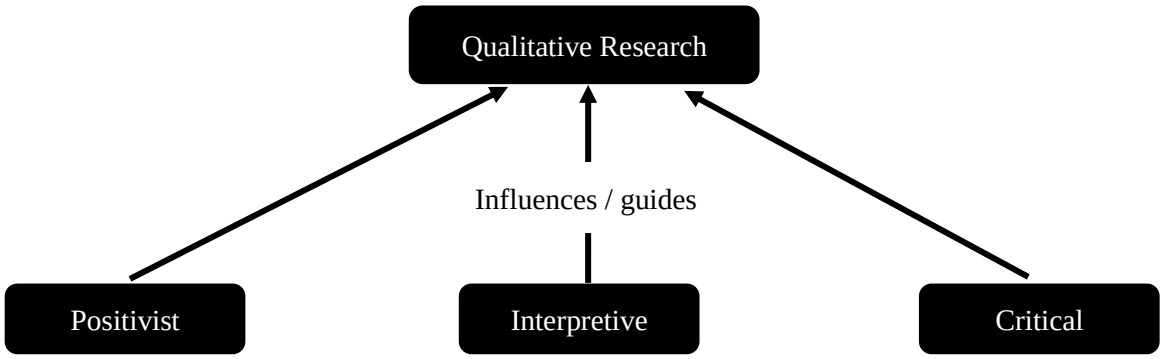
information systems (IS) research arena matures, it is no surprise that a number of researchers in recent years have called for a clearer definition of the underlying philosophy and assumptions of IS (e.g. Banville & Landry, 1989; Hirschheim, Klein, & Lyytinen, 1995; Iivari, 1991; Iivari & Hirschheim, 1996; Mingers & Stowell, 1997; Mumford, Hirschheim, Fitzgerald, & Wood-Harper, 1985; Nissen, Klein, & Hirschheim, 1991; Orlikowski & Baroudi, 1991; Winder, Probert, & Beeson, 1997). Myers and Avison (2002) contend that all research (whether quantitative or qualitative) is based on some underlying assumptions about what constitutes 'valid' research and which research methods are appropriate.

As earlier discussed, Kuhn (1970) defines a research paradigm as a "set of beliefs, values and techniques which are shared by members of a scientific community, and which acts as a guide or map, dictating the kinds of problems scientists should address and the types of explanations that are acceptable to them." These paradigms form the fundamental philosophical assumptions that define what 'valid' research is and the appropriate methods applied in that research (Myers & Avison, 2002).

Distinctions between the paradigms are made explicit by the set of taxonomies that come together to formulate the paradigms (Creswell, 2009). According to various scholars, ontology, epistemology, methodology, and axiology are the essential elements that characterise the underlying distinctions between these philosophical assumptions that shape the paradigms. (Fard, 2014; Eriksson & Kovalainen, 2008; Guba & Lincoln, 1994; Hallebone & Priest, 2008; Ponterotto, 2005).

There exist three main paradigms in information systems research as postulated by Myers and Avison (2002): positivist, interpretive and critical paradigms.

Figure 4.1 Underlying Philosophical Assumptions



Source: Myers and Avison (2002)

4.4.1 The Positivist Paradigm in IS Research

According to Alavi and Carlson (1992), positivism dominated early information systems research. This is confirmed by Fitzgerald and Howcroft's (1998) assertion that the history of IS research had been characterised by the domination of the positivistic research tradition with reference to Orlikowski and Baroudi (1991) and Walsham (1995).

The positivism paradigm has an objective reality, which is single and concrete. The researcher is independent of what is being researched. Researchers instrumentally predict or describe reality; that is, social reality is captured using formal propositions, predictions and control (Lee, 1991). Ontologically, the positivism paradigm has an objective reality, which is single and concrete. Regarding epistemology, it is postulated that positivists presume that reality is objectively given and can be described by measurable properties, which are independent of researchers and the instrument they use (Weber, 2004). Reality in a positivist's research can be known approximately. Distance or objective separateness is between the researcher and the object of study. Knowledge is discovered and verified through measurements of reality. Researchers try to be emotionally neutral and make a clear distinction between reason and

feeling, science and personal experience. According to Orlikowski and Baroudi (1991), such studies serve primarily to test theories in attempts to increase predictive understanding of phenomena. The criteria that are adopted in classifying studies as positivist are evidence of formal propositions, quantifiable measures of variables, hypotheses testing, and the drawing of inferences about a phenomenon from the sample to a stated population. Cavaye (1996) suggests that the methodology chosen depends on what one is trying to do rather than a commitment to a particular paradigm. Thus, the methodology employed must match a particular phenomenon of interest. Different phenomena may require the use of different methodologies (Krauss, 2005).

4.4.2 The Interpretive Paradigm in IS Research

Interpretive research has received increased attention and popularity in many social science fields, including but not limited to organisational studies, political science, sociology, marketing, education and psychology (Orlikowski & Baroudi, 1991). According to Walsham (1995), interpretive research methods adopt the position that our knowledge of reality is a social construction by human actors. Interpretive researchers assume the existence of reality or the real world; however, knowledge of this reality is subjective and not objective (Weber, 2004). In effect, interpretivists assume that it is only through social constructions such as conscious language and meanings shared that reality can be accessed (Myers, 1997). Some researchers, including Kaplan and Duchon (1988), discredited the over-publicised strength of positivism that most computer systems studies are based on methods that measure quantitative outcomes. Because such studies are restricted to readily measured static constructs, they neglect aspects of cultural environment and social interaction and negotiation that could affect the outcomes (Lyytinen, 1987) and the constructs under study. Information systems researchers who use the interpretive paradigm focus on understanding the context and how information

systems impact and are impacted in the context (Walsham, 1995). The interpretivists' assumption of social constructionism, according to Orlikowski and Baroudi (1991), is a fundamental difference between the interpretive and positivist worldviews. Interpretivism asserts that reality and our knowledge thereof are social products and hence incapable of being understood independent of the social actors (including the researchers) that construct and make sense of that reality. This is emphasised by Burrell and Morgan (1979), that the world is not conceived of as a fixed constitution of objects, but rather as "an emergent social process – as an extension of human consciousness and subjective experience". Interpretive research aims to understand how members of a social group, through their participation in social processes, enact their particular realities and endow them with meaning, and show how these meanings, beliefs and intentions of the members help to constitute their social action (Orlikowski & Baroudi, 1991).

The relative ontology of the interpretivist is to understand the intersubjective meanings embedded in social life to explain why people act the way they do (Gibbons, 1987). Further, Orlikowski and Baroudi (1991) assert that ontologically, interpretive information systems research assumes that the social world (that is, social relations, organisations, division of labour) are not "given." Rather, the social world is produced and reinforced by humans through their action and interaction.

By positing a reality that cannot be separate from our knowledge of it (no separation of subject and object), the interpretivist paradigm posits that researchers' values are inherent in all phases of the research process (Angen, 2000). The positivist philosophy challenges the positivist perspective's insistence of a disjuncture between everyday social practices and the language used to describe them. Orlikowski and Baroudi (1991) suggest that the research methods

appropriate for generating valuable interpretive knowledge are field studies, as these examine humans within their social settings. Following the ontological belief that reality is socially constructed, the interpretive researcher avoids imposing externally defined categories on a phenomenon.

4.4.3 Critical Theory in IS Research

Critical theory is founded upon a social theory oriented toward critiquing and changing society. Its work positions towards investigating issues such as exploitation, asymmetrical power, distorted communication and false consciousness. According to Horkheimer (1972), critical theory shines a critical light on the workings of society and finds them dominated by the interests of a wealthy elite who have succeeded in convincing most people that those elite interests are also the interests of society at large. According to the author, it also frames how we look at the world and involves the cultivation of a critical attitude on all levels. As such, the future of humanity depended on the existence of the consciously critical attitude, which is conceived as "part of the development of society". Research in the critical paradigm is often concerned with understanding and applying rationality (Cecez-Kecmanovic et al., 2002; Varey et al., 2002).

The positivist or interpretive research perspectives attempt to predict outcomes or explain the status quo; the critical researcher attempts to critically evaluate and transform social reality under investigation (Cecez-Kecmanovic et al., 2002; McAulay et al., 2002; McGrath & Johnson, 2003). It is concerned in particular with issues of power and justice and the ways that the economy, matters of race, class, gender, ideologies, discourses, education, religion, and other social institutions, and cultural dynamics interact to construct a social system (Kincheloe & McLaren, 2002).

Critical theory researchers assume that reality is a relative transformational periodic construct that needs to be critiqued. The aim is to critique the transformation of the social, political, cultural, economic, and ethnic and gender structures that constrain and exploit humankind by engaging in confrontation and sometimes conflict with the researcher. This implies that the researcher understands a priori what transformations are needed (Guba & Lincoln, 1994). The epistemological belief of the critical perspective is that knowledge is grounded in social and historical practices (Chua, 1986). Truth is negotiated through dialogue such that findings or knowledge claims are created as an investigation proceeds. That is, findings emerge through dialogue in which conflicting interpretations are negotiated among members of a community. To the critical theorist, knowledge does not accumulate in an absolute sense; rather, it grows and changes through a dialectical process of historical revision that continuously erodes ignorance and misapprehensions and enlarges more informed insights.

4.4.4 Critical Realism in IS Research

Several synonyms have been postulated for the word realism in research: Postpositivism (Guba & Lincoln, 1994; Lincoln & Denzin, 1994), Neopostpositivism (Manicas & Secord, 1983), and Critical realism (Hunt, 1991). This section will subsequently adopt the critical realism tag in further discussions.

Critical realism as a philosophical paradigm embraces elements of both positivism and interpretivism (Healy & Perry, 2000). Critical realists argue against empiricism and positivism that science is not just about recording constant conjunctions of observable events. Instead, it is about objects, entities, and structures that exist (even though perhaps unobservable) and generates the events we do observe (Mingers, 2004). On the other hand, according to empiricism and positivism, science involves recording constant aggregations of observable

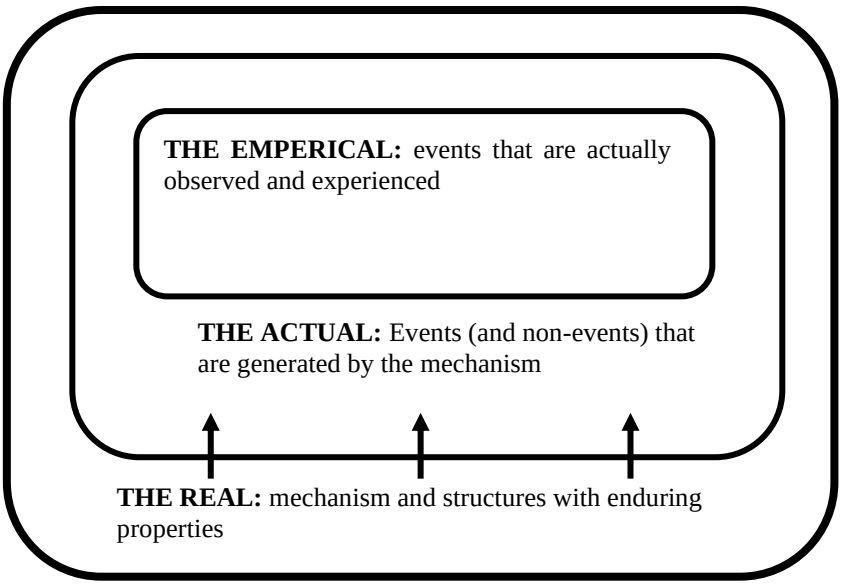
events. This, in effect, suggests that neither empiricism nor idealism can successfully explain such occurrences and that they necessitate some form of realist ontology. Thus, there must be some intransitive domain of objects and events, independent of the researcher's perceptions of them, which can indeed become objects of knowledge (Mingers et al., 2013).

Critical realism accepts the existence of different types of objects of knowledge —physical, social, and conceptual—which have different ontological and epistemological characteristics, therefore requiring a range of different research methods and methodologies to access them. For instance, a particular object of research may well have different characteristics, hence a mixed-method research strategy (i.e., a variety of methods in the same research study) will be necessary and Critical Realism supports this (Margaret et al., 1998; Mingers et al., 2013).

The critical realist ontology lies in two worlds: the intransitive and the stratified (Margaret et al., 1998). Mingers (2004) explains that the first form of stratification is between mechanisms, the events that they generate, and the subset of events that are actually experienced. These are known as the domains of the real, the actual, and the empirical.

From Figure 4.2, Mingers (2004) explains that the real contains mechanisms, events, and experiences, i.e., the whole of reality; the actual consists of events that do (or do not) occur and includes the empirical, those events that are observed or experienced. These distinctions arise from the transcendental arguments above that we should not reduce all events to only those that are observed, and we should not reduce enduring causal mechanisms to events.

Figure 4.2 The Three Domains of Realism



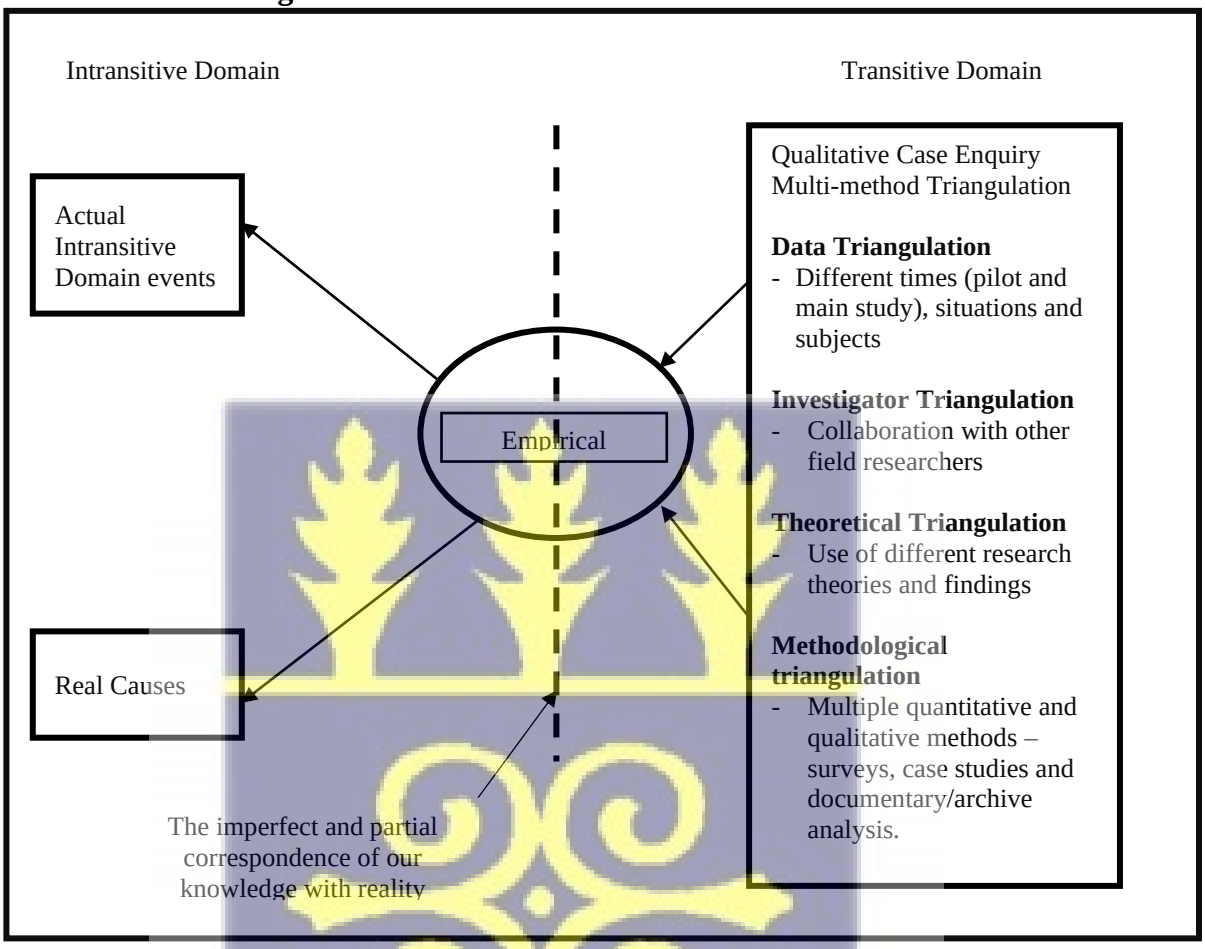
Source: Adopted from Mingers (2004)

The Critical Realist recognises the fragility of knowledge - for epistemological reasons. Knowledge is therefore derived from uncovering causal mechanisms. From the two worlds of Critical Realism, the transitive world is value-laden and changing continually, whereas the intransitive world has underlying structures and mechanisms that are "relatively enduring." The Critical Realist is interested in knowing these underlying structures (Dobson, 2002).

Figure 4.3 depicts the transitive and intransitive worlds proposed by Downward and Mearman (2006). On the left-hand side lies the intransitive domain of structured reality in which real causes trigger real events: the logic of inference required is retroduction of the causes. Likewise, on the right-hand side lies the transitive domain in which knowledge of the intransitive domain is obtained in an epistemologically relative context. The method of science of the critical realist is one of retroduction. This, Mingers (2004) expatiates as where some unexplained phenomena are taken, and hypothetical mechanisms are proposed that, if they existed, would generate or cause that which is to be explained.

Methods such as case studies and unstructured or semi-structured in-depth interviews are acceptable and appropriate within the paradigm, as are statistical analyses such as those derived from structural equation modelling and other techniques (Bhaskar, 1993; Mingers, Mutch & Willcocks, 2013).

Figure 4.3 The Domains of Critical Realism



Source: Downward and Mearman (2006)

4.5 Philosophical Underpinning of the Study

As discussed in earlier paragraphs, this study aims to unearth the mechanisms that underpin the commission of online romance scams in Ghana. In relation to the discussed paradigms, this study employs the critical realist approach as that tends to be more appropriate in unearthing structures of social reality (online romance scams). Further, critical realism fits well with the reality of IS as an applied discipline (Mingers, 2004), considering that cybercrime as a topic

leans towards criminology as a discipline. Mingers (2004) further asserts that critical realism enables the researcher to get beneath the surface to understand and explain why events occur as they do. This provides a solid framework for this study as it goes beyond labelling all IT-related crimes as cybercrime to thoroughly examine the different types of crimes committed by cybercriminals and assess how relevant current laws are in dealing with cybercriminal activities in Ghana. This study further adopted the critical realism paradigm because it also seeks to unveil reasons that perpetrators attribute to their unlawful behaviours.

Ontologically, this study focuses on the social practice of online romance scammers. Interviews with romance scam perpetrators to unravel their motivations, opportunities, abilities, and justifications would necessitate that the researcher outlines the cyber-culture in Ghana. Records and archival examination will also bring to bear the cost effects of cybercrime on the country.

With this in mind, it is essential to comprehend how CR was used in this research. To address this, the study adopted a retroduction research approach peculiar to critical realists (Scott et al., 2013; Strong & Volkoff, 2010). Researchers may use retroduction to move from knowledge of empirical phenomena articulated by events to the creation of explanations (or hypothesising) in ways that have "ontological depth" and can potentially disclose the presence of unobservable entities (Downward & Mearman, 2006). Retroduction, according to Danermark et al. (1997), poses one fundamental question. In this case, *what properties must exist for online romance scams to exist and to what extent is romance scam?* Retroduction's dexterity lies in its ability to assist a researcher in identifying generative processes that allow phenomena like online romance scams to occur. Taking this as a starting point, retroduction becomes a matter of trying to attain knowledge about what internal relations make romance scam what it is (Danermark et al., 1997).

Three main phases manifest in employing the retroductive research strategy for a study. At the initial phase, the study began by examining the observed events and connections in the social phenomena. At this level, the researcher must conduct a thorough literature review on cybercrime to bring to bear the theoretical and conceptual underpinnings used to explain cybercrime in previous studies (see chapter 2). Next, the study hypothesised the presence of real structures and mechanisms and how they describe the observed relationships. From the critical realist's viewpoint, this is done by theorising a model of an underlying mechanism that might have produced patterns seen in the data. It then works backwards from the data towards verifying or otherwise, that model (Mason, 2002). This step has been well outlined in chapter three of this study by combining the RAT, MOA and NT. Lastly, the third step is to establish that the structures and mechanisms postulated in chapter two operate and exist. The researcher then needs to select suitable data collection methods that support the purpose of the study. The findings are then used to redefine the theoretical framework to be more theoretically grounded and practically oriented (Chapters 7 & 8). The phases in the retroductive research strategy and its application in this study have been illustrated in Figure 4.4.

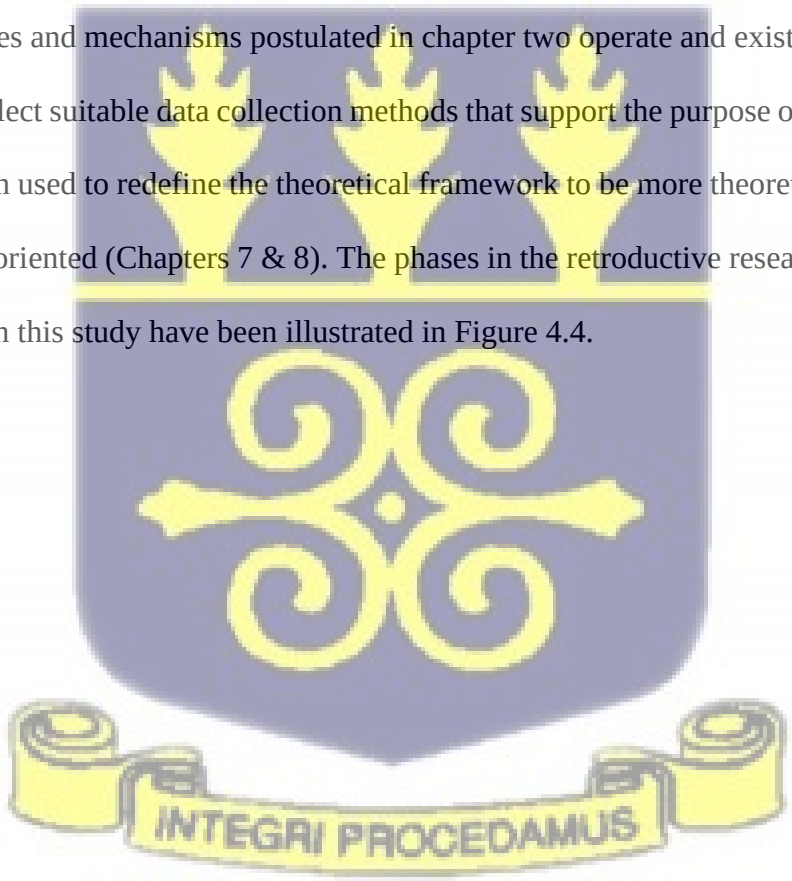
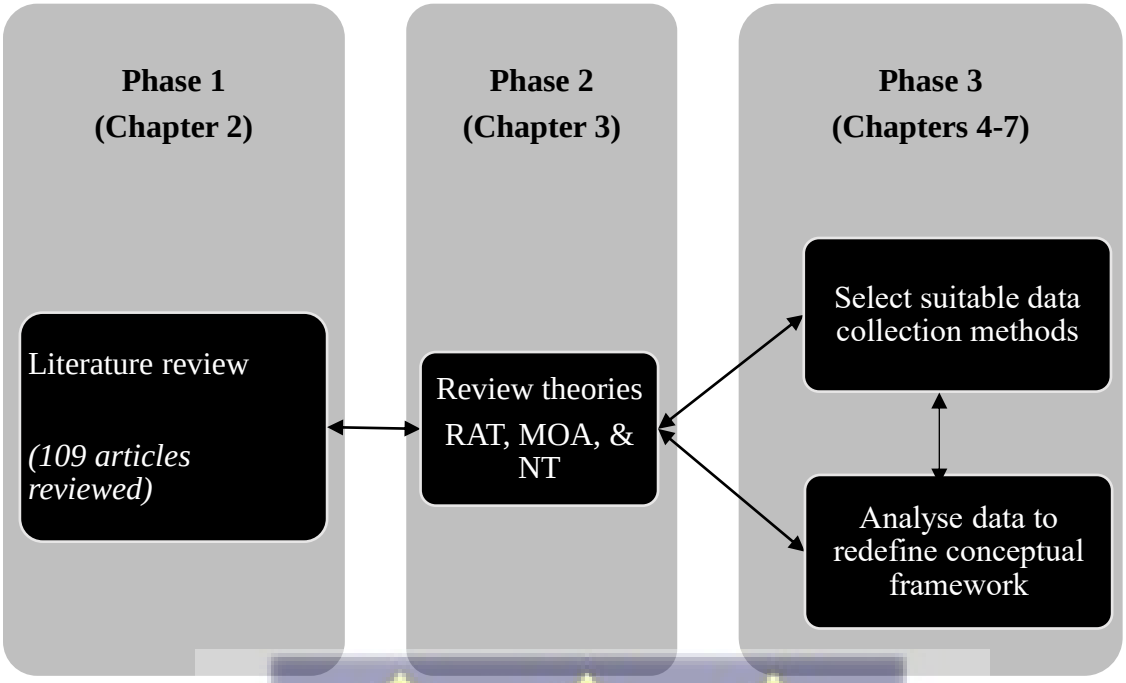


Figure 4.4 Phases in the Retroductive Research Strategy



Source: Author's Construct

4.6 Research Design and Methods

Research designs are types of enquiry within qualitative, quantitative, and mixed methods that provide specific direction for procedures in a study (Creswell & Creswell, 2017). Three types of designs were advanced by Creswell (2009): qualitative, quantitative and mixed-methods.

First, quantitative research involves the interplay among variables after they have been operationalised, allowing the researcher to measure study outcomes (Martin & Bridgmon, 2012). The variables can be measured typically on instruments so that the numbered data can be analysed using statistical procedures (Creswell, 2009). Concerning researchers' worldview, Neuman (2014) posits that quantitative researchers rely more on the principles of positivism and use a language of variables and hypotheses. Second, qualitative research is a means of exploring and understanding the meaning individuals ascribe to a human or social problem (Creswell, 2009). For instance, Jonker and Pennink (2010) contend that qualitative research is

characterised by the fact that the researcher works on the basis of an open question. This is in contrast to closed-ended questions asked by quantitative researchers. Regarding worldview, Neuman (2014) avers that qualitative researchers rely mostly on the principles from interpretive or critical social science. Lastly, according to Creswell and Creswell (2017), mixed-method designs involve combining both quantitative and qualitative research data in a research study. The authors contend that while qualitative data tends to be open-ended without predetermined responses, quantitative data usually includes closed-ended responses such as those found on questionnaire instruments.

With the preceding discussions in perspective, this study adopts the qualitative method. The decision to use qualitative methods was derived from the idea that qualitative methods seek to understand a phenomenon by examining people's experiences and behaviour in the circumstances and contexts in which they act (Kaplan & Maxwell, 2005). In the instance of this study, the researcher seeks to understand the motives for the commission of online romance scams from the perspectives of perpetrators in the natural settings within which they act. While this forms the foundation for the adoption of the method, it is also based on the fact that qualitative research explicitly embraces the contextual (social, institutional, cultural and environmental) conditions within which people's lives take place (Yin, 2015).

4.7 Case Study as a Research Method

The purpose of this research is to unearth the mechanisms underlying the commission of cybercrimes from the perpetrators' perspective to develop a comprehensive online romance scam pathway. To achieve the purpose, this study adopted a case study research strategy. This is done in accordance with Yin's (2002) argument that case studies are the preferred approach when asking *why* and *how* questions, when the investigator has little to no influence over

events, and when the subject is a contemporary phenomenon in a real-life setting, using multiple data collection methods to gather information from one or a few individuals (people, groups, or organisations). A case study focuses on the in-depth understanding of the phenomenon and its context (Cavaye, 1996).

Case study research can be conducted as either a single case or multiple-case design. The choice of which of the approaches to use principally depends on the nature of the phenomenon under study. Yin (2002), for instance, contends that one rationale for the use of a single-case design is when it represents a critical case in testing a well-formulated theory. Theories specify a clear set of propositions as well as circumstances within which the propositions are believed to be true. Therefore, a single case can be used to confirm, challenge the propositions of the theory, and extend the theory. In instances where the same study contains more than a single case, a multiple-case design is preferred. Multiple-case designs allow cross-case analysis and comparison and the investigation of a particular phenomenon in diverse settings (Darke et al., 1998). Both approaches have their advantages and disadvantages.

The choice of a single case approach for this study is grounded in the claim by Siggelkow (2007) that single case studies can cogently describe the existence of a phenomenon. Using a single case study also allows the researcher to question old theoretical relationships and investigate new ones, resulting in a more thorough study. This affords the researcher a deeper comprehension of the topic (Dyer Jr & Wilkins, 1991).

4.8 Case Selection

To better understand contemporary socio-technical phenomena and the causal mechanisms and contextual factors that lead to their emergence, case study research is well-suited to conducting a critical realist's research (Wynn & Williams, 2012). Boateng (2014) suggests that case

selection requires the researcher to be knowledgeable about the characteristics of the case before the beginning of the main case study. With this in mind, a pilot study was conducted before the commencement of the main study. Owing to privacy issues and the purpose of the study, some respondents in the pilot study preferred to perform interviews over the phone rather than face-to-face. The remaining interviews were then scheduled at an internet café frequented by the respondents.

After the pilot study, four out of seven respondents agreed to participate in the study. The four were a group of young men who operated together from the same room (which they refer to as 'the office'). A plausible reason for the other three's refusal to participate could be that one of them was in the process of withdrawing from the act and undergoing personal rehabilitation. The other two's refusal was on the grounds of privacy. The selection of one case for this research stems from the fact that, unlike a positivist research which seeks statistical significance, a CR-based case study research attempts to develop explicit causal explanations of the complex social, organisational, and inter-organisational phenomena encompassing the IS field (Wynn & Williams, 2008a).

4.9 Data Collection Methods

Data serve as the foundation for a research study (Yin, 2015). Benbasat, Goldstein and Mead (1987) posit that multiple data collection methods are typically employed in case studies research. Yin (2018), for instance, advances six sources of evidence in case studies research: documentation, interviews, archival records, direct observation, participant observation and physical artefacts.

4.9.1 Interviews

The primary technique of data collection for this study was interviews. In collecting data for the study, both structured and unstructured questions were used. To achieve the objectives of this study, the question framing for the interviews was done along the constructs of the theories employed for this study. The process to ensure that relevant questions were posed underwent three stages. First was the development of a tentative interview guide to guide the data collection. The second phase entailed the testing of the interview guide in a pilot study with some perpetrators. The outcome of the second stage required modifications of the questions posed in the interview guide. The final phase was the main data collection after all corrections had been made (See Appendix B).

The researcher spent 45 minutes to an hour with the respondents during face-to-face interview sessions and later over the phone to clarify unclear issues. However, for the self-identified scammers interviewed at the public internet cafés, the researcher asked spontaneous questions emanating from the data collected from the group in order to triangulate data collected from them.

4.9.2 Direct Participant Observations

Participant observation involves understanding the worldviews and the ways of life of actual people from the inside in the contexts of their everyday lived experiences (Crang & Cook, 2007). The researcher spent time observing the respondents' cyber activities (cybergang) and individual cybercrime perpetrators who patronised public internet cafés. During this period, the researcher established an excellent relationship with the perpetrators. This was deemed a crucial exercise as the gang members needed to be assured of their anonymity in this study. It is however, worth noting that while this was allowed, not all the activities of the gang were

allowed to be observed. For example, the researcher was blocked from observing *confidential* practices such as engagements on knowledge sharing platforms.

4.10 Population and Sample Selection for the Study

The aim of all quantitative sampling approaches is to draw a representative sample from a population so that the results of studying the sample can then be generalised back to the population (Marshall, 1996). On the other hand, qualitative methods often employ multiple sampling techniques to study a phenomenon, such as purposive, snowball, and theoretical sampling.

This study employed multiple sampling approaches. These comprised purposive sampling and snowballing techniques. By so doing, the researcher actively selected the most productive sample to answer the research questions.

The first respondent to be selected for this study was an internet café owner. This respondent was purposively selected. The choice of selection in this instance was motivated by the fact that the respondent may know potential internet crime perpetrators for snowballing technique to take effect. It is worth noting that several internet café owners, each of whom was earmarked for this study as the initial respondent refused to create contacts between the researcher to cyber-offence perpetrators. In terms of location of the internet cafés and subsequently the owners/operators, the researcher identified locations that have been named in various news and academic articles as hotspots for cybercriminal activities in Ghana.

After interviewing the internet café owner, it emerged that his café attendant was one of the perpetrators (Zack), thereby activating the snowballing technique to take effect. It further

emerged that Zack's elder brother (John) was the leader of the syndicate. This also brought into force the case selection for this study.

The results from the initial data collection from the syndicate and the café operator led the researcher to interview other key stakeholders to understand policies and strategies in place within the country to deal with cybercriminal activities. Table 4.1 presents the timelines for the data collection and population for the study.

Table 4. 1 Detailed Data Collection Methods, Timelines and Durations

Data collection method	Activity	Date	Duration of Interviews
Interview	Internet café Owner (CO)	12th October 2017	23 minutes
	Internet café attendant (Zack)	12th October 2017	53 minutes
	Leader of a cybercrime Syndicate: John	6th November 2017	1 hour and 37 minutes
	Franklyn	6th November 2017	13 minutes
	Lucas	6th November 2017	8 minutes
	Chris	6th November 2017	11 minutes
	Interview with other café operators	10th – 12th February 2018	13 – 18 minutes
	Interview with Bankers (one local and one foreign)	5th – 8th March 2018	15 – 25 minutes
	Interview with Lawyers	19th – 20th March 2018	15 – 25 minutes
	Interview with a law enforcement agent (Police)	10th May 2018	63 minutes
	Interview with Officer of the BNI	18th June 2018	47 minutes
	Interview Cybercrime Syndicate.	18th September 2018	15 – 45 minutes
	Independent Scammers	2nd – 12th October 2018	10 – 15 minutes
	Cybercrime Syndicate	14th March 2019	15 – 60 minutes
Email	Email from an ex-perpetrator (Patrick)	15th September 2019	N/A
Interviews	Cybercrime Syndicate	18th February 2020	15 – 60 minutes
	Independent Scammer (Esmond)	10th March 2020	73 minutes

Source: Author's Construct

4.11 Reliability

Validity and reliability are two characteristics that any qualitative researcher should consider while planning, analysing, and evaluating studies (Patton, 1990). In conducting this study, an instrument for data gathering and data collecting procedures were established as part of the case study protocol to increase the case study's reliability. To improve the dependability of the case study, an initial draft of the interview guide was submitted to an information systems professor interested in cybercrime research to review. The feedback helped shape the interview guide. This was done in consonance to Yin's (2004) recommendation.

Questions in the interview guide were organised to reflect the constructs in the research framework while not losing sight of addressing the research questions. First, questions were asked in relation to the backgrounds of the respondents i.e., education, employment and job experience, age, family size as well as how they got into the act of committing cyber offences. Second, the questions on the mechanisms were posed to ascertain the motivational factors, environmental constellations, their IT educational level and expertise of the offenders, as well as their justifications. Lastly, questions were asked on the strategies they employ in finding, preparing and how they sting their victims. During the interview sessions, some respondents were asked to share screenshots of chats between them and their victims. Though not all participants agreed to share, some of the respondents willingly shared the chat screens as well as other pages. These chats screens helped in conducting a discourse analysis to make sense and directions of the conversations. While the study's primary respondents were offenders, it also gathered data from other parties (i.e., law enforcers, bankers, lawyers). The questions presented to these stakeholders were formulated based on the offenders' responses. Content of the interviews were subsequently transcribed and analysed using Miles and Huberman's (1994) data analysis technique (see section 4.15)

4.12 Construct Validity

To begin, this study did not compromise on data triangulation in order to limit the impact of numerous biases on the research process and outcomes (Wynn & Williams, 2008b). This was done to help with validity testing by combining data from several sources (Carter et al., 2014), as recent cybercrime related studies have adopted this approach due to limited access to offender populations (Ardhianti & Yulianto, 2021; Hutchings & Holt, 2018; Richet, 2022). Internal (interviews with respondents at various times, as well as document and artifact examinations) and external triangulations (interviews with other stakeholders such as law enforcement agents, lawyers, bankers, internet café owners, internet café operators, and other self-identified independent online romance scam perpetrators) were conducted in this regard. Methodological triangulation was also used, which included participant observation, website visits, newspaper stories, and document analysis.

Furthermore, the findings of this study were shared in a live online group discussion with practitioners which included lawyers, police officers, a private security network administrator, a media practitioner and a representative from the cybercrime authority. The forum endorsed the study's conclusions and commented on the passage of the Cybersecurity Act (Act 1038) and its potential to tackle the phenomenon.

4.13 Internal Validity

Two strategies were used to enhance the internal validity of the case study. First, causal links based on the RAT, MOA and NT were established (Cohen & Felson, 1979; MacInnis & Jaworski, 1989; Sykes & Matza, 1957) to explain the mechanism that unite for online romance scams to be committed. In essence, the consolidation of the three theories helped in understanding that cybercrime offenders are individuals who are motivated either intrinsically

or extrinsically and take advantage of their environmental constellations amidst their social and technological capabilities to perpetrate romance fraud.

Second, the patterns predicted by the theory and those in the case study were matched against each other and any observed discrepancies were traced back to their most likely causes. The study discovered, for example, that online romance scammers use two methods to swindle their victims. As a result, there are client-led and scammer-led approaches. Existing romance fraud studies have previously recognised the scammer-led approach.

4.14 External Validity

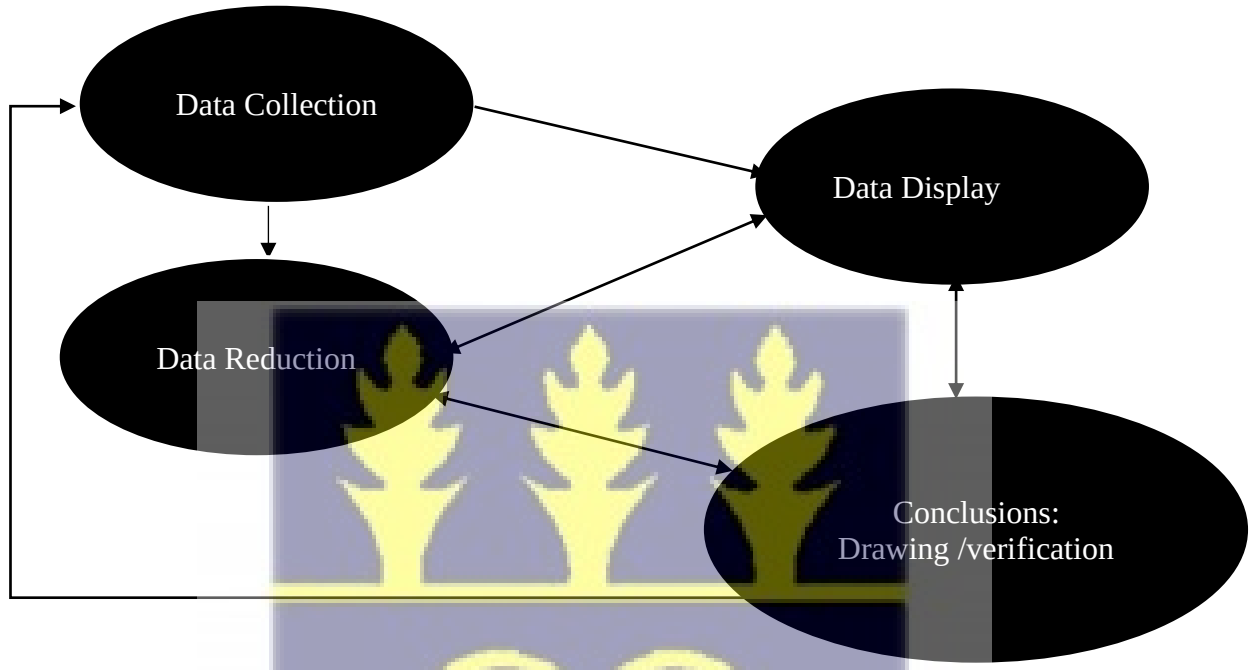
External validity is the extent to which a study's findings are generalisable or the extent to which conclusions may be applicable across varied people or circumstances (McDermott, 2011). Gay and Airasian (2000) contend that external validity is largely concerned with identifying risks or competing explanations that preclude the results of a study from being extended to other environments or groups. Typically, case study technique critiques assert that they do not provide substantial evidence for the generalisability of findings. Yin (2014) however, asserts that the objective of a case study technique is not to statistically generalise but to analytically generalise. Inasmuch as the study used a limited number of primary respondents due to the unique nature of the phenomenon, its external validation is enhanced by the explanatory power of the post-study theoretical framework developed.

4.15 Data Analysis

Data analysis is one of the most important steps in the research process. Pope, Ziebland and Mays (2000) argue that the analytical process of qualitative research starts during the data collection stage of the research. This in their view is because already collected data shapes subsequent set of data collection as researchers have the leverage of going back to refine

questions, develop hypotheses, and pursue emerging avenues of inquiry in further depth. This study's analysis technique is drawn from Miles and Huberman's (1994) qualitative data analysis technique. The authors define analysis as consisting of three concurrent flow of activities: data reduction, data display and conclusion drawing/verification as illustrated in Figure 4.5.

Figure 4.5 Components of Data Analysis: Interactive Model



Source: Miles and Huberman (1994)

4.15.1 Data Collection

Data collection for this study was done in three phases. The first set of data were collected in 2017. This was to aid the researcher in gaining a fair understanding of the nature of cybercrime in Ghana. Questions asked at this stage were general, not pointing to a specific type of online crimes. While the first phase exposed the researcher to the various forms of crimes, it also helped identify and select case subjects for the study. The second phase of data collection entailed interviewing cybercafé operators and owners, lawyers, bankers and cyber-law enforcement agents. This exercise was to align the responses from phase one with the opinions of the listed stakeholders. The second phase responses also helped the researcher understand

what key policies and structures have been put in place to curb the phenomenon. After critical analysis of the data, one form of crime emerged: online romance scams. This then warranted the beginning of the third phase of the data collection process, but with a specific focus on online romance scams. Interviews among the selected cybergang were conducted amidst direct observations. The final stage of data collection was done in 2020 amongst independent cyber-offenders. This was to confirm or contradict the data collected in 2018 and 2019 among the cybercrime syndicate. All information collected during this stage of the analysis was transcribed, which helped the researcher draw similarities, consistencies, and contradictions in the evidence collated.

4.15.2 Data Condensation/Reduction

According to Miles and Huberman (1994), data reduction is the process of selecting, focusing, simplifying, abstracting and transforming the data that appear in written-up field notes or transcriptions. Per their argument, data reduction starts even before data is collected. This is the anticipatory stage at which the researcher forecasts which set of data are or are not suitable to propel the purpose of the study. The researcher's decision on which case, questions, and research framework were appropriate for this study, for example, falls into the anticipatory stage of data analysis.

At this stage of the analysis, raw data collected from the field were organised through coding; the data was reduced into meaningful segments and assigned labels for onward analysis. The next step was to write summaries of the coded data to reduce the weighty statements expressed by the data subjects into fewer words in an effort to move closer to the core essence of the purpose of the research. While at this, the researcher kept focus on not losing the substance of the data as a result of data reduction.

4.15.3 Data Display

Data display has been considered an essential step during the qualitative data analysis or the writing up stages (Verdinelli & Scagnoli, 2013). Miles and Huberman (1994) defines display as an organised, compressed assembly of information that permits conclusion drawing and action. According to Boateng (2016), such displays may be in the form of graphs, charts, tables, networks, tabulating the frequency of events and diagrams of different types. To simplify the complex nature of the phenomenon under study, the researcher used diagrams, tables, and pictures (e.g. see Figures 5.1, 5.2, Table 5.1, et cetera). This was done in consonance with Verdinelli and Scagnoli's (2013) claim that a visual presentation should be as simple as possible, with the right combination of essential and minimal details, and avoid redundant off-topic material or information in order to assist the reader in understanding the intended message.

4.15.4 Conclusion Drawing and Verification

The final stage, conclusion drawing and verification, moves the interpretive effort from the description of patterns and relationships to higher levels of abstraction, subsuming the particulars into the general (Whittemore & Knafl, 2005). At the early stages of the data collection and analysis, the researcher identified and noted possible conclusions. However, those conclusions were ambiguous and revealed inadequate awareness of the facts. These conclusions in that regard were held tentative pending further review and were organised for presentation during analysis when all data were collected and analysed. Conclusions were then presented as lessons (See Table 8.1).

4.16 Approaches to Answering Research Questions

Following explanations in the previous sections on data analysis, this study iterated between the pre-research framework (Figure 3.4), the empirical data, and related literature to identify first-order codes, second-order constructs, and aggregate theoretical dimensions. The iterative nature of the analysis is illustrated in Figures 4.5, 4.6 and 4.7.

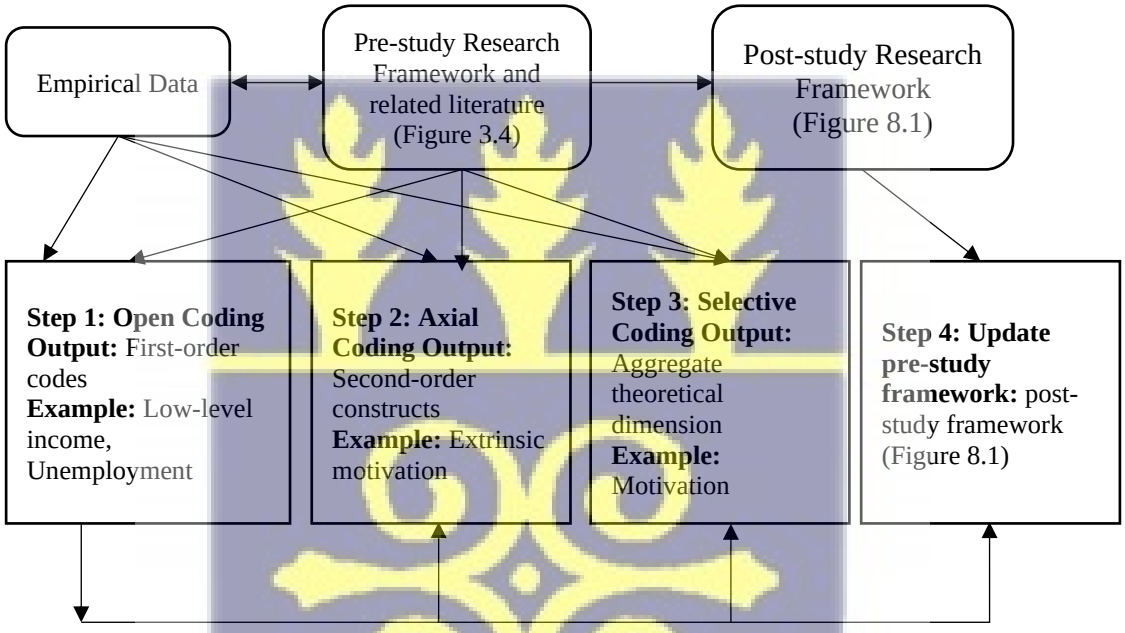
4.16.1 Approach to Research Question One

The first objective of the research seeks to unearth the mechanisms that trigger cybercriminal behaviours. The first step to achieving this objective involved open coding. Open coding entails breaking data down into discrete events and investigating each one attentively to identify concepts, attributes, and dimensions of emergent phenomena (Scott & Medaugh, 2017; Tzeng, 2018). To guarantee that the emerging codes were accurate, codes that were close to the data provided by the respondents were used. For example, a statement like "Thousands of cases go unreported. Sometimes, the public feels guilty for falling prey to cybercriminals. We are trying to educate our people to empathise with them and not to ridicule them. People do not also know where to report cybercrimes since it's not a conventional crime" was coded as "victims' inertia". The first-order codes are the primary output of this stage.

The second step involved axial coding (Scott & Medaugh, 2017; Strauss & Corbin, 1990). Axial coding is a coding framework for synthesizing and organizing data into more coherent, hierarchically structured categories and subcategories that offer complexity and dimension to emergent concepts and their possible relationships with other framework parts. For example, when comparing a first-order code C (Lack of confidence in the police) with first-order code D (collaboration with some police, banking and shipping officials), it was noticed that the two codes culminated into lack of combative laws (see Figure 6.2).

The aggregate theoretical dimensions were derived from the second-order components via selective coding (Strauss & Corbin, 1990). For example, it was evident in the coding that one set of second-order constructs (weakness in combative laws and technology ownership) pointed to the opportunity dimension, whereas the other set (social ability and technical ability) pointed to the ability dimension. The analysis required a continuous modification and reshaping of the emerging conceptual framework as more data are examined.

Figure 4.6 Data Analysis Method for Research Question One



Source: Adapted from Tzeng (2018)

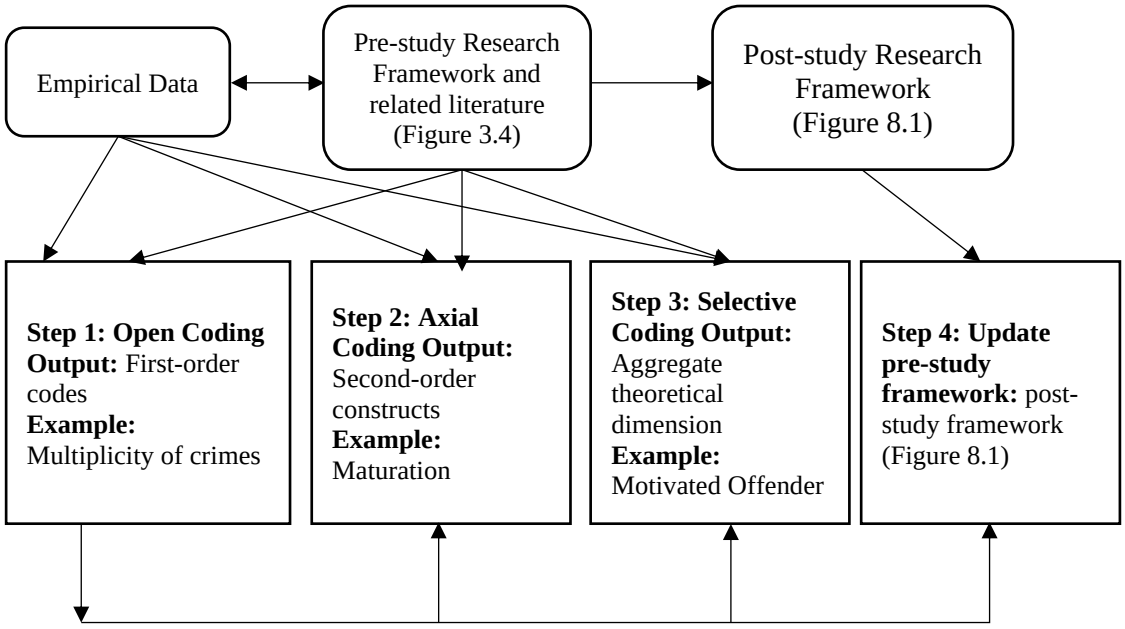
4.16.2 Approach to Research Question Two

The second objective seeks to explore the dynamics of cybercriminal behaviours. To establish the dynamics, respondents were interviewed in four phases (see Figure 5.7) to provoke answers that project the behaviours of the respondents in relation to the commission of crimes over the period of the research.

Similar to the approach in answering the first research question, this study adapted Tzeng's (2018) analysis method as illustrated in Figure 4.6. The first step to achieving the objective was to break the data down into discrete events closely related to the vocabularies of the respondents (Tzeng, 2018). The primary output of this step is first-order codes. Some codes elicited in this step are "Multiplicity of crimes", "ability to ghost IP addresses", "join knowledge-sharing groups" for the maturation stage of the behavioural dynamics (see Figure 6.11).

The next stage was to perform axial coding, which is an inductive, iterative process that combines related first-order codes into a collection of abstract second-order constructs (Tzeng, 2018). In this instance, identical codes were grouped into a collection of constructs such that "multiplicity of crimes" "ability to ghost IPs", "collaboration with law enforcement agents" were all grouped under "maturation". In the third stage, selective coding was used to generate aggregate theoretical dimension from the second-order constructs. For example, it was observed that all the three stages (i.e., creation, maturation and decline) looked at the "motivated offender" dimension of the research framework (see Figure 3.4).

Figure 4.7 Data Analysis Method for Research Question Two



Source: Adapted from Tzeng (2018)

4.16.3 Approach to Research Question Three

The third research objective attempted to explore the strategies that online romance scammers employ in finding, priming and defrauding their victims. The quest to address this objective began with the review of literature in regards to online romance scams and existing persuasive techniques. This was followed up by testing the applicability of the pathways identified (See Figures 2.3 and 2.4) with active perpetrators since the existing trajectories were developed using data obtained from victims and dating platforms.

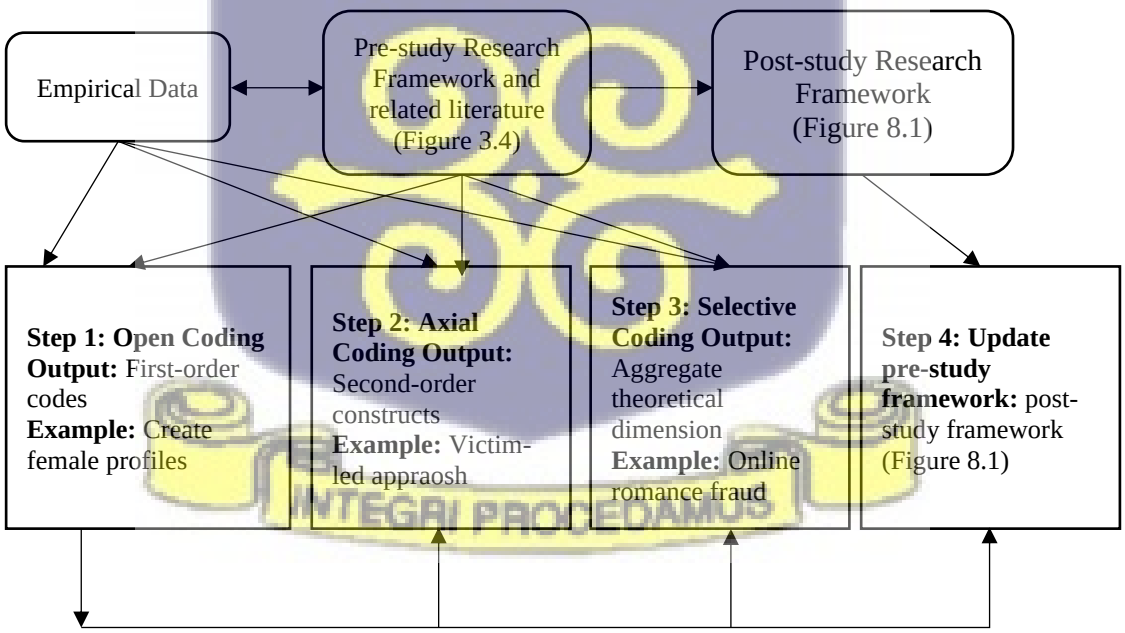
The first stage towards achieving this research objective involved open coding, which included breaking down data from the interviews into individual events and activities (Miles & Huberman, 1984; Tzeng, 2018). To keep the data as accurate as possible, the coding was done in a way that its contents were not too different from the respondents' vocabularies. For example, the codes “create female profiles” and “female accomplices” were derived from the

statement "… I have an account called Sarah Brown. She is my cousin. So, when the money comes, she is the one who will go for it at the bank. When the client calls too, I will give the phone to her and tell her what to say". This stage's main output is first-order codes.

The next step involved axial coding where related codes were combined to form second-order constructs. In this instance, codes such as "creating female profiles", exchanging naked photographs and *camshows*" were coded as "victim-led approach" whereas "creating male profiles", "forging flight documents" were coded as "scammer-led approach".

In the third stage, selective coding was used to generate aggregate theoretical dimension from second order constructs. For example, it was observed that both victim-led and scammer-led approaches pointed to the commission of online romance scams.

Figure 4.8 Data Analysis Method for Research Question Two



Source: Adapted from Tzeng (2018)

4.17 Ethical Considerations of the Study

Ethical consideration was not undervalued in conducting this study due to the unique nature of the phenomenon under consideration. The study draws upon earlier research by Hutchings and Holt (2018) about interviewing cybercrime offenders. Eight principles were drawn from the authors' study which guided the conduct of this research as illustrated in Table 4.2.

Table 4.2 Ethical Consideration of the Study

Identified Principle	Application in this study
Confidentiality of anonymity	Interviews were de-identified during transcription. This include the deletion of information that could be used to trace respondents. Again, while parts of this study have been published in various mediums, no third-party was allowed to have access to the whole transcript in order to track who was spoken to.
Data Security	Data were stored on a password protected computer with multiple security measures. Audio recordings were also deleted after participants confirmed the content of the transcriptions. Data that were of no use to the study were also deleted.
Open Data	Even though this study was partly funded by the BANGA-Africa Project, data from this study is not made freely available.
Morality	Research participants were asked not to mention any activities being planned, or that might have a serious impact, and reminded them of this during the interview if required. Furthermore, the researcher did not partake in the activities of the respondents other than enquiring about their activities.
Researcher Precautions	The researcher used a number of precautions to avoid potential risky situations. In- person interviews took place at public spaces, or areas that were deemed to be safe (e.g., internet cafés).
Presentation of Findings	The building of a narrative and the presenting of research findings, especially for vast volumes of rich data, is a particular problem in qualitative research. The researcher upon presenting findings in this study and ensuing publications ensured that respondents' identities were not disclosed. As such information that were found but deemed to have no relation to this study were not presented.
Incentivisation	The researcher did not pay any of the participants to participate in this study. Without being compensated, respondents took part on their own free will.
Psychological Impacts	The researcher made sure that any information that could have a psychological influence on the participants was left out of the study. As a result, respondents were not required to answer all questions.

Source: Adapted from Hutchings and Holt (2018)

Furthermore, an ethical clearance certificate (see Appendix C) and a letter outlining the researcher's details and the topic were obtained from the Department of Operations and Management Information Systems to interview the respondents and request entry into organisations. Again, the identities of respondents from the various organisations have been blacked-out for ethical reasons.

Lastly, all studies that have been mentioned in this study by way of providing insight, clarification and support have been duly referenced at the end of this thesis (see References) following the laid down procedures of the University of Ghana.

4.18 Chapter Summary

This chapter began by discussing research paradigms in their broad sense. This entailed taking into consideration the dominant paradigms in information systems research: positivism, interpretivism and critical realism and their philosophical assumptions. The chapter thence proceeded to justify critical realism as the preferred paradigm for this study as it helps unearth causal mechanisms behind the manifestation of events.

The chapter further elaborated on the various methodological approaches available for the researcher to carry out the study. The qualitative approach was selected as the researcher seeks to understand online romance scams from perpetrators' perspectives in the natural settings within which they commit the offences. With this in perspective, the next chapter will present the findings of the study.

CHAPTER FIVE

FINDINGS

5.1 Chapter Overview

The previous chapter discussed dominant paradigms in information systems research, which led to the selection of an appropriate paradigm for this study. This was followed by a discussion of the various methodologies available and the research methods used. The chapter also demonstrated how data was collected and analysed for each of the research objectives.

As pointed out in section 1.3, the purpose of this research is to unearth the mechanisms that underlie the commission of cybercrimes from the perpetrators' perspective to develop an online romance scam pathway. In view of this, this chapter presents the findings for this research and delves into the overview of cybercrime within the Ghanaian context.

5.2 Overview of Cybercrime in Ghana

Ghana was one of the first African countries to connect to the internet, and it now has one of the highest internet penetration rates on the continent (Mwakideu, 2021). In Ghana's Information and Communications Technology (ICT) industry, there have been many advancements in the last fifteen years, with the country steadily transitioning into an emerging information technology society. Ghana is still developing its ICT sector, and recent developments in mobile financial services have played a vital role in the sector's rapid development. The Ghana ICT for Accelerated Development (ICT4AD) Policy is the backbone of major ICT developments in the country.

While Information and Communications Technology (ICT) presents opportunities for development, there is a major setback that undermines the full realisation of ICT for social, political and economic transformation. The development and adoption of ICT have led to the

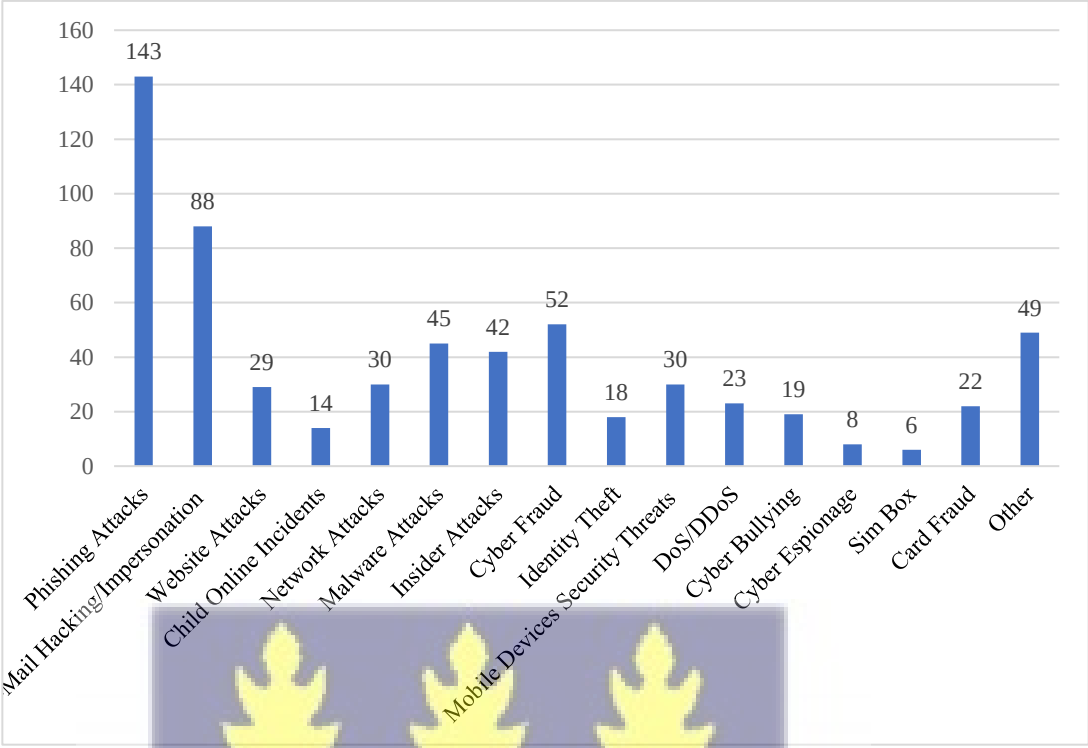
emergence and rise of cyber criminality in Ghana. Cyberattacks target confidentiality, integrity and available ICT assets. While the emergence of cyber criminality is a global phenomenon engineered by the development of ICT and internet technologies, available studies suggest that Ghana in particular and West Africa in general has become a hub for cybercriminal activities. For example, a study conducted by the United Nations Office on Drugs and Crime (UNDOC) – The Globalisation of Crime (2010) – identifies West Africa as a major cybercrime- offending region. The Global Internet Crime Report (2013) by the Federal Bureau of Investigations (FBI) also labels Ghana as being among the top ten cybercrime-originating countries.

To further highlight the country's seemingly global recognition as a major cybercrime region, Ghana has contributed to the global cybercrime lexicon with the word '*sakawa*', which refers to cybercrimes committed by Ghanaian perpetrators. Major international e-commerce operators and online merchants, including Amazon, Paypal and other online retail outlets, have partially blacklisted Ghana – residents in Ghana are sometimes unable to purchase goods and services online with their credit cards because of cyber fraud.

5.3 Cybercrime and cybersecurity Trends in Ghana

Cybersecurity issues have become national security issues for most countries, and Ghana is no exception. The evolution of cyber-attacks, including attacks targeting critical national infrastructure has contributed to the reasons why cyberattacks are now considered not only a social or economic issue, but also a national security concern (e-Crime Bureau, 2017). Figure 5.1 highlights the distribution of cybercrime incidents as reported by the e-Crime Bureau in 2016.

Figure 5.1 Distribution of Cybercrime Incidents



Source: E-Crime Bureau (2017)

5.4 Cybercrime Legislation in Ghana

One significant obstacle to treating and apprehending cyber offenders is the problem of jurisdiction and the capacity of existing legal frameworks to prosecute cyber criminals. Having been aware of the threats posed by cybercrime and its attendant effects on the image of the county and the social stigma that accompanies its citizenry, the Government of Ghana through the Ministry of Communication has promulgated some regulatory frameworks on which legal practitioners rely to prosecute cyber offences. These regulatory documents include the Electronic Transactions Act 2008, Data protection Act, 2012 and until recently the Cybersecurity Act, 2020.

Prior to the enactment of the electronic-related Acts was the Criminal Code, 1960 (Act 29) on which the police as well as lawyers rely to advocate or prosecute cyber offences. The Criminal

Code has been revised on several occasions in order to address the Act's shortcomings. It was, for example, amended in 2003 (Act 646) and then again in 2012 (849). Despite these changes, the Act lacked the rigor necessary to deal with the ever-changing nature of cybercrime plausibly due to the times within which it was promulgated (1960) in relation to internet penetration in Ghana. Regardless of the Act's inability to address modern forms of crimes such as cyber offences, parts of the Act were captured in the Electronic Transactions Act, 2008 (Act 772). Ghana's Parliament voted the Electronic Transactions Bill into law in December 2008. The Act's principal purpose is to secure the cyber space as a means of minimising criminality that may impair residents' ability to safely transact businesses. As with the Criminal Code, the ETA contains deficiencies due to the Act's jurisdictional restrictions, which are detailed in section 142/2 of the ETA, 2008. (772). It holds that "This Act shall apply if, for the offence in question, (a) the accused was in the country at the material time; (b) the electronic payment medium, computer or electronic record was issued in or located or stored in the country at the material time; (c) the electronic payment medium was issued by a financial institution in the country; or (d) the offence occurred within the country, on board a Ghanaian registered ship or aircraft or on a voyage or flight to or from this country at the time that the offence" (Electronic Transactions Act, 2008). Cyber criminals, on the other hand, take advantage of these legal loopholes by utilising virtual private networks to *"ghost"* their locations while conducting cybercrimes (see section 6.2.3).

To address the loopholes in the aforementioned Acts, the Parliament of Ghana passed the Cybersecurity Act, 2020 (Act 1038) which was assented on the 29th of December, 2020. The Act was enacted to govern cybersecurity operations in the country, to foster the growth of cybersecurity in the country, and to address other related problems. The legislation covers everyone who is involved in or could be harmed by cybercrime or a cybersecurity event.

Cybercrime is defined in this Act as the "use of cyberspace, information technology, or electronic facilities to commit a crime"; an act or effort to obtain unauthorised access to, disrupt, or misuse an information system or information kept on an information system is characterised as a cybersecurity event, regardless of whether it is successful or not. As a result, the Act covers a wide range of people, including government actors, banks and financial organisations, telecommunications corporations, energy and utility businesses, and transportation operators.

Despite the Act's comprehensive breadth (Act 1038), its seeming silence on type II offences remains elusive while it appears to be extremely vocal about protecting critical infrastructure and businesses, as well as protecting children (identified in the Act as most vulnerable).

5.5 Cyberculture Among Ghanaian Youth

As indicated in chapter one of this study, ICT and internet penetration in Ghana have been on the ascendancy. Prior to this, internet cafés in the country became extremely popular and served citizens who could not afford dedicated internet services, giving them the opportunity to temporarily use the cafés at a fee. An Earlier study by Burrell (2012) on internet café patronage and usage suggested that the typical internet user in these cafés – young, educated but not to the university level, and usually not from affluent families – had a different relationship to 'information' than older, university educated, and affluent users. The two groups of people identified both have different purposes for using the internet cafés. According to Burrell (2012), the younger groups spend more time in the cafés and usually come in groups pursuing entertainment and occasionally playing computer games. University graduates and students, on the other hand, patronised the internet cafés to research and acquire information.

The internet cafés served as a place where young people are, if at all, immune to the supervision of their parents. This, therefore, afforded young patrons of internet cafés the opportunity to gang up at nights after school hours at the cafés for conversations and sometimes arguments about subjects of interest. By so doing, harmless thoughts of looking for pen pals are developed into seeking partners on online dating platforms and thence developing petty cyberdeviant skills. It is worth noting that some cyber deviances are learnt through shared opinions of peers in the cafés. Examples of cyberdeviant behaviours among youthful café patrons include identity theft, credit card fraud, e-commerce fraud and online romance scams. It is common knowledge among the youth who patronise the cafés that there are specialisations in the above-mentioned forms of cybercrime. As such, they offer their services to their counterparts for percentages of the proceeds that emerge from such ventures. It is against this backdrop that cybergangs emerge. The ensuing sections present a detailed picture of one of such groups and their activities.

5.6 Cybergang Group Profile

The *group,* which began informally with seven people in 2015, currently houses four core members with one female affiliate. Before its inception, the members patronised the same internet café in their neighbourhood. However, at the time, they operated independently of each other, a situation which they referred to as *each one for himself*. John, the group leader, began engaging in internet crimes in 2008 while in senior high school. He graduated in 2012 and furthered his education at a reputable IT training school in Ghana. He dropped out of the IT training in 2013 after becoming disappointed with the program. Of the other three in the group, all of whom attended senior high school, two graduated while the third dropped out. John's reason for discontinuing the IT training program emanates from the fact that he wanted to study *"ethical hacking"*. According to John, his expectations of becoming proficient in the discipline

within the shortest possible time were not met. Table 4.1 summarises the educational level of the group members and their years of experience in perpetrating cybercriminal activities.

Table 5.1 Perpetrator Profiles

Pseudonyms	Age*	Educational Qualification	Experience	Family Size	Job Experience
John	27	Senior High School Leaver with partial IT training.	9 years	10 (including parents)	-
Franklyn	25	Senior High School Leaver.	7 years	6(including parents)	-
Chris	25	Senior High School Leaver.	7 years	5 (including parents)	Electrician
Lucas	26	Dropped out of senior high.	6 years	7 (including parents)	-

Source: Field data

John, the chief informant for this study, is the first of eight siblings (five males and three females). He claims that *"my family is not a rich family. My mother is a trader, and my father is also a watchman. I am the firstborn, and I have four brothers and three sisters".* John believed that the family's financial resources were insufficient to meet all their needs and *"being the firstborn I need to sacrifice and help my parents to take care of the rest".* He claims that he had previously searched and applied for jobs in several institutions without any success. According to him, his engagement in cybercriminal activities was not due to his inability to get employed but to his interaction with his peers in his vicinity. He opines that *"... No, not at all. I didn't start because I didn't get a job. I can't tell how I started, but all I remember is that every evening [we], me and my friends gather at the café to chat and argue about football and other things. But one day I asked one of my friends to shop for something for me, after that, I asked another one to shop another thing for me. I realised it was not difficult so I started doing it myself."*

In the first instance of data collection, John was a patron of the café he identified as the starting point of his engaging in cyber-offences. Prices at the café ranged from GHS 1.50 for 30 minutes to GHS 2.50 for one hour of browsing using the internet café's computers, while those who came with their laptops enjoyed "Bring your own device" prices of GHC 1 for 30 minutes and GHC 2 for an hour. He avers that *"I only buy time when I have a meeting with my client*[2]*, shop or track a control.*[3]*"* As to the frequency of meeting with the clients, John craftily schedules his meetings such that he can hold multiple sessions concurrently. This minimises the number of times he visits the café and saves money by not buying browsing hours at different times. He opines that *"it depends. Sometimes I can do three at the same time so that I don't waste time coming here and going … It also makes my mind active".*

During the second stage of data collection, John had rented a space for himself, thereby moving away from the family. At the time, he had been able to take care of one of his younger brothers (fifth born) who had completed Senior High School and was working as the café attendant at the café John used to frequent. Further, John, at this time, was not working alone. He had intelligently recruited three more of his friends (Pseudonyms: Franklyn, Chris and Lucas) to work with him under the same roof away from the public. John explained their decision to come together: *"everybody has his strength and weakness. I am good at shopping. Another person is good at chatting clients. So, we decided to come together since we are all doing the same thing. At one point, my light will shine. At another point, another person's light will shine so we will all not go dry at the same time".*

[2] Client is the name given to romance scam victims/would-be victims by cyber-offenders
[3] Contextually used for shipped items or the ability to swindle a client.

Apart from the fact that the group decided to keep their activities out of the public eye, John claims that working outside of the café is less expensive in terms of actual costs and privacy. He claims that *"I don't go there nowadays because I now have internet at home. It is cheap, it is always on. Whenever I want to do something, it is available… We are just four in this room. So, no one can steal your client, no one can point fingers at you that you are a sakawa*[4] *boy and other things".* As to whether it is right or not to refer to him as a sakawa boy, John claims that *"I am not a sakawa boy. They are those who visit the Mallams and things… I don't do that".* He further maintains that *"No one can judge me with what I am doing; unless a judge tells me that I am a criminal, nobody can call me a criminal".* John was of the view that cybercriminal activities are common practices that people commit even without knowing. He asks, *"those who have been downloading movies from torrent sites … do they pay? Do you call them cybercriminals? Do you?".* John maintains that cybercrime is less a crime than traditional crimes *"it is better to do something than do nothing… I can't go and rob from people… No, I can't do that".*

In 2020 when the final set of data for this study was collected, the group had had one more member who can more or less be described as an *aide-de-camp* (Pseudonym: Caleb). According to John, Caleb's role in the team was based on necessity. He explains that *"… he has something that he is doing already. Myself and the other* [three] *guys, this is all we do. He is a graphic designer. He works with a printing press at Circle. We only call him when we need to make changes on some documents and create flight schedules and things. So, he is not always with us".*

[4] Unlawful cyberculture that combines internet crimes and Ghanaian traditional rituals.

John was 30 years old at the time of the final stage of data collection in 2020. He had rented an apartment for himself, living independently of the family. John owned a 2010 Toyota Corolla vehicle, a MacBook Pro 2017 model and an iPhone 11 Pro Max. When asked about the source of funds for purchasing his mobile phone, he expounded that *"I shopped five for someone and I got two, and I gave one to my brother because he brought the address and sold the last one".*

Chris, the second group member, was 26 at the second stage of data collection in 2018. He was an apprentice electrician before joining the group in 2018. He claims that *"I started to learn electronics so that one day I can open my own shop… when will I finish learning and start looking for customers for my shop ... so I stop".* Chris' transition from ganging up at the café for chats and arguments into perpetrating cyber-offences was not different from that of John. He opines that *"One day I had a problem with my phone so I asked John to shop it for me, but he asked me to look for address before he can do it for me".* In the scheme of perpetrating cyber-offences, perpetrators have their specialities in the forms of crimes they commit. As John puts it, "*everybody has his strength and weakness. I am good at shopping. Another person is good at chatting clients".* As such, since certain items cannot be delivered directly to Ghana due to shipping restrictions, shoppers (like John) will have to find an address in the United States to send the items to, from where they would be shipped to Ghana. In the event that John does not have an address, he would be compelled to look for someone in Ghana who has a client through whom the items would be shipped to Ghana.

Chris continues *"So, I asked a friend who was chatting someone and John used the address to shop the phone for me … then I started doing it myself".*

On how he was recruited into the group, he maintains that *"they are my paddies*[5] *, and we move together, so we do everything together".*

Franklyn, the third member of the group, is the second of three siblings. Aged 25 at the time of the second set of data collection in 2018, he dropped out of school while in his second year of studying visual arts. When asked why he dropped out of school, Franklyn opines that *"I didn't continue because of school fees; my senior sister too didn't finish because of school fees. My junior brother is also going to school, but I don't know what will happen".*

On why he engages in internet scams, Franklyn explains that *"there are no jobs and man must eat";* however, he joined the group as a result of association. He narrates that *"I can't tell how I started, but I know it is through when meeting at the café every day after training".*

Lucas is the last member of the syndicate. He is a senior high school graduate who studied general arts. He is fluent in English and specialises as the chat lead of the group. He claims that *"I started doing it while in SHS".* Lucas is the third in a family of seven and lives independent of the family. At the time of the last set of data collection, Lucas had shipped a *"consignment"* containing two laptops, four iPhones and a camera he intends to sell. He opines that *"John did the shopping, but we used my client to ship the items to us".*

Among the crimes perpetrated by the syndicate are online romance scams, credit card fraud, identity theft and online shopping.

[5] Group of Friends

5.6.1 Online Dating Scam

The group's ultimate motive is to acquire wealth, and as such online romance scam seems to be at the top of the agenda. This activity commences with the creation of attractive profiles on social media sites, especially online dating platforms. In this instance, identities provided are either of a rich old man (60 years plus) seeking a financially sound middle-aged female 'lover' or a young philanthropist and financially independent female (usually between 25-35 years) seeking equally rich old men for relationships. They use appealing descriptions such as military profiles, globetrotters, civil engineers, and international social workers undertaking humanitarian projects in Africa.

One of the independent scammers interviewed for this study, for instance, explains that *"I download pictures of American and Russian models who are not popular ... but I make sure they have camshows*[6] *otherwise when the client asks me to show live videos I can't"*. While this tends to be the beginning of a long journey of the scam process, it is essential to the perpetrator because *"if you don't use a beautiful lady, you will stress"*. Further, the perpetrators use unsuspicious names that conceal the fact that they are not whom their profiles say they are. John reveals that *"We use names like Sarah Brown. So that the client will not know we are chatting from Ghana"*. Such self-descriptions tend to appeal more to women, mostly single, divorced, or widowed, seeking to begin new relationships. However, it must be noted that the scammers create multiple accounts, stalk and send friend requests (known among the perpetrators as *winking*) to one particular target until he or she falls for one of the fake identities.

[6] Naked webcam videos

The first step to starting the relationship after a client falls for a profile is for the scammer to find out the experience of the client, that is, to ask how long he or she had been looking for a relationship on the dating platform. According to Zack, *"it can take one year for you to control someone who has been there for long but like six months for someone who has been there not for long".*

The scammers begin forging appealing stories about themselves to get the targets glued to the friendship. At this phase, the motive is to surge intimacy with the victim with the intention of building trust. To do this, both parties introduce themselves and discuss their past experiences and plans to rebuild a lasting relationship (see Figure 5.2). Lucas, for instance, narrates that "*Sometimes I tell them my former wife left me because I was travelling too much ... but now that I want to come back to my country and settle, I need someone as sweet as you".* When affection and trust have fully been established, the scammers then migrate the client out of the dating platform to Google Hangout, WhatsApp or Telegram. According to Zack, *"... if you don't move them out of the site, the site can know that you are not real, and they will remove you".* Apart from site audits, some clients also report suspected accounts, necessitating investigations by the dating platforms. He continues, *"sometimes those that we wink*[7] *can report us if they think the account is fake ... they have not blocked me before, but I know some people who have been blocked ... the small boys".*

[7] Scammers' invitation to clients to establish relationships

Figure 5.2 A Chat Screen Between a Scammer and a Client

Source: Field data

In order to maintain anonymity, the perpetrators employ virtual private networks (VPN) software. This, in effect, warrants them the leverage to decide their browsing locations. Such schemes work for scammers who pretend to be globetrotters or humanitarian seeking funding and engaging in humanitarian projects worldwide. In responding to how they maintain anonymity, one respondent indicated that *"... I install SOCKS on the computer, so I am able to control from anywhere ... sometimes it is a business trip. Sometimes too I visit my family".*

The second stage of the scheme is to keep the client bonded to the relationship. Scammers then maintain constant contacts with the client, for example, by sending early morning messages and goodnight love messages. It is worth noting that scammers do not exchange phone numbers with the clients at this phase of the scheme. As such, all contacts or chat sessions are held on the dating platform. Further, the scammers create fun and love stories, all in the quest to keep the clients in the relationship. At this stage, they maintain a perfect storyline in order not to create a sense of mistrust. In the words of John, "*you have to correctly remember the story for each client".*

After establishing trust at this level, scammers need to be in tune with topics raised by the client. For example, some clients raise political issues within the countries the scammers claim to hail from and the latter must be able to respond to discussions put up by the clients. In this instance, scammers cling to search engines such as Google to conduct fast searches on topics similar to the ones posed by their victims. For instance, a café owner narrated that *"I saw someone who didn't even know the name of an airport in London ... the person asked him which airport she should expect him and he said London Airport Limited... the woman ended the conversation".* Scammers who go through this test stage then go on to purchase flower gifts from online giftshops to be sent to the would-be victim, thereby instilling confidence in them that the relationship is real. This gesture then opens the way for exchanging gifts between the two and grants the scammer access to the victim's addresses and phone numbers for illegal online shopping deliveries.

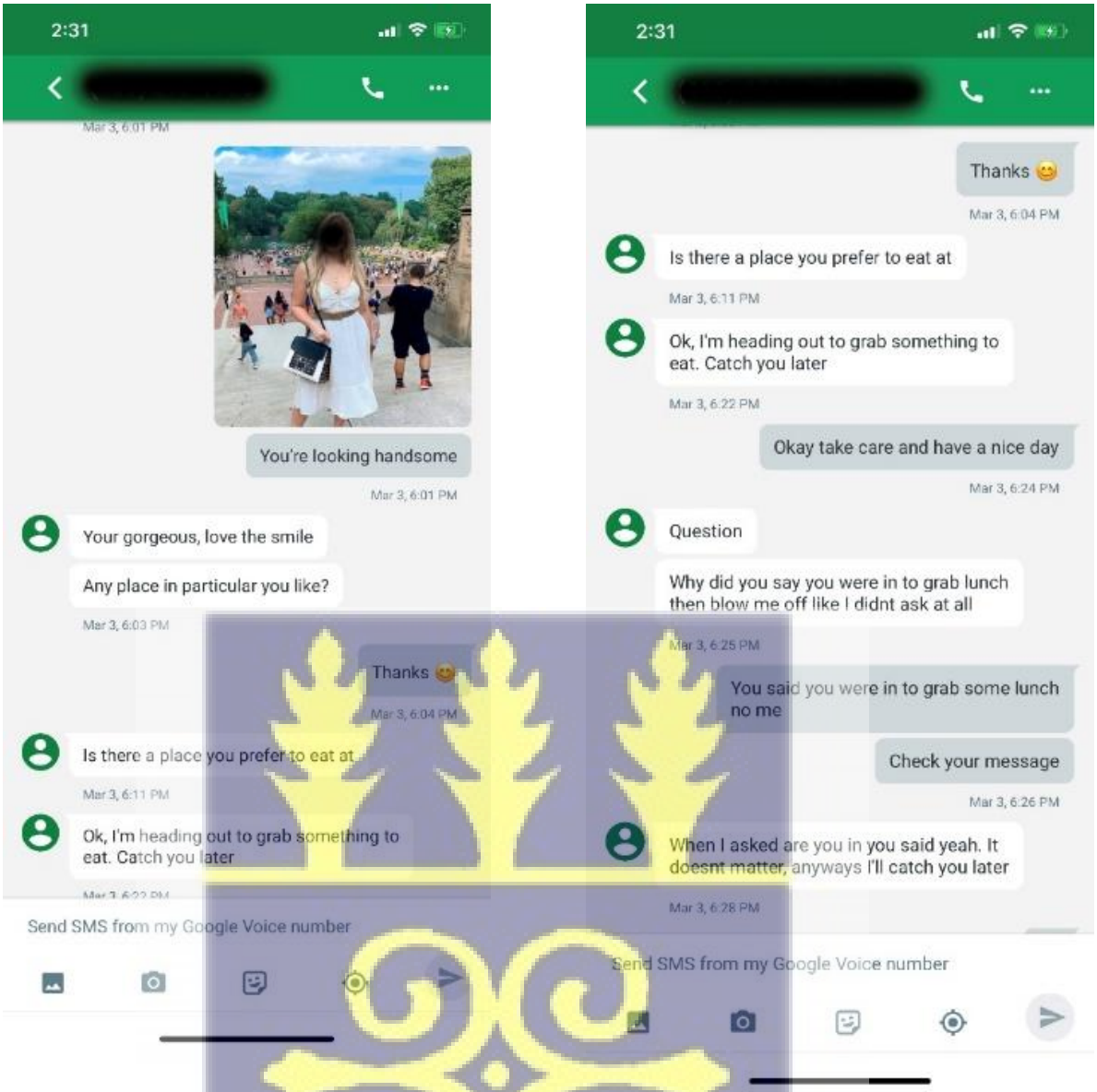
After some weeks, the scammer then begins to request little gifts such as mobile phones, google play cards, and wristwatches. This initiative marks the beginning of the second set of activities which can be led by either the scammer or the client. Scammers make the demands when they

lead the discussion and vice versa. Victims' ability to provide little gifts then signals to the scammer the ability to give more. In some instances, the scammers request small amounts of money between $100 to $500. Zack, for instance, avers that *"When I ask him for $100 and they give, I will wait for some time and let John send him a flower for me … so, I tell him I wanted to surprise him but I wanted to test him if he trusts me … then next time I will ask him for around $500 and buy him something like a watch … if he gives me the $500, it means his mind is soft, so I will push him to John so that he can win like $1000 or more for me".*

Another form of the scheme is to create tragic stories that speak to the emotions of the victims. It is worth noting that this scheme is usually orchestrated against women, while the scheme described above is best suited for men. Zack narrates that *"So, I was robbed on the day that I had to leave back to America by the taxi driver who drove me to the airport. So, I am stranded in Ghana right now".* This then means the criminal needs to stay in the country for a while to *"Get a new passport, a new flight ticket, a new phone".*

Intelligent victims or victims who are familiar with how cybercriminals work abruptly end the relationship at this stage. However, those who fall prey send the monies for the 'scammer' to come home so that they can start their family. Here, the scammer requests the victims to send the funds through an assistant since he (scammer) has lost all belongings due to the robbery, *"and then we agree to meet at the airport".* The newly introduced assistant in real life, in most cases, are the real identities of the scammers or the female accomplices.

Figure 5.3 Chat Screens of a Client Testing a Scammer.



Source: Field data

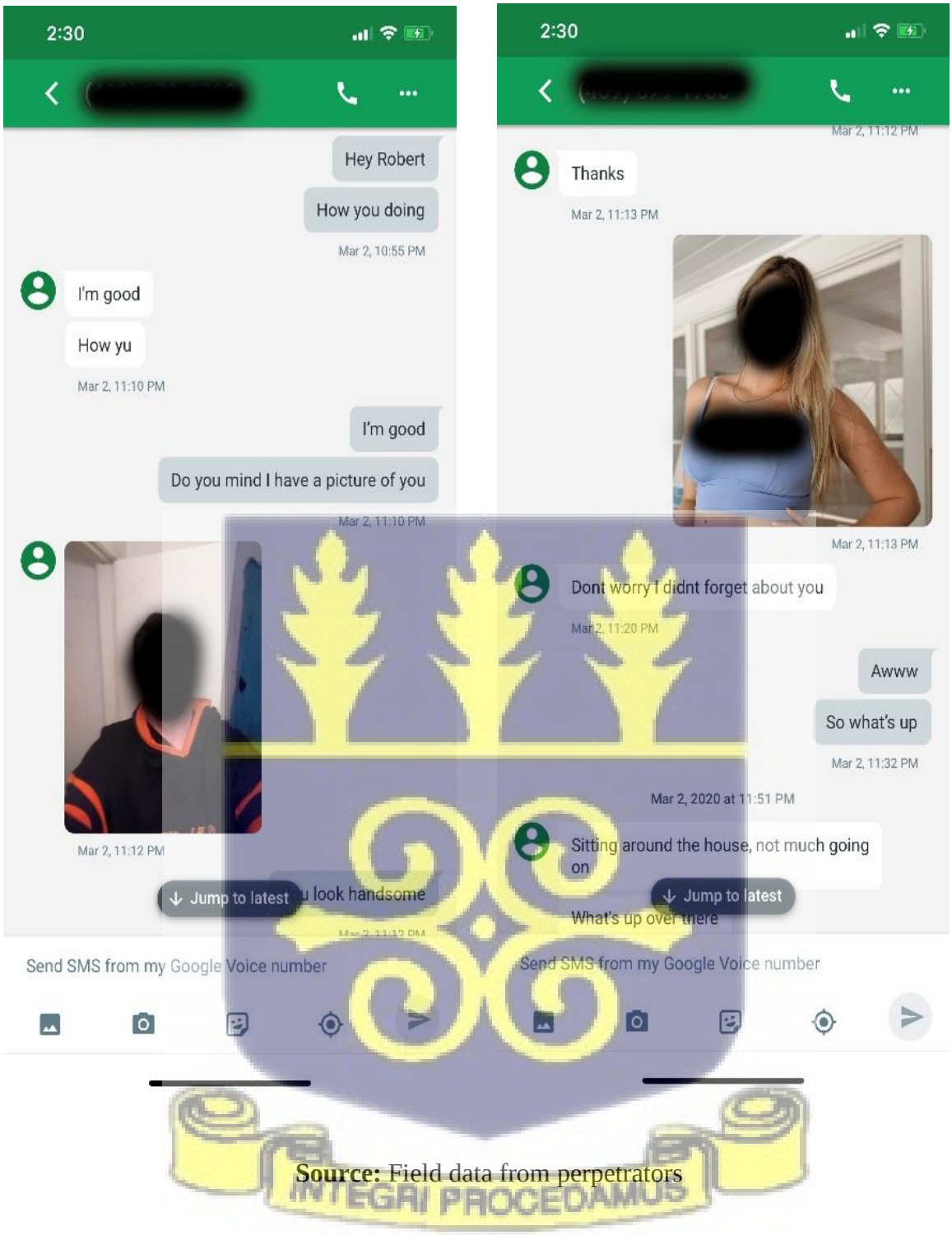
After the funds have been received, the scammers hire Caleb's (a graphic designer) services to fabricate flight documents to persuade the victims that they will be returning home at the agreed date and to the agreed-upon destination airport. The scammer never shows up, and that marks the end of the relationship.

Figure 5.4 A Snapshot of a Forged Flight Ticket

Source: Field data from perpetrators

The second type of scheme is the situation where the client leads the conversations. For instance, while in the scammer-led scheme, the scammer demands monies, the client demands naked pictures and videos from the scammer in the client-led scheme. In such instances, the scammer devices another scheme of demanding money in exchange for the photographs and videos. Zack explains that *"if they ask for pictures, I will tell them if I send 10 naked pictures, you will give me $200 and if I send a video, you will give me $500 … they ask for reduction and I send the video or pictures and they also send the money"*. The demands for naked pictures are for the most part not for explicit images. Thus, *"he will send a picture like he is half naked and I will also send him half naked picture. I will not send him anything again till he asks for it and I also start asking the money"*.

Figure 5. 5 Chat Screens of a Client-let Approach



Source: Field data from perpetrators

The scheme then progresses to the next stages depending on the success rate of the exchanges. Since the scammers do not own the photographs they use, they must formulate tactics to end the transactions. As a result, they threaten the clients with sexual exploitation. An independent

perpetrator posits that *"when I feel the money is not coming like at first, I will create confusion and he will get angry … then I will also tell him that I will report him to the FBI because he has used me … some of them will send some money so that I won't do that and some of them will block me".*

5.6.2 The Complex Web of Online Crimes

Data collected during the interview indicate that most scammers in Ghana knowingly or unknowingly engage in multiple internet crimes at a point in time. This is because the bulk of the scammers' activities are intertwined (see Figure 5.6). The following sections describe the crimes and their interrelationships.

5.6.2.1 Credit Card Theft

As outlined in the preceding narratives, the scammers employ the scheme of purchasing items to win their victims' trust. The scheme works in two ways. First, scammers circulate monies received from victims. For instance, they seek funding from one client and lavish it on other clients (gaining trust). The second strategy is to engage in credit card theft. It is worthy of note that, while for some of the scammers, the motive is to profit from their clients, others aim at using them as conduits for shipping illegally purchased items. Data collected throughout the research indicated an advancing sophistication in credit card theft among scammers. For instance, in the first instance of data collection, the scammers were using credit card number generating websites where they generate credit card numbers randomly, after which they are required to find identities behind the cards. These cards are then used to purchase flowers and other gifts for their clients to cement the legitimacy of their relationship. According to Franklyn, *"... if I want her to believe me more, I buy things with the credit card for her so that she will know that I am original ... As for her, she don't know but me, I am testing the card … if the card works, I will shop and ship to her to ship to me in Ghana".*

Nonetheless, data collected in the final phase revealed a more sophisticated credit card theft that aids romance scams. This is a usual practice for scammers whose main objective is to use the victims to transit illegally shopped items from online shops such as Amazon, Walmart, and eBay. In this practice, scammers buy credit cards from the black-market using internet currencies such as bitcoin and Ether for between $5 and $30. Esmond narrates that *"If you have a $100 bitcoin, for instance, you can purchase about ten cards. But there are other sites that sell the cards for about $20"*

The black-market agents are faceless people who hack into individuals' bank details and sell cards at cheaper rates to scammers. In this case, "*They* [hackers] *may not know* [the amount of money on the card] *because, for them, they hack from the store. For example, he may have been successful in hacking Walmart. So, he may not know the amount on the card, but we have ways of checking whether the cards are working or not".*

The risk involved here is that the credit cards may or may not contain money. However, in instances where the cards contain some amounts of money, the scammers use the actual details of the cards to buy from online retail shops such as Amazon, Apple, Walmart, Best Buy et cetera, but the difficulty in this venture is the blacklisting of some countries including Ghana by these shops. This then compels scammers to resort to alternate means and that is by finding lovers/clients on online dating sites who may later fall for their tricks (see section 5.5.1). After the trust is won, the client is told the scammer is organising a charity initiative in Africa and that donors would be sending donations to him in Africa. However, they (the donors) cannot do so because most shops in the states do not ship directly to Africa. Esmond narrates:

"You will use your real name. When chatting the client, you chat with a different name so tell the client that you are sending the thing to your assistant or you have won a contract and

supplying the people so they should send it to the contact person in the company you are supplying to that is, if they are laptops and other gadgets. But the story depends, if the packages are clothing, you can tell the client that you are donating it to a charity organisation so the name on it is the one receiving the package."

This, in effect, implies the lover would have to receive all donations and ship them to the home country of the scammer in the name of his personal assistant. It is worth noting also that some clients do not ship the items. Such victims-turned-scammers also terminate the relationships with the Ghanaian scammers.

5.6.2.2 Gift Cards and Trading

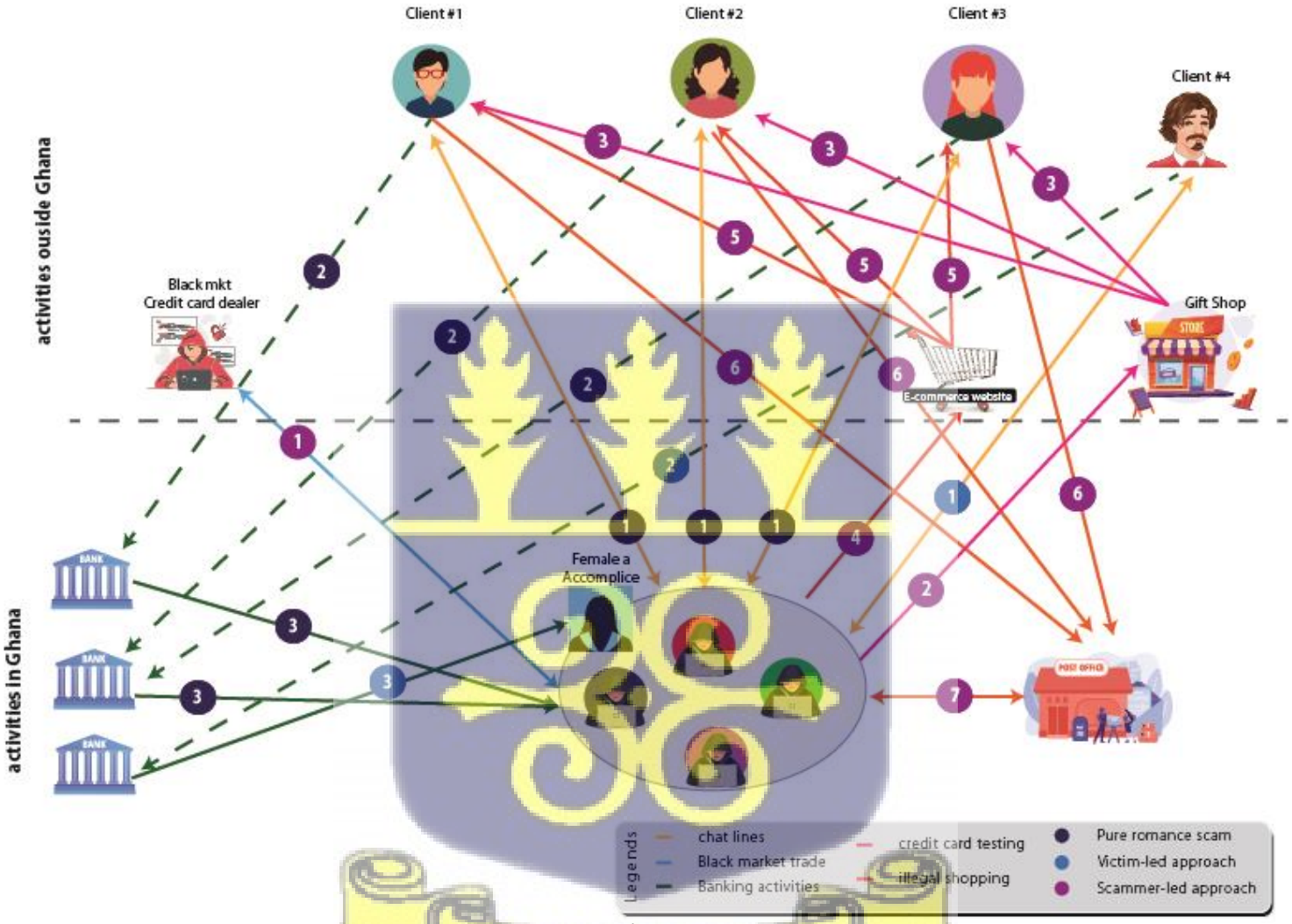
One common activity found among independent perpetrators was the gift card trade. While data collected in the early stages of this study did not reveal this trend, it became apparent in the final phase of the data collection. Gift card trading is popular among cybercrime beginner-perpetrators. It can loosely be described as the exchange of gift cards gained from online romance scams for cash or bitcoin. This is also common among scammers whose main aims are not necessarily to defraud clients of vast sums of monies—for example, between $100 to $200.

While some perpetrators are fortunate at getting buyers for their cards within their communities, others resort to trading on online platforms where their returns are in the form of bitcoins. An independent perpetrator narrates that *"When they win the card, and they don't get anybody to buy it here, they go to www.abxsd.com* [8]*to sell it … but some of them cannot do it, so I trade it for them and I also get small cut".*

[8] Truncated

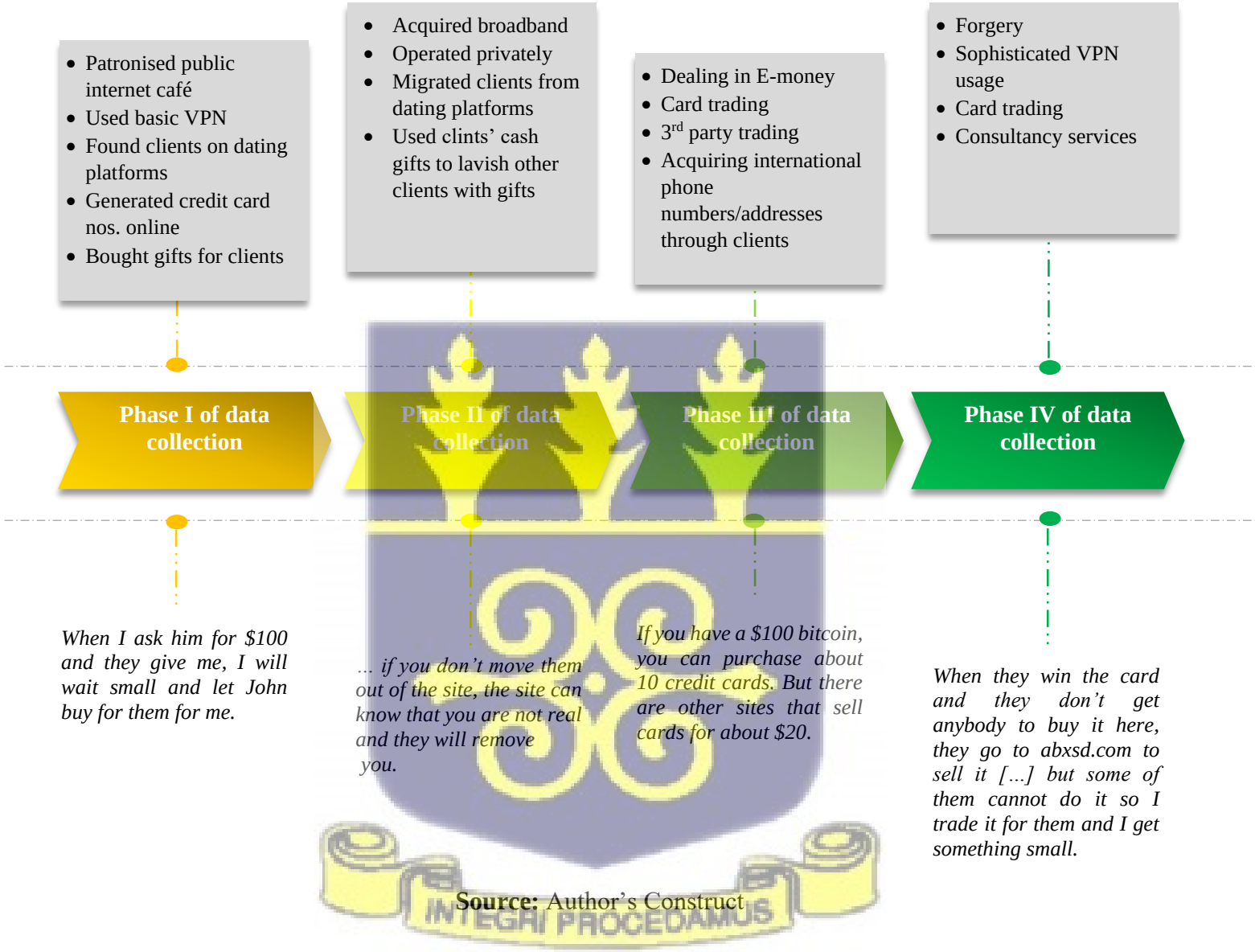
After trading the cards for bitcoins on the platform, they then trade the bitcoins, for example, for mobile money, which is then withdrawn from mobile money merchants. Essentially, by the time the money gets to the scammer, he would have lost about 70% of the total value of the deal.

Figure 5.6 The Complex Web of Online Romance scam Activities



Source: Author's Construct

Figure 5.7 Behavioural Dynamics During Longitudinal Data Collection



Source: Author's Construct

5.7 Other Stakeholder Perspectives on Cybercrimes in Ghana

In the quest to triangulate data from the field, eight bankers, seven café operators/owners, eight lawyers and two public law enforcement agents were interviewed.

5.7.1 Bankers

The minimum period of service for bankers interviewed was three years. In Ghana, one requirement for withdrawing or redeeming sums of money for international money transfer is any national identification card such as a Voter's ID, Passport, Health Insurance Cards or Drivers' license. Also, recipients must fill out a form indicating their full names, name and address of the sender, the amount he/she is redeeming and access codes. However, there are instances where recipients are required to answer random questions at the request of the sender

When asked whether the banks had ever suspected fraudulent withdrawal of funds from their banks, one respondent answered in the affirmative that "*Yes, we know when they withdraw money suspected to be fraud monies".*

The follow-up inquired about their pre/post-withdrawal actions, but the respondent said, "*There is nothing we can do about it because they present every legal document and fulfil all mandate required of them. In short, we lack the legal evidence to deny them of their withdrawal. One of their tricks is also that they don't come themselves. They send ladies".*

Another follow-up was why the bank does not report the suspects for investigations to continue from there. The respondent answered that "*Like I said, first of all, we don't hold any legal evidence. Secondly, it will take a long while to conclude. It is usually difficult following such cases, especially when the person had met all the requirements to withdraw money".*

Regarding efforts to combat cybercrime in Ghana, respondents indicated that they ensure maximum security on their online platforms on the side of the banks. Therefore, when one makes a transaction online, a One-Time-Password (OTP) is sent to his/her phone for confirmation. A respondent avers that:

"*Even before you can access another persons' online banking interface, there is a verification code that is sent to the person's phone. So, if it's a third party who is doing that… so it's now a two-way thing. If you don't have your mobile phone, you can't do a transaction online because a verification number will be sent to your phone. Formerly it wasn't like that, but because of our reputation, we are trying to bridge all those loopholes and all those gaps to make the system tighter".*

Bank respondents further pointed out that "*the police should be equipped technologically to be able to access intelligence on cybercrime activities".*

5.7.2 Internet Café Operators/Owners

Regarding public internet cafes, the operators indicated that the proliferation of mobile telephony and internet data penetration had disadvantaged their operations. However, cybercrime perpetrators are forced to come to their cafés to perform their activities because they do not like operating without pressure. For instance, *because they buy time, they need to finish what they are doing before the time runs out. So, they like working under pressure".*

They also indicated the multi-stakeholder awareness in the cybercrime phenomenon. They pointed out that the Banks, Police, ISPs and international shipping agencies are "*aware of the thing going on. This thing is no longer illegal oooh. Don't be lied to. I have seen it before; a*

clearing agent was tipped GH¢1,000.00 for the clearance of a consignment. Who says the police are not aware (he inquired)*?... A cousin of mine who does some was chased for driving a DV* [defective vehicle] *plate car, but he tipped them for them to leave him. It has become legal, but people have turned their blind eyes to it".*

Café operators also perceive *unemployment* as contributing to the cybercrime phenomenon. "*There are those who want to come out of it, but there is an issue with what they are going to do after stopping the thing?"*

5.7.3 Legal Practitioners' Perception of Cybercrime

The questions posed in this perspective sought to evaluate why lawyers will or will not defend cybercriminals, as well as whether there are regulations in place to combat this form of crime. However, lawyers were unaware of whether there are current state policies on cybercrime. The respondents pointed to the Electronic Communications Act as well as the Criminal Code of Ghana. On jail term for cybercriminals, one criminal lawyer who had defended a client on sim-box fraud indicated that "*One is not guilty until proven guilty and when found guilty, the various acts I mentioned* (Electronic, data protection and taxation) *provide for custodial sentences where applicable".*

Regarding law enforcement and the lack of prosecution of cybercriminals, a litigation lawyer said, "*Well, my personal experience with law enforcement agencies with respect to cybercrime is that cybercriminals are friends with the police… I think that cybercrime is thriving because the police benefit from it. Once they benefit, there is nothing they can do about it.*

This assertion corroborates the internet café operator's claim that *"the police are aware of the crime but little has been done to tackle it"*.

5.7.4 Public Law Enforcement Agents

Considering the rate and scope of cybercriminal activities in Ghana, the Ghana Police Service in August 2015 separated the Cybercrime Unit from the Commercial Crime Unit of the Ghana Police Service. Data from the field interview with the enforcement agents suggested several elements that contribute to the presumed slow efforts to combat cybercriminals. For instance, "*Thousands of cases go unreported. Sometimes, the public feels guilty for falling prey to cybercriminals. We are trying to educate our people to empathise with them and not to ridicule them. People do not also know where to report cybercrimes since it's not a conventional crime".*

The Officer also pointed out that "*we are adequately resourced knowledge-wise. But technologically, we need to be resourced. Even though we rely sometimes on forensics, I must say we are not adequately resourced technologically.*

On laws and policy documents that are used to prosecute cybercriminals, one of the officials confirmed the claims of the lawyers that, "*We rely mostly on the Electronic Transactions Act, the Data Protection Act and the Criminal Offences act but to the extreme, we sometimes use a joint charge by combining the acts".*

Lastly, the enforcement agents also called for a multi-stakeholder venture in the fight against cybercrime. "*Even though IP addresses are no more static, how prepared are the ISPs to furnish the police with such information … the banks must be prepared to report suspicious account revamps to the Financial Intelligence Centre, which in turn investigates and report to us".*

5.8 Chapter Summary

The chapter sought to present evidence of data collected for the study. It began by providing a brief overview of the current state of internet penetration as well as the types of crimes identified by the e-crime Bureau. The chapter also included an overview of cyber-culture among Ghanaian youth, which led to the presentation of the case of the study. Next, the chapter highlighted the different approaches cybercrime perpetrators adopt in order to convince their victims to part with significant amounts of money as a result of the complicated nature of online romance scams.

The next chapter delves further into the relevant factors discussed in this chapter, extracting themes and descriptions for discussion.

CHAPTER SIX

ANALYSIS OF FINDINGS

6.1 Chapter Overview

This study aims to unearth the mechanisms that underlie the commission of online romance scams from the perpetrators' perspective and to develop an online romance scam pathway. Evidence from the field interviews was presented in the preceding chapter highlighting the various forms of crimes perpetrated by a romance scam syndicate. It also took into consideration the age groups of perpetrators and their targets. This chapter advances the former by analysing the details presented in the previous one with regard to the perpetrators, guided by the framework discussed in chapter three of this study. This chapter is organised in a manner that is consistent with the presentation of the research aims (Section 1.4).

6.2 Mechanisms That Trigger Online Crimes

As indicated in chapter four, this study adapted Miles and Huberman's (1994) four-component interactive data analysis model. After several rounds of data collection and reduction, it emerged that these four mechanisms are candidate triggers for online romance crimes. First are the conditions that drive perpetrators to commit online romance scams. These conditions are largely extrinsic. Second is the configurations in their environment that they take advantage of. The third is the abilities that they possess, which they leverage to commit cyber-offences. Last is the defence mechanism they employ to justify their actions and avoid the true explanation for their unlawful behaviours.

The data analysis went through several iterative processes in order to determine the causes of the phenomenon under investigation. The first step was to triangulate the primary and secondary data sources to gain more insights. The data coding process was divided into two

stages. The first step involved looking for entities that typified the commission of online romance scams in Ghana, followed by data analysis via abduction and retroduction, as shown in Figure 6.1.

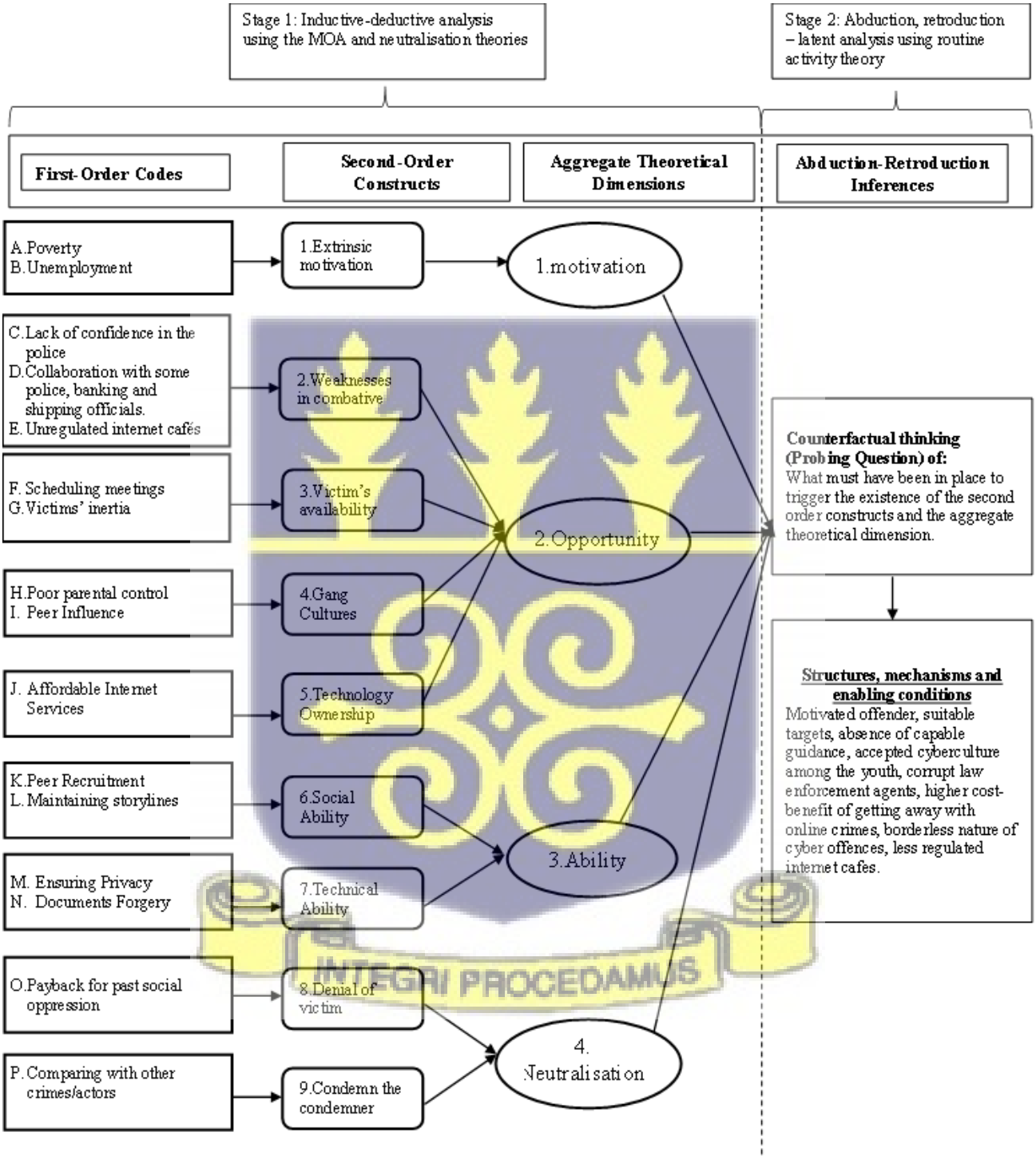
The cycles of the coding process followed the inductive-deductive logic via a flexible theory directed coding process during the first step (Inuwa et al., 2019). The theories used here are the MOA framework and the neutralisation theory, in which four concepts – motivation, opportunity, ability, and neutralisation – are used as terministic clusters of entities or themes based on data (Angel & Bates, 2014; Braun & Clarke, 2006). The terministic clusters are a theoretical grouping that was created by verbalising the responses of multiple interviewees as separate entities (e.g., Table 6.1). They are represented by the word clusters. These entities each express a unique dimension that is associated with the occurrence of online romance scams.

The analysis of latent data was the subject of the second step of the process. This involves engaging with pre-existing theories (i.e., routine activity theory) in order to identify instances of romance scamming through the use of abductive and retroductive reasoning (Felson & Clarke, 1998; Inuwa et al., 2019). Abductive reasoning is identifying patterns and relationships in data and matching them with theories or theoretical concepts to select those with the most explanatory power (Dixon, 2012; Eastwood et al., 2014).

In the final step of the data analysis process, the goal is to determine the contextual condition that must exist in order for the causal mechanism to become active and produce the results that were observed in the empirical data. Retroductive reasoning is used to identify contextual conditions by moving from the empirical domain to deeper levels of reality through

counterfactual thinking and questioning. *What must have been in place for the data to have been observed in the empirical domain* (Meyer & Lunnay, 2013).

Figure 6.1 Inductive-deductive semantic and abductive – retroductive latent data analysis



Source: Adapted from Braun and Clarke (2006) and Inuwa et al. (2019)

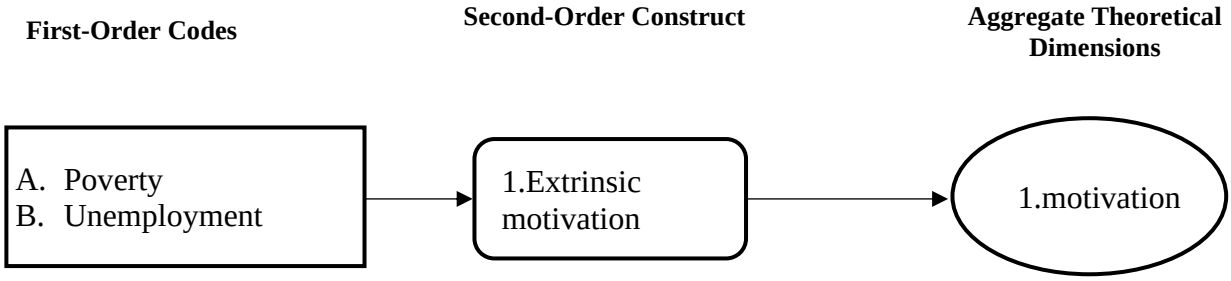
6.2.1 Motivation

The case design and selection for this study dwelled on a single case approach intended to unearth the mechanisms that underly the commission of online romance scams in Ghana. Evidence gathered from the data suggested that most perpetrators shared similarities. These similarities can be viewed in terms of age, gender and educational levels.

As indicated in Table 4.1, the cybercrime space in Ghana is mostly dominated by males with female decoys. While all the respondents who agreed to take part in this study were male, one of them affirmed that *"... I have an account called Sarah Brown* (Pseudonym). *She is my cousin. So, when the money comes, she is the one who will go for it at the bank. When the client calls too, I will give the phone to her and tell her what to say."* While this is a usual practice among the perpetrators, there seem to be a few females who engage in the act. According to Esmond, *"... oh, there is one loud girl in the Telegram group. They are not very common to see because people will laugh at them. And also, because now, routers and USB modems are common, they just use them and keep out of the public space."*

Guided by the MOA framework, four mechanisms that trigger the commission of online romance scams among Ghanaians were identified. As indicated in Figure 6.1 with supporting evidence from Table 6.1, first among the triggers identified was motivation. Motivation can be viewed as the socio-economic conditions that drive individuals to commit internet romance scams. The study found that motivation in the commission of online romance scams is primarily extrinsic. In studying the phenomenon, it was revealed that a number of factors come into play to motivate young Ghanaians to participate in cybercriminal activities. These include poverty, social status, low-level income.

Figure 6.2 Data Structure Related to Motivation



Source: Author's Construct

Further, the evidence from the data presented in the preceding chapter revealed that romance scam perpetrators are young, mostly between the ages of fifteen and thirty-five years with basic to tertiary level of education. While it is common knowledge among some Ghanaians that cybercrime perpetrators are mostly uneducated and school dropouts, the perpetrators deny this assertion and counter that "*... Oh, they* (University Students) *are there, some of your mates. You just don't know them but they are there. They do it underground."* Nonetheless, the data gathered for the study shows that some perpetrators drop out of school, more often than not, during their secondary school education stages. This is evident in the assertation of a café owner that

"... They use English to chat but they don't like going to school too ... most of them quit school for the sake of money. How do you expect to make money when you don't understand or speak good English? In fact, some of them cannot even put three to five words together to make sense. That is how come they come and copy and paste and some of them even steal clients."

Additionally, it was revealed that scammers are mostly unemployed and depend predominantly on the proceeds from the practice. In essence, perpetrators do not have steady incomes apart

from the funds that accrue from their engaging in cyber offences. Therefore, it is worth noting that the shortage of funds from scam activities impels some of these perpetrators to indulge in consulting spiritualists, *sakawa.* Although this study did not find any respondents in this category of crimes, respondents attest to the fact that it exists amid societal disapprobation. For example, Patrick, a former perpetrator, narrates that:

"Things got bad for me somewhere around 2009. Fraud news in Ghana began to enjoy popularity and for that matter, the shops began to tighten their security holes. The cards I used to generate were no more functional on these shops. While things got worse for me, my friends were really making it big. Some even suggested it was a spiritual matter and for that matter suggested consulting spiritual agents like Mallams but I refused. Instead, I began to intensify my friendship with my real identity."

This public displeasure about sakawa was further confirmed by John's displeasure about people referring to him as such: *"I am not a sakawa boy. They are those who visit the Mallams and the priests… I don't do that."*

Data collected over the period of the study suggested that poverty seems to be the most pressing factor that drives young people to engage in cybercriminal activities. Deductions from the data demonstrate that the scammers in the group come from relatively poor backgrounds with arguably poor parental control and monitoring. To that effect, they seek to liberate their families from the shackles of poverty. By so doing, some of them tend to help their parents in paying school fees for their younger siblings. This is evident in John's claim that *"my family is not a rich family. My mother is a trader and my father is also watchman. I am the first born and I have four brothers and three sisters … I need to sacrifice and help my parents to take care of the rest."* This was further amplified as Zack (John's younger brother) claimed *"... he*

paid my school fees and found this job for me." Again, poverty as a motivating factor is evident in the case of Franklyn who claimed that *"I didn't continue because of school fees; my senior sister too didn't finish because of school fees. My junior brother is also going to school but I don't know what will happen."* As evidence of poverty in relation to the payment of fees and family support became ostensible during the data collection, it also emerged that some young people also engage in online sports betting to fulfil their personal needs as well as support their families. Chris for instance narrated that *"... No, sometimes the money is not enough to take care of myself and also the family. So, I do bet too. The times that I get plenty cash-out then I give them some. If it is not plenty, I use it for myself."*

Table 6.1 Qualitative evidence: Motivation Dimension

Second-order Constructs and First-Order Codes	**Representative Data**
Motivation	
1. Extrinsic motivation	
a. Poverty	**a1.** "*I didn't continue because of school fees; my senior sister too didn't finish because of school fees. My junior brother is also going to school, but I don't know what will happen."* (Franklyn)
	a2. *"My family is not a rich family. My mother is a trader, and my father is also watchman. I am the firstborn, and I have four brothers and three sisters."* (John)
b. Unemployment	**b1.** *"... there are no jobs and man must eat..."* (Franklyn)
	b2. *"... he has something that he is doing already. Myself and the other [three] guys,* ***this is all we do****. He is a graphic designer. He works with a printing press at Circle. We only call him when we need to make changes on some documents and create flight schedules and things. So, he is not always with us."* (John)

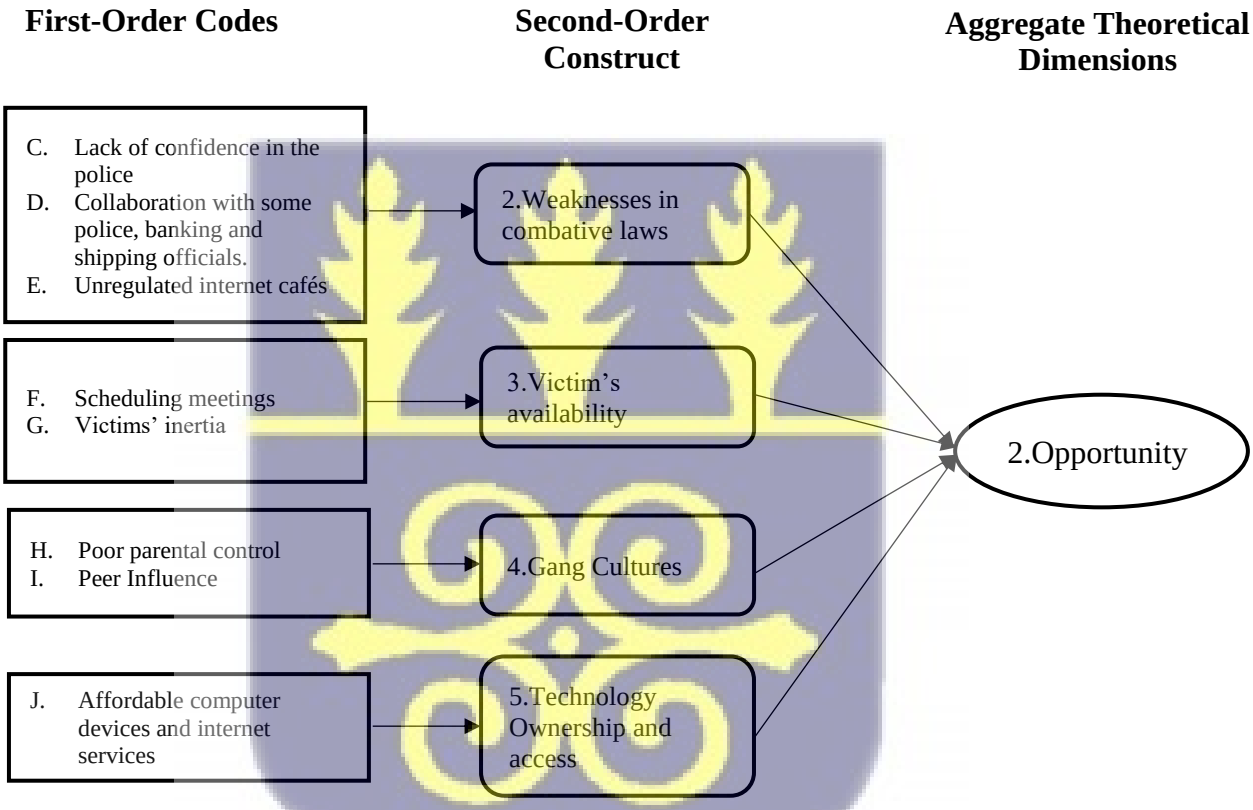
Source: Author's Construct

6.2.2 Opportunity

Opportunity in this study is operationalised as the forces in a person's environment that enable the person to engage in online romance scams (see Table 3.6). As such, the study sought to investigate these environmental factors that serve as opportunities for the commission of online

romance scams. With reference to Figure 6.3 and supporting evidence from Table 6.2, four second-order constructs were identified as the assemblages in the environment that aid perpetrators in committing online romance scams. Evidence from this construct of the framework revealed that perpetrators capitalise primarily on computer and computer-related device ownership, low cost of internet services, absence of guardianship, routine activities of victims and weakness in public laws and perceived enforcement inefficiencies.

Figure 6.3 Data Structure Related to Opportunity



Source: Author's Construct

Regarding technology ownership, perpetrators in one way or the other have access to computing devices which aid them in the commission of online crimes. For individuals who do not own personal computers, the internet cafes serve as breeding grounds for the commission of these crimes. Again, perpetrators are of the view that owning a computer gives

one the leverage of privacy when browsing the web. John avers that *"those days when we used to browse at the café, we always had to clear history after browsing otherwise the next person will see what you have done and if you are not lucky the person can steal your client … but when you use your own laptop and all that, you can just close the cover and not think about someone stealing your client".* This assertion corroborates the claims that there are female perpetrators, but they do not use public spaces because they own personal computers and internet dongles.

Furthermore, internet penetration in Ghana seems to have been on the ascendancy in recent times; 94.79% as of January 2020. That notwithstanding, cybercrime perpetrators intensify their privacy by subscribing to affordable internet service either with mobile dongles or fixed broadband. For instance, the case group as of the second round of data collection in 2018 had subscribed to Vodafone Broadband, thereby moving away from the public cafés. This affords them the opportunity to schedule meetings with their clients at their own convenience as opposed to the period they patronised the internet cafes. Again, this guarantees them the opportunity to synchronise browsing credentials on multiple devices. It is worth emphasising that Vodafone broadband service is just one of existing internet provision services that the group had subscribed to. As individuals, the members of the syndicate owned various USB dongles which also afforded them access to internet services outside of their working space.

In relation to the advantages perpetrators take regarding law enforcement, scammers are of the belief that the police are not technologically inclined to combat the menace. Again, cybercrime does not seem to be perpetrated from a single location, thereby making it a daunting task for law enforcers to track down perpetrators. For example, one of the perpetrators enquired: *"how will the police know where I stay … They don't have the technology"?* This underlines their

confidence that the police and agencies responsible for clamping down on cybercriminal activities lack the capabilities to do so. Again, as of the third phase of data collection, the group had moved from their earlier location, presumably to make it difficult to be tracked for possible apprehension.

Apart from the fact that perpetrators believe officials lack the skills to combat their activities, there are external perceptions that they also connive with some of the officials during swoop operations. For example, a litigation lawyer avers that *"... well, my personal experience with law enforcement agencies with respect to cybercrime is that, cybercriminals are friends with the police... I think that cybercrime is thriving because the police benefits from it. Once they benefit, there is nothing they can do about it."* While the preceding narration is in relation to law enforcers, evidence from the data similarly points to the fact that cybercrime perpetrators also scheme with officials of shipping agencies when they are suspected to have engaged in criminal activities. For example, perpetrators often purchase electronic gadgets through their clients. When this happens, they are required to pay customs duty on the shipped items, which compels them to sell some of the items to pay for the rest. A self-identified independent scammer who had had an encounter of such nature opined that *"the customs charges are expensive so the strategy is to buy plenty of the items and sell some to pay for the duty".* In some instances, however, perpetrators pay their way through difficult situations such as being reported for suspected unlawful cyber-activities. This claim was further substantiated by Patrick who asserted that *"When the items got here in Ghana, the postal guys began to suspect me. They even threatened to report me but I tipped them and they made me go through. This was a usual practice but this was huge".*

Concerning victims' routine activities, perpetrators place high premiums on first, their choice of victims. Thus, their targets are mostly people who have predictable daily activities. This way, they (scammers) are able to determine victims' routine activities and adjust and play along those lines. For example, scammers in drawing up their meeting times purposefully place meetings at times that the clients are mostly free so as not to inconvenience them. In so doing, victims tend to believe that the scammers are thoughtful and for that matter could be perfect partners for them in the near future.

Additionally, cybercrime perpetrators also take advantage of the borderless nature of their crimes and the fact that victims are often slow at reporting cyber-fraudulent activities. Even though online romance scams and related crimes have been on the ascendancy in recent past, many of such crimes go unreported. The American Embassy in Ghana for instance reports on their website that *"... there are victims who do not report their losses to authorities due to either fear or embarrassment"*. This claim was assented to by the police, who remarked that *"Thousands of cases go unreported. Sometimes, the public feels guilty for falling prey to cybercriminals. We are trying to educate our people to empathise with them and not to ridicule them. People do not also know where to report cybercrimes since it's not a conventional crime"*. This was further revealed in the responses of the perpetrators, as both the group members and independent perpetrators claimed none of their victims had reported them even though they have threatened to do so. Again, none of them had been convicted in relation to either traditional crimes or online romance offences.

Table 6.2 Qualitative Evidence: Opportunity Dimension

Second-order Constructs and First-Order Codes	Representative Data
Opportunity	
2. Weaknesses in Combative Laws c. Lack of Confidence in the Police	**c1.** *"How will the police know where I stay ... They don't have the technology"?* (Independent perpetrator) **c2.** *"The police should be equipped technologically to be able to assess intelligence on cybercrime activities."* (Banker)
d. Collaboration with some police, banking and shipping officials.	**d1.** *"The banks, Police, and International Shipping agencies are aware of the thing going on. This thing is no longer illegal oooh. Don't be lied to. ... A cousin of mine who does some was chased for driving a DV [defective vehicle] plate car,* ***but he tipped them for them to leave him****. It has become legal, but people have turned their blind eyes to it."* (A café owner) **d2**. *"Well, my personal experience with law enforcement agencies with respect to cybercrime is that* ***cybercriminals are friends with the police****... I think that cybercrime is thriving because the police benefit from it. Once they benefit, there is nothing they can do about it.* (Lawyer) d3. *"****Oh they connive with them every day*** *... how can you a lance corporal afford a range rover? How much is your salary? They are sponsored by the fraud boys."* (BNI agent)
3. Victim's availability e. Scheduling Meetings	***e1****. "it depends. Sometimes I can do (meet) three at the same time so that I don't waste time coming here and going ... It also makes my mind active."* (John)
f. Victims' Inertia	***f1.*** *"Thousands of cases go unreported. Sometimes, the public feels guilty for falling prey to cybercriminals. We are trying to educate our people to empathise with them and not to ridicule them. People do not also know where to report cybercrimes since it's not a conventional crime."* (Police) ***f2.****"... there are victims who do not report their losses to authorities due to either fear or embarrassment."* (US Embassy Website)
4. Gang Culture h. Poor parental control	**h1.** *"... I can't tell how I started, but all I remember is that every evening [we], me and my friends gather at the café to chat and argue about football and other things..."* (John)
i. Peer influence	**i1.** *"... they are my paddies, and we move together, so we do everything together."* (Chris)
5. Technology Ownership	**j1.** *"I don't go there nowadays because I now have internet at home. It is cheap, it is always on. Whenever I want to do something, it is*

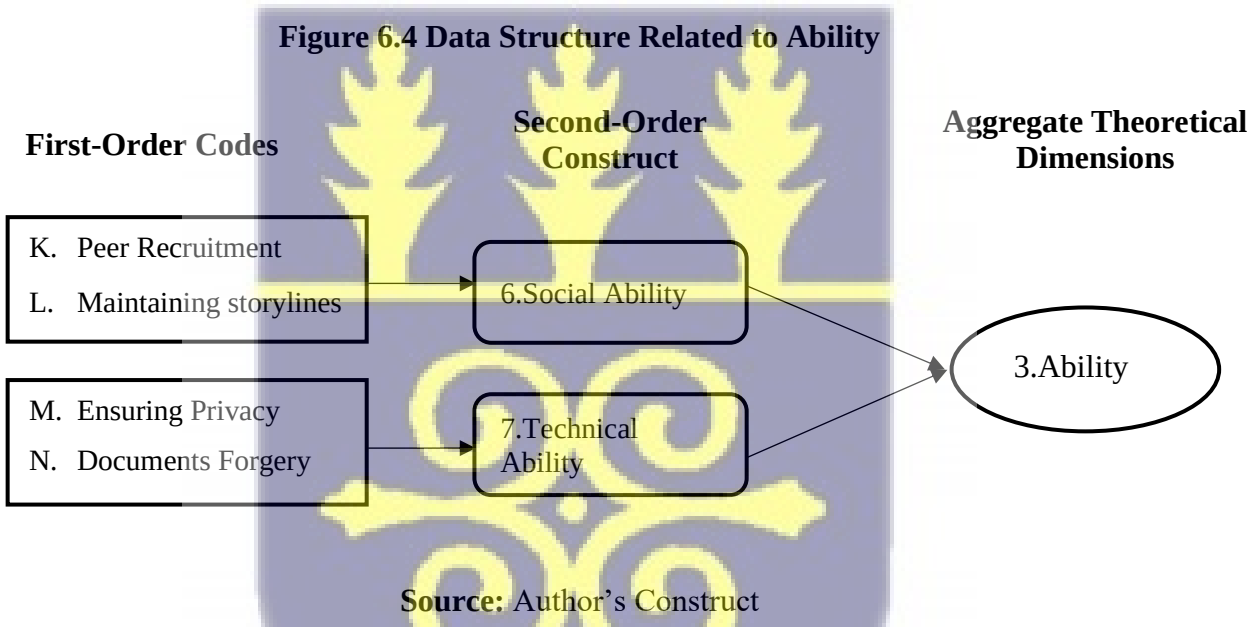
Second-order Constructs and First-Order Codes	Representative Data
j. Affordable internet services	*available… We are just four in this room. So, no one can steal your client, no one can point fingers at you that you are a sakawa boy and other things."* (John)

Source: Author's Construct

6.2.3 Ability

Ability in this study refers to the qualities that an individual possesses to perform online romance scams. With reference to Figure 6.4 and backed by evidence in Table 6.3, two second-order constructs were identified during data analysis. Thus, social and technical abilities. This section delves into these abilities and how they impact the perpetrators' workflow.

Figure 6.4 Data Structure Related to Ability



Source: Author's Construct

Social abilities are related to perpetrators' abilities to identify with societal norms and values. For example, perpetrators interviewed for this study were aware of the fact that fraud and, for that matter, cyber fraud is frowned upon by the societies within which they live. However, they manage to stay within these societies. Perpetrators also find ways to keep the public away from their acts. This ability can be deduced from the group's decision to end their operations at the internet café to operate from a private location. However, the ability to keep cyber-offensive

activities from the public eye largely depends on the perpetrators' ability to purchase and maintain private internet service. Perpetrators who are not able to acquire such services continue to use public cafes, but with caution. Observations at the internet cafes revealed that strict privacy rules are ensured in all the internet cafes observed. This is as a result of complaints by patrons, especially the perpetrators, that bystanders observe their activities. Again, there were noticeable posts on the walls of the cafes indicating *"No standing in the café"*. This in effect is a caution to patrons without browsing time to keep some distance from active users of the café. While this may seem like a privacy issue, it is more of a move instigated by the perpetrators to keep the public away from their activities.

The second social ability possessed by perpetrators is their ability to peer recruit and manage resources. It is worth noting that while a single group was used for this study, evidence from data collected indicated that many more of such groups exist in other regions and locations in Ghana, many of which were started by individual perpetrators. As outlined in the previous chapter, cybercrimes perpetrated in Ghana seem to be an interlace of several crimes. Therefore, gang leaders recruit peers who have expertise in certain forms of offences. According to John, *"there are no leaders in some of the groups but someone started it, that is why we see them as leaders … it is just that they called the people to come together or because he has made more money than the rest… like I said, we formed this group because one man cannot do everything. I can shop and someone too can chat so it is just good to be together as a group so that when the money comes, we share it together"*. Apart from the leaders' abilities to bring together individual perpetrators to form a group, they also need the ability to manage the members and resources (utilities including internet service charges). Most groups, according to respondents, have between four and ten individuals who are usually camped and share resources, including apartments. The residences most often than not are the leaders'. This kind of arrangement

requires the management of resources so as to avoid an abrupt end of operations of the group. Organised perpetrators, therefore, allocate funds from their operations for the maintenance of their facilities. In order to mitigate unanticipated circumstances such as internet data runouts, some groups purchase the highest packages available.

Figure 6.5 A News Article on an Apprehended Cybercrime Syndicate in Ghana

Source: Ghanaweb (2018)

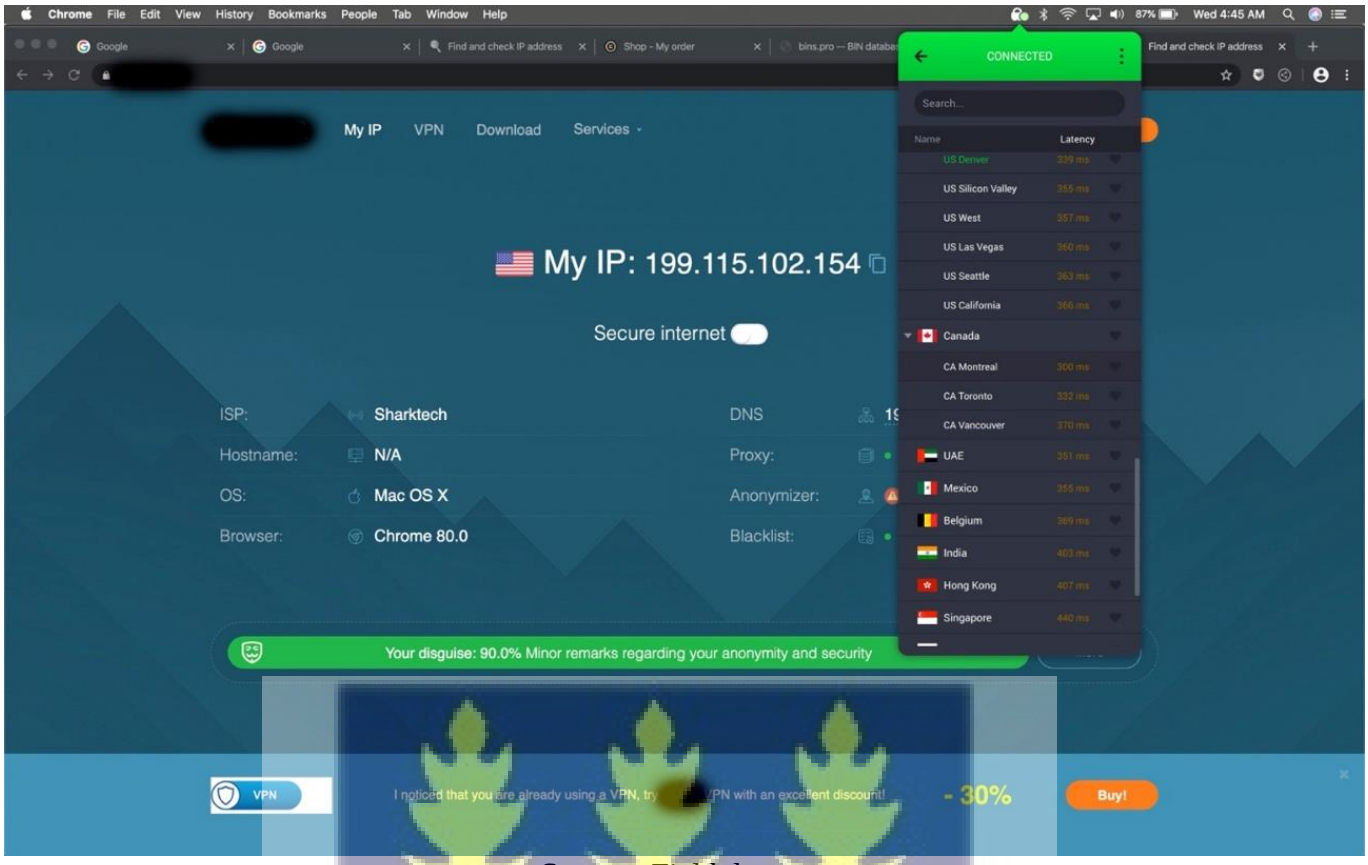
Technical ability was found to be the second second-order construct for the ability aggregate theoretical dimension. The whole operation of perpetrating cyber-offences requires heavy use of computers and other computing devices. This further requires that they build considerable IT skills in order to perpetrate cyber-offences. For instance, cybercrime perpetrators need to install and configure computer applications in order to ensure anonymity. These applications come in different levels of sophistication. It was observed from the field study that beginners often employed web plugins such as SOCKS5 proxies. In this instance, perpetrators insert SOCKS5 proxy addresses in their browsers which grants them the leverage to alter their virtual

location. These addresses are mostly generated online but are often restricted to the locations available at the time of generation. A higher-level tier of anonymity is the use of premium VPN accounts. According to the perpetrators, SOCKS5 is limited to the countries, unlike the premium ones. For example, Esmond narrated that

"With the [one of the VPNs[9]*], it is like having access to someone's computer in the US and using it. So, you will get access to the person's user ID and password and browse on the person's laptop without his knowledge. When you finish you have to clean the browsing history so that the person won't suspect it … Amazon can sometimes track so like if I want to shop and the state on this card is Massachusetts, then I have to connect or buy a proxy of the same state as the card I am having. If the state is different from the one on the card, they will suspect something fishy so you have to connect to the same location so that they will think you are in the state* (he shows a page of the proxy setting)".

[9] Name of application truncated

Figure 6.6 A Snapshot of a Premium VPN



Source: Field data

Again, in committing online romance scams, perpetrators often engage in identity theft by sourcing for pictures of less well-known models. They make sure the selected model has a sequence of pictures from other activities and also a *camshow*[10]. However, they are compelled to alter pictures when their clients/victims begin to request different pictures. In such instance, scammers use face-changing applications and other graphic designing tools to swap the faces of the models as represented in Figure 6.7. It can be noticed in the photographs that while the images present the same location, the faces and the notes on the sheets are different.

[10] Naked webcam videos

Figure 6.7 An Altered Photograph of a Model

Source: Field data

Another form of forgery in the scheme of affairs of the scammers is the flight details forgery where already existing passports and flight tickets are altered to appear as though they were genuine. The technical difference between this and the photograph alteration is that they need an expert in graphic design to skilfully find and align texts on the documents without traces of suspicion. That is, they must find the same fonts as those on the original document as well as match the colours and patterns on the passport and flight documents.

Table 6.3 Qualitative Evidence: Ability Dimension

Second-order Constructs and First-Order Codes	Representative Data
Ability *6. Social Ability* k. Peer recruitment	**k1.** *"I can't tell how I started, but I know it is through when meeting at the café every day after training."* (Franklyn)
l. Keeping constant storylines	**l1.** *"You have to correctly remember the story for each client."* (John)
7. Technical Ability m. Ensuring Privacy	**m1.** "*You need to open the site but you need to use a VPN because when you open Amazon for instance, you will a Ghana IP so you need to change the IP by using a VPN. There a number of them."* (Esmond)
n. Document forgery	**n1.** *"He works with a printing press at Circle. We only call him when we need to make changes on some documents and create flight schedules and things. So, he is not always with us."* (John on outsourced abilities)

Source: Author's Construct

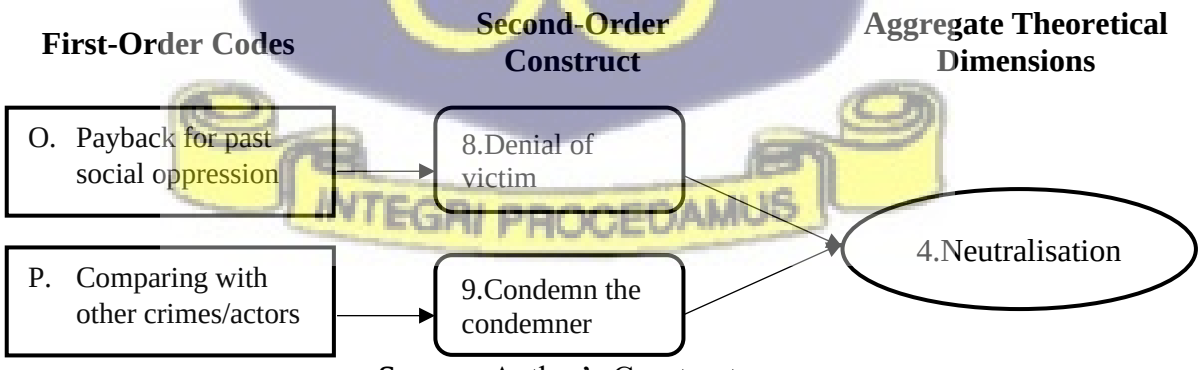
6.2.4 Romance Scam Rationalisation

Having given the background of why individuals engage in cybercrime as well as their abilities and the environmental opportunities, this section of the study presents the justification that romance scam perpetrators impute to their involvement in the crime. It is important to note that the justification given by perpetrators of online romance scams may differ from person to person. Rationalisation may be understood in this sense as the justification for one's unlawful behaviour. In studying cybercriminal rationalisation strategies, it is easy for one to confound offenders' motivation with their crime rationalisation. For example, while poverty may be the driving force for one's financial needs (motivation), the justification for whom he/she defrauds is his/her rationalisation for the commission of the crime.

Evidence from the data indicates that cybercriminals' targets are mostly the wealthy and financially sound westerners seeking romantic relationships. While one of the respondents believes the victims are wealthy and, for that matter, do not lose anything when they are

scammed, an astonishing revelation was when one of the group members said, *"They are credit cards from the Osama Bin Laden Bombing... those who died didn't die with their cards."* Even though this assertion may not be directly related to online romance scams, the respondent believed the September 11 World Trade Centre attack victims still have their monies on their cards. For that matter, they are robbing no one. Again, online romance scam fraudsters interviewed for this study rationalise their activities as not being as dangerous as traditional crimes like robbery and murder. For example, a respondent claimed that "*No one can judge me with what I am doing unless a judge tells me that I am a criminal; nobody can call me a criminal".* He is of the view that cybercriminal activities are standard practices that people commit even without knowing. He again questions other activities that he considers to be similar to cybercrime: *"those who have been downloading movies from torrent sites, do they pay? Do you call them cyber criminals?".* The respondent further maintains that cybercrime is less a crime than traditional crimes *"it is better to do something than do nothing... I can't go and rob people ... No, it is bad to do that".* Romance scammers also claim that they take advantage of greedy, gullible and unintelligent westerners who are slow at identifying scam relationships. They claim this is a retaliation for the suffering inflicted on their forefathers by westerners during the era of the slave trade.

Figure 6.8 Data Structure Related to Neutralisation



Source: Author's Construct

Table 6.4 Qualitative Evidence: Neutralisation Dimension

Second-order Constructs and First-Order Codes	Representative Data
Neutralisation	
8. Denial of victim o. Payback for past social oppression	***o1.*** *"… they stole our gold; they also used our grandfathers and things for slaves. My guy, we are taking back."* (an independent perpetrator) **p1.** *"… those who have been downloading movies from torrent sites, do they pay? Do you call them cyber criminals?"* (John)
9. Condemn the condemner p. Compare with other crimes and their actors	**p2.** *"It is better to do something than do nothing... I can't go and rob people ... No, it is bad to do that."* (John) **p3.** *"No one can judge me with what I am doing unless a judge tells me that I am a criminal, nobody can call me a criminal."* (John)

Source: Author's Construct

6.3 Perpetrators' Behavioural Dynamics

With the preceding sections highlighting the motivations that underlie the commission of online romance scams, the environmental opportunities, the technical and social abilities possessed by the perpetrators, and the justifications they ascribe for their actions, this section seeks to emphasise the behavioural dynamics in the commission of internet crimes. Again, perpetrator behavioural dynamics, according to the data, occurs in three stages: the creation stage, maturation stage and decline stage. These dynamics are elucidated in the ensuing sections.

6.3.1 Creation

Several mechanisms converge in the creation stage of cyber-deviant behaviours. The creation stage is observed as the starting stage of an individual's ingress into the commission of online crimes. Evidence from the data collected over the period exposed an indication of how unassuming young individuals pick up behaviours at internet cafes. Different groups of people patronise public cafes for different reasons. For example, school pupils patronise the cafes to access the internet to do their homework. Junior and senior high school students also use the cafes for research purposes, and so also are those with duplicitous motives. It is, therefore,

apparent that the cafes, more often than not, are crowded with patrons with various agendas and purposes.

Further, young individuals also use internet cafes for leisure. Thus, they purchase browsing minutes to play games and watch YouTube videos. In so doing, they pick up hints on how to find friends and connect on Facebook and other social media platforms. They further graduate into attempts to benefit from their friendships by requesting little gifts from their friends and, through that, become habituated.

Figure 6.9 A Group of Young Individuals in a Browsing Session at a Café

Source: Field data

Contrary to the use of internet cafes by students and other groups of people, public cafes hold a strong appeal for young people who spend time chatting with friends and making arguments about topics of interest such as football, music and entertainment. These young people gradually form a cyber-culture that sometimes runs late into the night and is often wrought by the fact that some cafés operate twenty-four-hour service known among patrons as *"twenty-*

four". Through these social interactions, young unintended individuals with needs request cyber-deviant peers to shop for items for them illegally. Once these requests are met, the act is repeated, and these individuals are subsequently coached in the rudiments of deviant cyber activities.

At this stage of the dynamics, perpetrators resort to the use of scripted content with close assistance from their mentors. A deviation from the template destabilises beginner-perpetrators to fall on their coaches for a take-over the chat sessions. These steps are repeated until the beginner has the self-assurance to continue with the activities unattended.

6.3.2 Maturation

After individuals have received enough coaching that secures their independence from their mentors, they move to the maturation stage. At the maturation stage, it is assumed that individuals who hitherto did not have the confidence to convince victims can independently engage in various forms of sophisticated internet crimes. Analysis of data collected over the period indicates that internet crime perpetrators, at the peak of their activities, engage in a multiplicity of crimes (See Figure 5.5).

Contrary to what happens during the rudiment stages, perpetrators on their own create profiles on dating platforms, engage date seekers on these platforms, find, prime and migrate would-be victims to instant messaging platforms. Again, there is little or no regard for law enforcement during this stage. This is due to the perpetrators' right to privacy and their abilities to manipulate proxies. Perpetrators are of the belief that law enforcement agencies are weak at combatting technological crimes. This belief, coupled with the viewpoint that victims may not

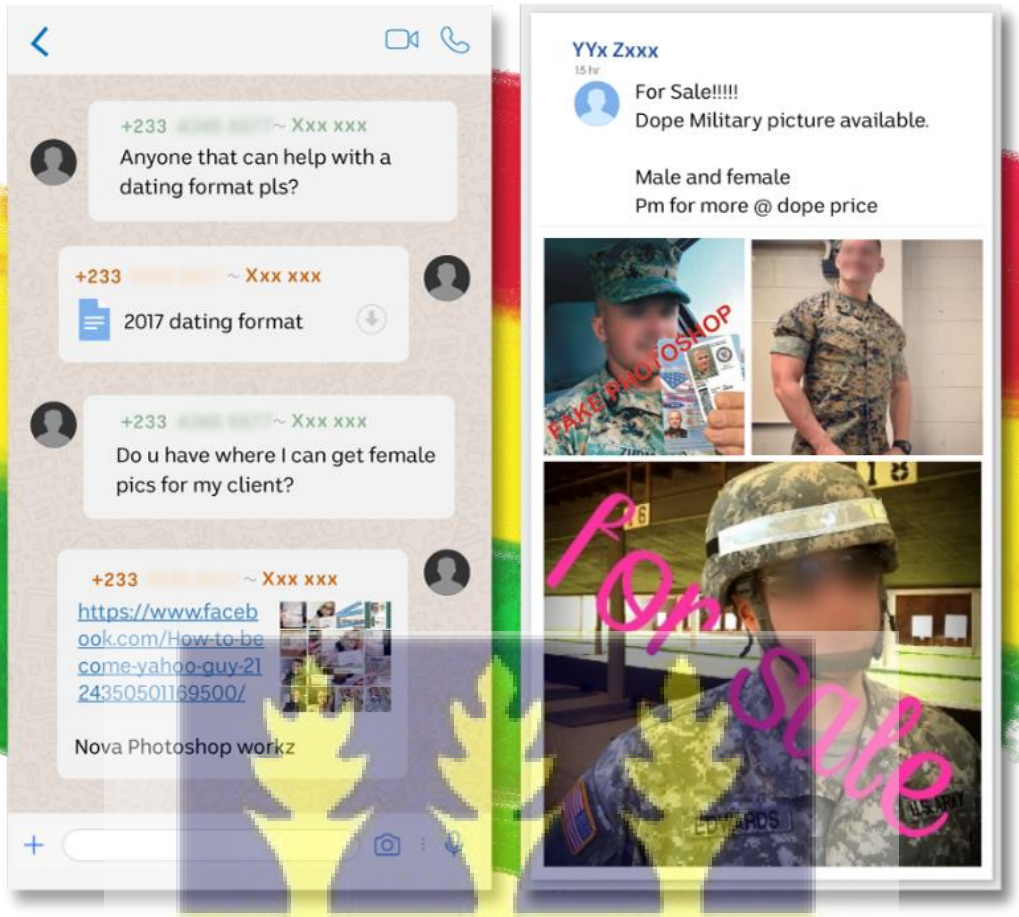
report cybercriminal incidents emboldens scammers to go all out to get what they want from their clients.

Further, cybercrime perpetrators at this stage partner with their counterparts within Ghana and internationally organised cybercrime groups. This is evident in their quest to outsource some of their activities to friends. Again, evidence indicates that the clients from the dating platforms are often channels for illegal shopping and shipping of items from their countries of residence to the perpetrators. In so doing, perpetrators at this stage, either by themselves or through the services of *carding* specialists, trade in credit cards with global organised groups.

Another activity of interest at the maturation stage is that internet crime perpetrators seemingly scheme with corrupt law enforcement, banking and shipping agents to bypass state laws and evade arrest. This point is evident in the remarks of the BNI official interviewed for this study *"Oh they connive with them every day ... how can you a lance corporal afford a range rover? How much is your salary? They are sponsored by the fraud boys".* This account is supported by one of the lawyer respondents for the study *"I think that cybercrime is thriving because the police benefit from it. Once they benefit, there is nothing they can do about it."*

Lastly, at this stage, perpetrators also join knowledge-sharing groups where codes and information about bypassing platforms and pictures are traded. According to the perpetrators in this study, such platforms are premium forums, meaning the administrators charge patrons a fee to enlist them. While evidence of the case group's involvement cannot be substantiated, it seems to be a new trend among cybercrime perpetrators, particularly independent perpetrators. Figure 6.10 illustrates one of such knowledge-sharing groups.

Figure 6.10 A Cybercrime Knowledge-Sharing Platform



Source: abc.net.au (2020)

6.3.3 Decline

The maturation stage lasts for a more extended time, usually between five and ten years, during which decline begins. Various factors come into play to trigger this stage. They may include public education and upgrades of security features on dating and e-commerce platforms. When this happens, perpetrators are required to find other means of finding their victims as well as bypassing security features on e-commerce platforms. However, it is worth noting that resilient individuals who find ways around the systems remain in the maturation stage or diversify into other schemes. Unsuccessful ones, on the other hand, decline. Such individuals, according to the BNI officer, "*very much likely engage in traditional crimes and some go as far as*

kidnapping foreigners". According to the officer, however, there is no decline until the individual is arrested, making their behavioural changes more of a cycle than a curve.

However, from the accounts of the perpetrators, most perpetrators at this stage either become intermediaries for cyberdeviant shoppers or stray into sports betting and other forms of gambling. By being intermediaries, perpetrators establish connections with specialised shoppers for individuals who seek to illegally purchase items on e-commerce platforms but do not possess the ability to do so. The middle-man earns a percentage of every item purchased in such cases. The middle-man, in most cases, earns twenty per cent of the transaction; the consultant, forty per cent; the *brainer*, twenty per cent; and the remaining twenty per cent is sold to defray the cost of shipping. To illustrate this point, if five laptops are purchased, the middle-man takes one, the shopping consultant takes two, the *brainer* takes one, and the remaining one is sold to settle the cost of customs duty.

It is also worthy of note that declining perpetrators are counselled by friends to try spiritual means to remain in the maturation stage. This is evident in the words of Patrick:

"Things got bad for me somewhere around 2009. Fraud news in Ghana began to enjoy popularity and for that matter, the shops began to tighten their security holes. The cards I used to generate were no more functional on these shops. While things got worse for me, my friends were really making it big. Some even suggested it was a spiritual matter and for that matter suggested consulting spiritual agents like Mallams but I refused."

Figure 6.11 The ORS Perpetrators' Behavioural Dynamics

CREATION
- Beginners start basics with no clear sense of direction.
- Possess little or no skills
- Guided by mentors
- Follows strict templates

MATURATION
- Multiplicity of crimes
  - *Forgery*
  - *Credit card fraud*
  - *Identity theft*
  - *Shopping*
- Ability to "ghost" IP addresses
- Collaborate with law enforcement officials to evade apprehension.
- Join knowledge-sharing groups
- Mentor others

DECLINE
- Unsuccessful attempts to bypass credit card verifications
- Difficulty in convincing clients
- Scammers venture into sports betting
- May cross into cyber-spiritualism.
- Traditional crimes become attractive.

Source: Author's Construct

6.4 Online Romance Scam Pathway

This study's third objective sought to explore the strategies that online dating romance scammers employ in finding, grooming and defrauding their victims. In the quest to satisfy this objective, three stages were realised. These have been explained in detail in the following sections.

6.4.1 Phase One

The first phase of the pathway is the preparation stage. At this stage, perpetrators register and create attractive profiles on dating platforms. Such profiles are created with fake images of unpopular American or Russian models with accompanying descriptions. Very often, personalities in the profiles are young women between the ages of twenty-five and forty. After profiles have been created, the perpetrators advance to find suitable targets. Qualities of targets sought by the perpetrators include new users who have not engaged on the platforms for long time. It is assumed that such users are inexperienced in determining scams.

Scammers then proceed to stalk the found users (would-be victims), after which they wink them. Upon acceptance, they progress to establish a relationship, but the scammer may go back to search for other suitable targets when the initial request is declined. It is important to note that users of dating platforms who have been exposed to scams in one way or the other may adopt some tricks to puzzle the scammer. For example, they may ask questions pertaining to happenings in the countries the perpetrator's profiles indicate. Such quizzes may relate to subjects including politics, leisure and education. In instances where the perpetrator is unable to answer the questions, the clients terminate the relationship. In other instances where the perpetrators answer the questions correctly, the relationship progresses to the second phase.

6.4.2 Phase Two

The second phase of the strategies is the crisis stage. This phase further manifests in two ways. The first is the scammer-led approach, and the second, the client-led. In the scammer-led approach, scammers, after gaining trust from phase one, create exciting storylines to keep the client bonded to the relationship. A familiar story among the scammers is to pose as a philanthropist engaging in humanitarian projects in Africa, specifically in Ghana. In such cases,

donors from the United States will donate items through the client to the scammer who claims to be a philanthropist. But what is unknown to the client is that his/her address is being used as a transit for the shipment of illegally purchased items from e-commerce platforms. This approach often develops when the scammer fakes the attributes of a man of fifty-years or more. Other professions that scammers often use include US or UK military men on a mission in Africa. In an established relationship, the scammer begins to request a supposed inconsequential favour such as $100 gift cards from the clients, which gradually advances into significant amounts of between $500 and $1000. When both the scammer and the client agree to establish a permanent relationship, which would require the scammer to *come home,* the latter begins to falsify documents (e.g., passports and flight tickets) and tragic stories that appeal to the emotions of the clients (e.g., kidnapped relatives, robbery, accident). They then use the opportunity to sting the clients by requesting huge sums of money to pay hospital bills and facilitate their return home. Successful scammers at this phase progress to the next phase while unsuccessful ones resort to blackmail using naked pictures and videos obtained during the course of their relationships.

On the other hand, the client-led approach transpires when scammers pose as young ladies on internships in Africa. Their professions often include nurses, social workers and students, and they target older men (known among the scammers as *mugu*) who are not interested in lasting relationships but would often request naked pictures and videos of the scammers. According to the scammers, ten pictures go for $200, and videos go for between $500 and $1000 depending on one's negotiation prowess. However, some men found in this category are also interested in lasting relationships and fall prey to the scammers' requests for petty gift cards.

6.4.3 Phase Three

This phase is the termination stage in the scheme of affairs of the scammers. The manifestation of this stage ensues when either the scammer succeeds in duping the victim, or the victim identifies the relationship as a scam. It is important to note that scammers terminate the relationship as soon as they succeed in defrauding their victims. Thereafter, all digital footprints of the profile used are wiped out. These include the profiles on the dating platforms, email accounts and, to a large extent, the mobile numbers used for communication.

On the other hand, scammers tend to blackmail their victims in the client-led approach by threatening to report them to the FBI for abusing them in the form of requesting naked pictures and videos in return for money. The scammers then demand huge sums of monies from the victims. To avoid this seeming embarrassment, some clients pay the monies, after which the scammers reveal themselves as scammers and verbally abuse the victims. Again, digital footprints are deleted after the revelation.

Table 6.5 Romance Scam Pathway Activities and Corresponding Platforms and Technologies

Phases	Activities	Platforms/Technologies
Phase I: Preparatory	Register on Dating Platforms.	Dating platform
	Download pictures and camshows of not well-known models.	Knowledge sharing platforms (WhatsApp and Telegram Platforms)
	Create attractive profiles with the pictures.	Dating platform
	Find suitable targets on dating platforms.	
	Stalk and wink would-be victims on dating platform.	
	Migrate victims off dating platforms to instant messaging applications.	Dating platforms, WhatsApp, Telegram, Google Hangout
	Pass quiz in order to proceed to the crisis stage.	Dating platforms and Search Engines to find answers.
Phase II: Crisis	Create and tell consistent storylines.	Instant messaging apps: WhatsApp, Telegram, Google Hangout

	Shop online (e-commerce fraud) and exchange gifts with clients.	E-commerce platforms: Amazon, Walmart, GlobalRose
	Download and edit pictures of naked models.	Photo editing applications: Photoshop, Photo Editor Pro
	Trade pictures and videos for money.	Instant messaging apps: WhatsApp, Telegram, Google Hangout
Phase III: Termination	Delete profiles and wipe off all digital footprints.	Dating platform
	Blackmail victims and demand money.	Instant messaging apps: WhatsApp, Telegram, Google Hangout

Source: Author's Construct

6.5 Forms of Cybercrime

The study sought to unearth the mechanisms that underlie the commission of online romance scams. After attempting to accomplish this goal in the preceding sections, the study discovered ancillary results that cannot be overlooked. The evidence from the data suggested three broad forms of cybercrimes perpetrated in Ghana. These are crimes that are perpetrated against systems, crimes that need both offline and online interactions of both perpetrator and victims, and cybercrimes rooted in religion.

Even though data collected for the study did not capture primary evidence of pure technical crimes, document examinations and responses from perpetrators revealed that that type of crime does occur in the jurisdiction under investigation. As represented in Figure 6.12, the Ghana police arrested twelve members of a cybercrime syndicate who allegedly attempted to transfer GHC326 million from a state-owned bank. A statement in the news indicated that: *"according to the police, all the suspects, believed to be part of a wider cybercrime syndicate made up of Nigerians and Ghanaians, attempted transferring a whopping GHC326 million from the vault of Universal Merchant Bank (UMB), electronically".* Aside from the fact that

this may be purely a Type I crime, it also corroborates the existence of cybercrime syndicates in the country, giving credence to the group that was used for this study.

Figure 6.12 A Snapshot of a Technical Crime News Item.

Source: Daily Graphic (2020)

As evidenced in the data collection, the study considered crimes that needed both online and offline involvement of victims and scammers to make the crime materialise. The researcher terms this form of crime socio-technical cybercrimes. Throughout the study, it can be realised that almost all activities that were put under inquiry for this study primarily needed the active participation of the scammer aided by technological systems and the clients' participation. For example, whereas in technical crimes, one may not necessarily need the participation of another party on the other side of the system to facilitate one's activities, in such crimes as romance scams, scammers require that clients are actively involved, as would the various collaborators such as bank staff, shipping agents among others. Figure 6.13 presents a news headline about a romance scam syndicate apprehended.

Figure 6.13 News Headline of a Romance Scam Syndicate Apprehension

Source: Daily Guide (2017)

On the spiritual dimension to cybercriminal activities in Ghana, primary data did not elicit evidence, but inferences from discussions with the respondents and document examination educed its existence. Termed sakawa, the spiritual dimension of cybercrime entails perpetrators seeking the backing of spiritualists and, to some extent, pastors who bless and pray on the devices used by the scammers in their activities. Sakawa boys are rumoured to often operate in groups and perform socially grotesque activities such as eschewing bathing, carrying out requirements such as submitting human body parts at their cult meetings, sleeping in coffins and committing incest. Whereas the first two forms of crimes mentioned are solely cyber-related, the techno-religious crimes incorporate elements of both cyber-offences and traditional offences like murder.

6.6 Chapter Summary

The chapter set out to analyse the case findings presented in chapter five with particular relation to the research questions. The outcome of the analysis revealed the four mechanisms sought out by the first research question motivation, opportunity, ability and rationalisation. The chapter thence went on to delineate the behavioural dynamics of online romance scammers, thereby revealing that such people undergo three stages regarding their behavioural dynamics. The stages are creation, maturation and decline. This chapter's third activity was to analyse online romance scammers' strategies in finding, priming and defrauding their victims. This was done in an effort to answer the third research question. By so doing, a three-phase activity was outlined. This comprises the preparatory, crisis and termination phases.

Despite the above, the study discovered three broad types of cybercrimes in Ghana: technical crimes (Type I), socio-technical crimes (Type II), and cyber-religious crimes, which add a spiritual dimension to the already established forms of crimes accompanied with some forms of traditional crimes.

The next chapter discusses the analysis presented in this chapter and maps the studies and existing literature to confirm, counter or reveal new findings.

CHAPTER SEVEN

DISCUSSION OF FINDINGS

7.1 Chapter Overview

The findings presented in Chapter five were analysed in the previous chapter (chapter 6). The mechanisms that trigger cybercriminal behaviours were identified in this chapter. It also highlighted the stages in the romance scam pathway, as well as the dynamics in the perpetrators' behaviour.

This chapter discusses the findings presented in the preceding chapters in line with the literature reviewed (in chapter 2) in order to answer the research questions and draw lessons. In this regard, the chapter compares the literature reviewed and the case findings and analysis in chapters five and six.

The discussion is organised into three parts, each of which is organised around one of the research questions. Thus,

1. What mechanisms trigger cybercriminal behaviours?
    a) *What are the motivational factors of these cyberdeviant behaviours?*
    b) *Which environmental forces (opportunities) enable the work performance of cyber-offenders?*
    c) *What abilities do cybercrime perpetrators possess that aid them in committing online crimes?*
    d) *What neutralisation strategies do romance scam perpetrators employ to justify their unlawful behaviours?*
2. How do cybercrime behaviours change over time?
3. Which strategies do online dating romance scammers employ in finding, priming, and defrauding their victims?

7.2 Triggers of Cybercriminal Behaviours

This section attempts to find answers to the first research question: What mechanisms *trigger cybercriminal behaviours?* In that regard, the ensuing subsections are structured along the respective sub-questions under the broad question.

7.2.1 Motivation

This section presents a discussion of the research framework's motivation dimension. Also, it seeks to answer the first sub-question of the first research question: *what are the motivational factors of cyberdeviant behaviours*?

Motivation is advanced in the literature as the pressures to commit scams, including social pressures such as how individuals wish to be seen by others in society (Murphy & Dacin, 2011). While the literature pointed out two main forms of motivation: intrinsic and extrinsic, findings from the current study revealed ample indication that motivation among romance scam perpetrators is largely extrinsic, while intrinsic motivation is related to other forms of online crimes such as hacking. For example, previous studies (Kopp et al., 2015; Whitty, 2018b) on romance scams found that the primary motive for romance scam perpetrators is to financially profit *(extrinsic)* from their victims while hackers are mostly ideological and inherent (Kshetri, 2013a).

That notwithstanding, analysis of the findings for this study suggested a number of socio-economic factors that impel individuals to engage in romance scams. Such drivers include poverty, unemployment, low level of education and low income. For instance, the romance scam syndicate studied for this research were made up of young unemployed persons aiming to live meaningful lives from cybercriminal activities. Even though they gave no confirmatory

responses to questions about their involvement in traditional crimes, they believed cybercrime is less a crime than traditional crimes. This finding lends credence to those of previous studies by Okpan and Anigbogu (2016) and Olaiya et al. (2020) that internet criminals commit crimes primarily as a result of unemployment, deprivation, and a desire to aspire to the higher socio-economic statuses of those they see, despite the lack of readily apparent income-generating activities to justify such wealth. To further bolster this finding, online romance scams take a lot of time and effort to accomplish. However, scammers take their time to walk victims through the romance scam pathway. According to scammers, one's awareness of one's situation (poverty, unemployment, among others) is enough motivation to be patient. Hence the lesson:

Lesson One: *An interplay of various socio-economic factors, including unemployment, low-level income, low-level education, and the quick money syndrome, is a major driving force behind the commission of online romance scams.*

7.2.2 Opportunity

In considering the motivations for the commission of internet crimes, a complete explanation must ultimately consider the sociocultural environments in which people conduct their daily activities (Choo & Tan 2007). This then leads the discussion to the configurations of the forces in a person's environment that enable the person's work performance: opportunity (Blumberg & Pringle 1982). Findings from the current study suggest that cybercriminals take advantage of weaknesses in existing laws to commit internet crimes. This underlines their confidence that the police and agencies responsible for clamping down on cybercriminal activities lack the capabilities to do so. Again, persistent alliance with some corrupt officials of law enforcement agencies, bankers and shipping agents tend to reinforce the confidence perpetrators have about

succeeding in their activities. This finding corroborates Olayemi's (2014) assertion that laws to combat cybercrimes are useless if law enforcement agencies do not have the education and training necessary to operate a computer. This finding further supports Mui and Mailley's (2015) claims that opportunity becomes more attractive to perpetrators when the probability of being caught is low. This finding informs the second lesson:

Lesson Two: *Romance scam perpetrators take advantage of weaknesses in regulatory laws to commit romance scams.*

Further, a finding worthy of note is that romance scam perpetrators use computers and computer-related technologies to perpetrate romance scams. For example, they synchronise their computers with their mobile phones to enable them to communicate with clients synchronously. To attain privacy from the public, romance scammers acquire dedicated internet services and other mobile internet facilities. A possible interpretation of this finding can be linked to the affordability of internet services in Ghana. This finding, coupled with the evolving cyber-culture which creates avenues for easy transfer of knowledge among young Ghanaians, is substantiated by Park et al. (2019), who found that even though internet access has been beneficial to individuals and communities regarding education and employment, the connection between the internet and cyber offences seems more potent with the broad deployment of broadband internet. A suggestive lesson is then drawn:

Lesson Three: *Romance scam perpetrators take advantage of computer ownership and the affordability of dedicated internet services.*

An important point that cannot be discounted with respect to the findings' analysis was scammers' exactitude at extrapolating the routine activities and availability of victims. Victims

tend to share their schedule of activities with their *lovers* in their quest to plan meeting times due to differences in time zones, which allows scammers to better meet the relationship expectations of the would-be victims. Additionally, victims' constant presence tends to allow the scammers the leverage of time to financially profile them. Financial profiling includes income levels, creditworthiness, and properties owned by the victim. Obtaining detailed information about victims is made more likely when they spend sufficient time online with scammers. This finding is in line with Leukfeldt and Yar's (2016) that cybercrime victims often spend so much time online, which provides a greater chance of being exposed to online crimes. A lesson is thus suggested that:

Lesson Four: *Victims' availability and constant online engagement with perpetrators warrant them opportunities to commit internet romance scams.*

7.2.3 Ability

Ability has been identified as a person's internal skills or proficiencies required to complete a task. Lickiewicz (2011) pointed out some traits perceived as cybercriminals' abilities in that regard; social and technical abilities. Social abilities constitute the ability of an individual to function in a group and internalise social norms. On the other hand, technical skills are general knowledge concerning programming languages, computer systems, and network functioning. Evidence from the data collected for this study indicates that online romance scammers possess both social and technical abilities. Social abilities refer to the perpetrators' abilities to function as a group and understand the functional duties of all members. Again, their social relationships and ability to maintain constant storylines with victims cannot be overlooked. The preceding discussions about perpetrators' social abilities thus inform the following lesson:

Lesson Five: *Scammers hold a high level of interactional social ability that aids them in keeping their victims believing seemingly legitimate truths, which turn out to be lies.*

Further, online romance scammers possess technology-related abilities that cannot be overemphasised. While most perpetrators interviewed for the study had no formal IT training, they use basic functions of computers and related technologies in their daily operations. Except for the group leader, who had some level of computer training, the members learned the act of committing cyber-offences on the *job*. Also, the perpetrators' awareness of the needed technology and applications to use at particular points in time affords them the leverage of outpacing their victims and, by extension, law enforcement. For example, perpetrators use sophisticated applications to ensure anonymity in cyberspace. This outcome of the study is in line with Clough's (2010) assertion that the ability to commit computer crimes was limited mainly to those with access and expertise. Today, the technology is ubiquitous and increasingly easy to use, ensuring its availability to both offenders and victims. This finding, therefore, informs the lesson:

Lesson Six: *Romance scammers employ sophisticated IT skills even though they do not possess formal education in IT. This is made possible due to the easy transfer of knowledge among scammers.*

7.2.4 Rationalising Online Romance Scam

This research has provided a context for why people participate in cybercrime and their abilities and opportunities. As a result, the justifications that romance scam perpetrators offer for their crime participation are presented in this section. Analysis of the findings suggests that online romance scammers perceive their activities as less dangerous than traditional crimes like

robbery and murder. Clearly, they seem not to be mindful of the post-victimisation issues that their victims are left to deal with. Per the views of online romance scammers in Ghana, cybercriminal activities are standard practices that people commit even without knowing. Comparisons are often queried by romance scam perpetrators between their cybercrime activities and piracy (i.e. torrent downloads), which is a common practice among students (Akbulut & Dönmez, 2018).

Along with targeting their victims, romance scammers see them as selfish, ignorant, and unintelligent people who are slow to recognise scams and often fail to complain even after being deceived. This attribution is made against the backdrop of scammers spending a considerable amount of time with their victims in an effort to get to know them inside out. Some romance scammers engage their victims for close to a year or more. This is evident in data showing that victims who emotionally attach themselves to the scammers are likely to be swindled out of large sums of money. Romance scam perpetrators often profile themselves as men on dating platforms and create impressions that they are wealthy independent men capable of ensuring the victims' financial and emotional contentment. It is in the context of such falsehoods that some victims fall for the deceit of the scammers. This finding aligns with a previous study by Akanle et al. (2016), which recorded that greedy, gullible individuals and foreign nationals are the primary victims of cybercriminals in West Africa. It further endorses a claim by Whitty (2018) and Cross (2015) that many romance scam victims are often promised wealth as well as perfect relationships by scammers. In that regard, to make enormous personal profits quickly, victims are motivated to believe stories from scammers.

Regardless of what has been discussed so far in the preceding paragraph, online romance scam perpetrators also profile themselves on dating platforms as young girls who, along the line,

exchange photographs (mostly nude pictures) for money at the request of their victims (see section 5.5.1). More often than not, when scammers assume this position, they tend to engage men whose only interests are to prey on young ladies on dating platforms. Scammers, after several exchanges of naked photographs and videos, blackmail the men into paying huge sums of money, else they risk being supposedly reported to the FBI for exploitation. In terms of research on online romance scams, this result appears to be novel, hence the corresponding lessons:

Lesson Seven: *Perpetrators moderate the severity of their offences by engaging in selective social comparisons. For example, they compare romance scams to traditional crimes and digital piracy.*

Lesson Eight: *Romance scam perpetrators moderate the salience of their crimes by perceiving victims as greedy, gullible, and unintelligent.*

7.3 Romance Scam Behavioural Dynamics

This section seeks to answer the second research question; *how do cybercrime behaviours change over time?* The corresponding analysis in section 6.4 provides valuable insights to address this question. The analysis brought to bear three stages to represent romance scammers' behavioural dynamics. Whereas data from the cybercrime perpetrators described a curvature in respect to their behavioural dynamics – creation, maturation and decline, a divergent argument was made by a top law enforcement official against the notion of a curve in favour of a cycle (see Figure 8.3).

In attempting to answer this question, it is imperative to profile the characteristics of individuals who engage in romance scams. The online romance scam space appears to be dominated by males between the ages of fourteen and forty years. Even though this study did not consider minors in data collection, assertions by internet café owners and operators revealed that there are younger individuals (of less than 14 years) sponsored by their parents to engage in scams. A plausible reason for this development may be linked to the fact that the space also involves females who do not necessarily show up at the internet cafés as their male counterparts do. It also supports the idea that computer illiterates pay computer savvy people ostensibly to commit scams on their behalf, thus creating an opportunity for outsourced ability. Earlier studies have indicated that universities and other higher learning institutions are breeding grounds for cybercriminals (Aransiola & Asindemade, 2011). Even though this claim's cogency was not investigated in this study, the data analysis suggests that community-based internet cafés serve as the hotbeds for instigating cyberdeviant behaviours. Again, the findings contradict another finding by the authors (Aransiola & Asindemade, 2011) that since the knowledge of computers is a precondition for an individual's involvement in cybercrime, most students below the postsecondary level of education could not be involved in it. The following lessons are thus drawn from these findings:

Lesson Nine: *Cybercrime is a male-dominated space with female accomplices who act as decoys on behalf of their male counterparts.*

Lesson Ten: *Community-based internet cafés serve as breeding grounds for instigating cybercriminal behaviours.*

In terms of dynamics, individuals in the development stage are characterised by a lack of clarity regarding the types of crimes they expect to commit. What is perceptible to them is their quest

to acquire gadgets for personal use or make profits from selling them. Analysis of the data from this perspective indicates that individuals at this stage are often guided by their mentors (established perpetrators). They often possess little to no skill and operate on a very narrow repertoire when they start engaging in chat sessions. These catalogues of lines are often repeated until the beginner-perpetrator advances to the maturation stage. Unlike the creation stage, the maturation stage is characterised by a multiplicity of internet crimes committed with the aim of making quick money. For instance, while the creation stage involves clients finding and chatting and attempts to bypass e-commerce platforms with acquired credit cards (often given to them by their mentors), the maturation stage delves deeper into instances of forgery and black-market trading for credit cards.

Over the past few years, the government has made some progress with attempts to combat cybercrimes in Ghana. Such attempts include establishing the Cybercrime Unit of the Ghana Police Service, formulating the Ghana National Cyber Security Policy & Strategy and passing the Cybersecurity Act 2020 by Parliament. However, activities of corrupt law enforcement officials, bankers and officials of state postal agencies who collaborate with cybercrime perpetrators threaten the realisation of the goal of combatting cybercrime in Ghana. It is noteworthy that romance scam activities thrive when perpetrators can establish these relationships.

The final stage of the behavioural dynamics is the *decline stage*. This stage is characterised by changes in the environment within which the perpetrators operate. From the data analysis, public education and tightening of security features on dating and e-commerce platforms limit perpetrators from effortlessly having their ways. Perpetrators are then compelled to delve into other ventures such as mobile money fraud, sports betting and intermediation when they start

declining. One thing that is not clear from the perpetrators' perspective is whether they branch into traditional crimes when they are no more able to keep up with the extravagant lifestyles they hitherto lived. However, it is evident from the data analysed that perpetrators have the option of seeking religious/spiritual relief to keep up with their lifestyles. While there was no primary evidence to validate this claim, it seems to be common knowledge among the study respondents. Again, this study cannot substantiate the success rate of cyber-religious activities.

Despite the fact that parts of the above results confirm what is in the literature, such as association with corrupt state officials and bankers (Aransiola & Asindemade, 2011), it also provides an interesting starting point for understanding the behavioural dynamics of romance scam perpetrators, especially with the perpetrators as the primary source of evidence. As a result of these findings, the following lessons were derived:

Lesson Eleven: *Cybercriminals at the creation stage possess little to no skills in committing cybercrimes and have no clear sense of direction.*

Lesson Twelve: *Online romance scam perpetrators at the maturation stage engage in a multiplicity of carefully calculated internet crimes. They also join cybercrime syndicates and knowledge-sharing groups and mentor others.*

Lesson Thirteen: *Online romance scam perpetrators during their decline endeavour in mobile money fraud, sports betting and intermediation for the beginner-perpetrators. Traditional crimes become attractive at this stage.*

7.4 Romance Scam Pathways

This study adds to existing studies on the Romance Scammer Persuasive Techniques Model (Whitty, 2013a) by bringing new insights to the initial model. The findings from this research suggest that the success and failure of a romance scam attempt depend on the perpetrator's perseverance and the victim's unfamiliarity with scammers' strategies (Whitty, 2019). Therefore, this study compressed Whitty's (2013) five-stage trajectory into a three-phase pathway: preparatory, crisis and termination phases.

At the heart of the *preparatory phase* is the establishment of relationships with victims. The analysis of the finding suggested that for perpetrators to progress to the next phase of the pathway, they must pass a test that victims pose to them in attempts to relate to them based on their perceived nationalities. Contrary to previous research on perpetrators' romance scam trajectories (Cross, 2015; Whitty, 2013), there seems to be no evidence of would-be victims using tests to ascertain the genuineness of the relationships. This finding perhaps stems from the fact that some victims may be oblivious of the consequences of their questions to perpetrators. In contrast, others may have been aware of perpetrators' approaches and, therefore, the test. This finding, therefore, suggests the following lesson:

Lesson fourteen: *Strategies for finding, priming, and defrauding victims vary from perpetrator to perpetrator. Targets often include independent and wealthy individuals seeking lasting relationships.*

The second phase of the scam pathway is the *crisis phase*. As highlighted in the analysis of the findings, this phase has two main approaches. First is the scammer-led approach where scammers under the pretence of date seeking lead and take charge of communication with the

victims. Second is the victim-led approach in which scammers profile themselves as young ladies seeking relationships with older men.

This phase is primarily made distinct by the multiplicity of internet crimes that are perpetrated. These include simultaneous crimes such as credit card theft, black-market under dealing, and illegal shopping on e-commerce platforms. Central at this phase is the scammers' attempts to solidify their relationships, hence exchanging gifts that scammers acquire using stolen credit cards and stolen identities. Button and Cross (2017) noted that at this phase, the offender is testing the trust established between themselves and the victim and pushing the boundaries to see what is acceptable, which also corroborates Whitty's (2013) foot-in-the-door technique adopted by perpetrators. Unknown to the victims, their addresses, obtained through the exchange of gifts, are often used as a transit for shipping the items purchased using stolen credit cards under the guise of undertaking humanitarian projects in Africa. Scammers, to court victims into parting with colossal sums of money, further craft tragic stories of robbery, kidnapping or accidents that appeal to the victims' emotions of love.

As evident from the data analysis, the second approach in this phase is the victim-led approach, in which scammers pose as young ladies searching for relationships with older men. This approach's uniqueness is that perpetrators go into relationships with the intention of supplying victims with naked pictures and videos in return for money. A striking incident of note with this approach is the practice of using females as decoys to answer phone calls and show up at the banks on behalf of their male counterparts. While the scammer-led approach is evident in previous studies (Cross, 2015; Kopp et al., 2015; Whitty, 2013a, 2013b; Whitty & Buchanan, 2016), the dynamics of the victim-led approach seem not have been previously identified in the literature. Hence the following lessons:

Lesson Fifteen: *Romance scam perpetrators use stolen credit cards to lavish their victims with gifts while utilising that opportunity to establish their relationships' legitimacy.*

Lesson Sixteen: *Romance scam perpetrators, under the guise of undertaking humanitarian projects in Ghana, often use victims' addresses as transits for shipping items purchased with stolen credit cards.*

The *termination phase* is made up of two main activities: the first is the deferred sting, and the second is the termination. In the deferred sting, which emanates from the client-led approach, perpetrators predominantly rely on naked pictures of unfamous pornography models and face-changing graphics applications which are used in exchange for money in the previous phase. They often blackmail clients whom they accuse of having exploited them with threats to report to the FBI and publish naked pictures of the clients on social media platforms unless they part with huge sums of money. Little can be said about this approach in previous research plausibly because victims often feel embarrassed about reporting such scams (Deevy et al., 2012). The sting in this approach is labelled deferred because, ordinarily, stinging takes place in the crisis phase; however, perpetrators in the client-led approach defer their sting to the final phase of the pathway and then terminate the relationship.

Existing studies have identified sexual abuse as an activity that occurs prior to termination (Cross, 2015; Kopp et al., 2015; Whitty, 2013a). However, analysis of the findings of this study projected contrary evidence. It was revealed that, upon becoming financially content with the relationship, perpetrators terminate it by deleting all digital footprints that may lead the victim or forensic investigators to them.

Lesson Seventeen: *Romance scammers in the victim-led approach blackmail their victims into parting with colossal amounts of money before terminating their relationships.*

Lesson Eighteen: *Romance scammers clean their digital footprints after terminating relationships with their victims to avoid being traced for apprehension.*

7.5 Chapter Summary

The chapter set out to analyse the findings presented in the previous chapter with particular interest to three research questions:

Concerning the first research question on *the mechanisms that trigger cybercriminal behaviours*, the outcome of the analysis emanating from the case indicted that several factors converge to motivate one to commit romance scams in Ghana. Among the several factors are unemployment, low-level income, low level of education and ultimately, the desire to liberate oneself from the shackles of poverty. The chapter further revealed that cybercrime perpetrators leverage the opportunities provided to them in their environment, such as weaknesses in combative laws against internet crimes, cybergang cultures, victims' routine activities, ownership of computer and computer-related technologies, and internet affordability. Again, the chapter revealed that perpetrators acquire social and technical abilities to aid them in engaging in internet crimes. Lastly, in relation to the first research question, the analysis suggested that scammers tend to find self-satisfying excuses to make sense of their unlawful actions.

Regarding the second research question of *how cybercrime behaviours change over time,* the study found three cybercriminal behaviour dynamics. First is the creation stage, which marks the conception of ideas to commit online crimes, coaching and mentoring, and compliance to a scripted repertoire of scam lines until a person gains the self-confidence to act independently. Second is the maturation stage, where perpetrators become mature in the act of committing internet crimes. The analysis projected that scammers at this point engage in a multiplicity of crimes such as forgery, credit card fraud and identity theft. However, at the core of this stage is the connivance with corrupt state officials to circumvent laws enacted to combat internet crimes. The decline stage was identified in the analysis as the last stage in the perpetrator behavioural dynamics. This stage marks the retrogression of activities that hitherto brought a constant flow of money to the perpetrators.

Regarding the third question on the *strategies online dating romance scammers employ in finding, priming, and defrauding their victims,* the analysis developed a three-phase pathway based on previous studies by Whitty (2013a): the preparatory, crisis and termination phases. The preparatory phase per the analysis comprised the creation of profiles, winking and grooming victims. Perpetrators then create tragic stories of robbery, kidnapping or accidents that appeal to the victims' emotions to manipulate them into parting with colossal amounts of monies to help them out of their predicaments in the crisis phase. The last phase is the termination phase, where scammers, upon duping their victims, delete all digital footprints to avoid being traced.

The chapter thence produced eighteen lessons emanating from the results of the findings.

CHAPTER EIGHT

SUMMARY, CONCLUSION AND CONTRIBUTIONS

8.1 Chapter Overview

In the previous chapter, a discussion of the analysis of the findings of this study was conducted. The discussions aimed to address the research questions raised in chapter one while also keeping in mind the guidance of the research framework in chapter three. This chapter concludes by summarising the entire research journey with particular emphasis on the findings of this study. The chapter consequently reflects on the theories employed for this study, the conceptual framework and the methodology. Lastly, the research's contributions and implications, limitations and directions for future research are discussed.

8.2 Summary of the Research and Major Findings

This study aimed to uncover the mechanisms that underpin the commission of online romance scams and establish an online romance scam pathway from the perpetrators' perspective. The study set out three primary research objectives to achieve this goal, which were later translated into research questions. The first was to unearth the mechanisms that trigger cybercriminal behaviours. This objective was further broken down to reflect four research questions; a) What are the motivational factors of romance scam behaviours? b) What abilities do cybercrime perpetrators possess that aid them in the commission of online romance scams? c) Which environmental forces enable the work performance of cyber-offenders? and d) What neutralisation strategies do romance scam perpetrators employ to justify their unlawful behaviours? The second objective was to explore how romance scam perpetrators' behaviours change over time. The last objective was to explore online dating romance scammers' strategies in finding, priming, and defrauding their victims.

Literature on romance scams, advance fee fraud, identity theft, and credit card fraud was reviewed in a quest to achieve these objectives. Definitions of cybercrime and, by extension, online romance scams were given. The definition was largely in conformance with Barn and Barn's (2016) concept that "An agent is motivated by either an intrinsic desire or an extrinsic need to commit an action. Actions are perceived as crimes depending upon a receiver agent's viewpoint. If an action is a cybercrime (and so subsuming the concept of crime), then the cybercrime must be mediated through technology. That is, some form of technology must be involved to enact a cybercrime. An action must have a target, and the target must endure some impact. An impact is the effect of a crime on a target and can be economic, psychological or geo-political". (p.6)

An enquiry into the literature on cybercrime was undertaken to understand the dominant issues, methodologies, theories, economic distribution, and levels of analysis to find answers to the research questions posed in chapter one. The review was limited to peer-reviewed articles published between 2010 and 2018. This was to limit the study to current findings and gaps in the area of research. A few observations were made during the literature review, which served as the backbone for this study. First is the arguable paucity of theory-based studies in cybercrime research, hence the call to explore how existing theories could help understand both the victims' and perpetrators' behaviours and intentions (Boateng et al., 2011; Holt & Bossler, 2014; Jaishankar, 2008; Venkatraman et al., 2018). Second, information systems research has tended to concentrate on Type I crimes while ignoring the socio-technical component, leading to the decision to research romance scams, a type of cybercrime that encompasses people's social behaviour as well as their use of technology to commit crimes against other people.

Subsequently, the theories and frameworks used in previous cybercrime research were reviewed. A conceptual framework was developed to direct the current study's research method, drawing on routine activity theory, the motivation, opportunity, ability framework, and neutralisation theory. The framework suggests that scams are committed when a socioeconomically motivated agent exploits opportunities in his or her setting and his or her ability to commit scams. The framework further posits that the agent invents explanations to deny the true motivation of his/her actions: neutralisation, and it varies from agent to agent.

With the developed framework as a guide, interview guides were developed for subsequent engagement with respondents. Respondents were carefully selected to reflect the various dimensions of the phenomenon under study. The data collected were transcribed, coded and analysed, and subsequently discussed in line with previous studies on the phenomenon. Eighteen lessons were derived from the conduct of the research. The lessons are presented in Table 8.1 in line with the research objectives and corresponding contributions.

Table 8.1 Summary of Findings and Contributions

Research Objectives	Research Findings	Gaps Address	Core Contribution
a. To unearth the mechanisms that trigger cybercriminal behaviours.	**Motivation** ***L1:*** *An interplay of various socio-economic factors, including unemployment, low-level income, low-level education, and quick money syndrome, is a major driving force behind the commission of online romance scams.* **Opportunity** ***L2:*** *Romance scam perpetrators take advantage of weaknesses in regulatory laws to commit romance scams.* ***L3:*** *Romance scam perpetrators take advantage of computer ownership and the affordability of dedicated internet services.* ***L4:*** *Victims' availability and constant online engagement with perpetrators warrant them opportunities to commit internet romance scams.* ***Ability*** ***L5:*** *Scammers hold a high level of interactional social ability that aids them in keeping their victims believing seemingly legitimate truths, which turn out to be lies.* ***L6:*** *Romance scammers employ sophisticated IT skills even though they do not possess formal education in IT. This is made possible due to the easy transfer of knowledge among scammers.*	The first research objective addressed the gap in the need for future research to explore the mechanisms that converge to trigger cybercriminal behaviours (Venkatraman et al., 2018; Arora, 2016).	The results of this research showed that there are four different mechanisms that, when combined, can induce cybercriminal behaviours (i.e., motivation, opportunity, ability and rationalisation). In addition to this, the research established and empirically tested a conceptual framework on how people who commit romance scams rationalise these mechanisms. Consolidating these theories (i.e., routine activity theory, Motivation-Opportunity-Ability framework and neutralisation theory) is critical to answering questions about why and how people commit online crimes, as well as the discussion around the RAT's inability to adequately address online crimes as a standalone theory.

Research Objectives	Research Findings	Gaps Address	Core Contribution
	Rationalisation ***L7:*** *Perpetrators moderate the severity of their offences by engaging in selective social comparisons. For example, they compare romance scams to traditional crimes and digital piracy.* ***L8:*** *Romance scam perpetrators moderate the salience of their crimes by perceiving victims as greedy, gullible, and unintelligent.*		
b. To explore the dynamics of cybercriminal behaviours.	***L9:*** *Cybercrime is a male-dominated space with female accomplices who act as decoys on behalf of their male counterparts.* ***L10:*** *Community-based internet cafés serve as breeding grounds for instigating cybercriminal behaviours.* ***L11:*** *Cybercriminals at the creation stage possess little or no skills in committing cybercrimes with no clear sense of direction.* ***L12:*** *Romance scam perpetrators at the maturation stage engage in carefully calculated multiplicities of internet crimes. They also join cybercrime syndicates and knowledge-sharing groups and mentor others.* ***L13:*** *Online romance scam perpetrators during their decline endeavour in mobile money fraud, sports betting and intermediation for the beginner-perpetrators. Traditional crimes become attractive at this stage.*	The second research objective addresses the need to establish direct, complementary evidence from attacker-side data and explore how their behaviours change over time (Venkatraman et al., 2018; Hui et al. (2017).	The research made a contribution by highlighting three separate behavioural dynamics associated with cybercriminals. These dynamics are creation, maturation, and decline (See Figure 6.11). This work is one of a kind in the sense that it is the very first time that an explanation of this kind has been provided regarding the behavioural dynamics of individuals who commit cybercrime. The uniqueness of this contribution is the fact that the study elicited and empirically examined data from active cybercrime perpetrators. The data collection was done in four phases (see Figure 5.7)

Research Objectives	Research Findings	Gaps Address	Core Contribution
c. To explore the strategies that online romance scammers employ in finding, priming and defrauding their victims.	***L14:*** *Strategies for finding, priming, and defrauding victims vary from perpetrator to perpetrator. Targets often include independent and wealthy individuals seeking lasting relationships.* ***L15:*** *Romance scam perpetrators use stolen credit cards to flourish their victims with gifts while utilising that opportunity to establish their relationships' legitimacy.* ***L16:*** *Romance scam perpetrators, under the guise of undertaking humanitarian projects in Ghana, often use victims' addresses as transits for shipping items purchased with stolen credit cards* ***L17****: Romance scammers in the victim-led approach blackmail their victims into parting with colossal amounts of money before terminating.* ***L18:*** *Romance scammers clean their digital blueprints after terminating relationships with their victims to avoid being traced for apprehension.*	This objective addresses the call for future research to investigate the tactics used by criminals on dating websites, as well as the cruel ways in which they continue to exploit vulnerable victims (Cross & Holt, 2021; Whitty, 2013b, 2013a; Carter, 2021).	The consolidation of complementary evidence from online romance scam offenders led to the development of a romance scam pathway (see Figure 8.2). Knowledge about the strategies employed by romance scammers seems to have been dominated by evidence from the victims' perspectives in developing frameworks to this effect. In this regard, the romance scam pathway developed in this study serves as a starting point towards appreciating the techniques that romance scam perpetrators employ in finding, priming and defrauding their victims, particularly from the perspective of the offenders. The study also revealed an approach (i.e., victim-led approach) in the commission of internet crimes which has not been captured in literature. In the victim-led strategy, scammers pose as young ladies and allow victims (mostly males) to make demands in the form of naked photographs and webcam videos in exchange for money. Scammers who use this strategy sting their victims by blackmailing them.

Research Objectives	Research Findings	Gaps Address	Core Contribution
			This finding is unique because the victim-led approach in the scammers' persuasive techniques has arguably not been documented in previous studies, making this study a pioneering one in that regard.

Source: Author's construct

8.3 Reflections

Given a study of this nature, it is appropriate to reflect on the processes and approaches employed to conduct the study in the quest to find solutions to the research problem and achieve the objectives. This exercise aims at making compelling arguments for the designs adopted for this study and their appropriateness in realising the research contributions. In that regard, three areas were selected (theories, conceptual framework, and methodology). These represent the fundamental building blocks that hold this research together.

8.3.1 Reflections on Theories

In an effort to solve the research problem and find answers to the research question, it was essential to conduct a review of the existing literature on cybercrime. The review indicated a paucity of cybercrime studies in information systems and, by extension, the use of theories in that regard. For example, the categorisation of articles in the course of the literature review pointed out that articles that did not employ theories in their studies unsurprisingly formed about 70% of the papers analysed (e.g. Arora, 2016; Lindsay, 2017; Menon & Guan Siew, 2012; Mueller, 2017). Nonetheless, routine activity theory dominated most of the consolidated papers, that is, articles from the eight journals in the Senior Scholars' Basket of Information Systems and other related journals. Even though the RAT has been extensively used in cybercrime research, there seems to be an intense debate about its applicability in explaining online activities (Leukfeldt & Yar, 2016; Eck & Clarke, 2003). The study, in light of this, adopted the RAT (Cohen & Felson, 1979), MOA (MacInnis & Jaworski, 1989) and NT (Sykes & Matza, 1957). These theories were chosen not only in response to calls to look at how current theories could help explain the actions and motivations of both victims and perpetrators in cybercrime studies (Holt & Bossler, 2014; Jaishankar, 2008; Venkatraman et al., 2018) but also because they better suit the study's objectives.

It is important to note that the consolidation of the frameworks to study the phenomenon provided a rich insight and enriched the applicability of the conceptual framework in addressing the research questions. Again, it is instructive to note that other theories such as the space transition theory (Danquah & Longe, 2011; Jaishankar, 2008), deindividuation theory (Festinger et al., 1963; Wada et al., 2012) and protection motivation theory (Jansen & Leukfeldt, 2015) which have been used in previous cybercrime studies could to some extent have aided in addressing the research problem. However, their assumptions did not fall in line with the requirements outlined by the research objectives.

8.3.2 Reflection on Conceptual Framework

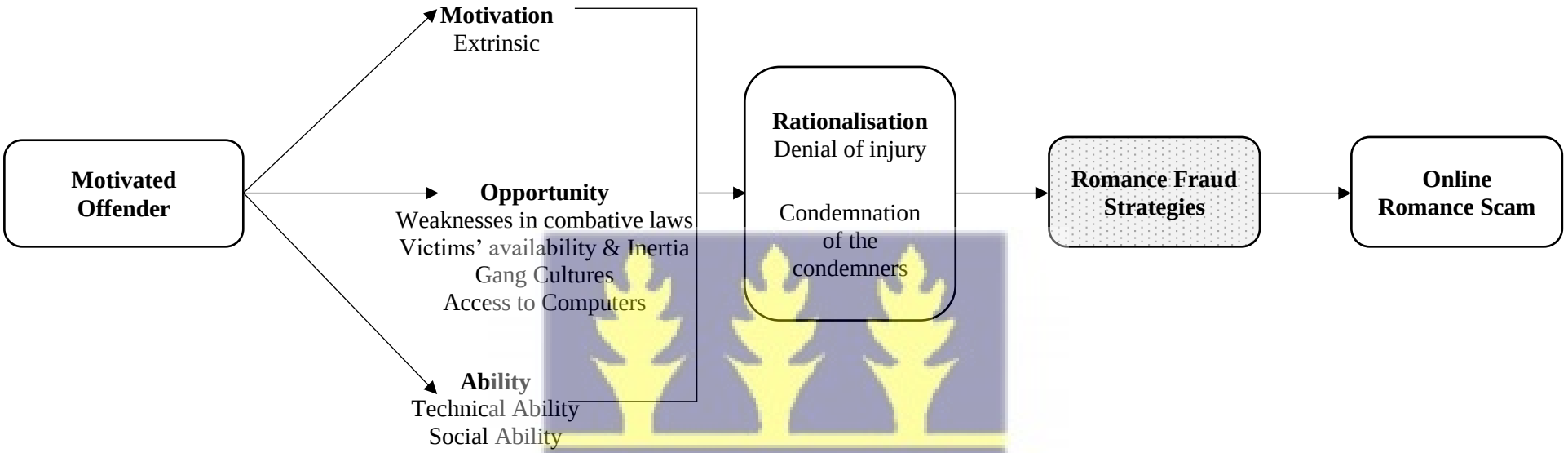
A research framework was subsequently developed by merging the RAT (Cohen & Felson, 1979), MOA framework (MacInnis & Jaworski, 1989) and neutralisation theory (Sykes & Matza, 1957). A conceptual framework is a visual or written product, one that "explains, either graphically or in narrative form, the main things to be studied – the key factors or concepts – and the presumed relationships among them (Miles & Huberman, 1994, p.18). The development of the research framework took into consideration studies that reflect the research objectives hence combining factors that best fit the constructs of the selected theories from previous literature. It is essential to understand that the constructs had been studied in previous cybercrime literature, but either in isolation or in unison with other constructs.

The framework suggested that for online romance scams to be perpetrated, five active components must be present: a motivated offender, motivation, opportunity, ability, and rationalisation. The motivated offender is someone who must be an agent willing to commit internet crimes (Akers, 2013). Motivation assumes that the said offender must have socio-economic conditions that drive him/her to commit internet romance scams. Opportunity

reflects the forces in a person's environment that enable the person to engage in the commission of online romance scams. Ability is either the social or technological qualities that the individual possesses to perform online romance scams, and rationalisation is the defence mechanisms that individuals raise to hide the true motivation for their unlawful behaviours. In effect, the framework suggests that scams are committed when a socioeconomically motivated agent takes advantage of opportunities in his or her environment and fraud capacity. It further claims that the agent fabricates justifications to defend his or her actions.

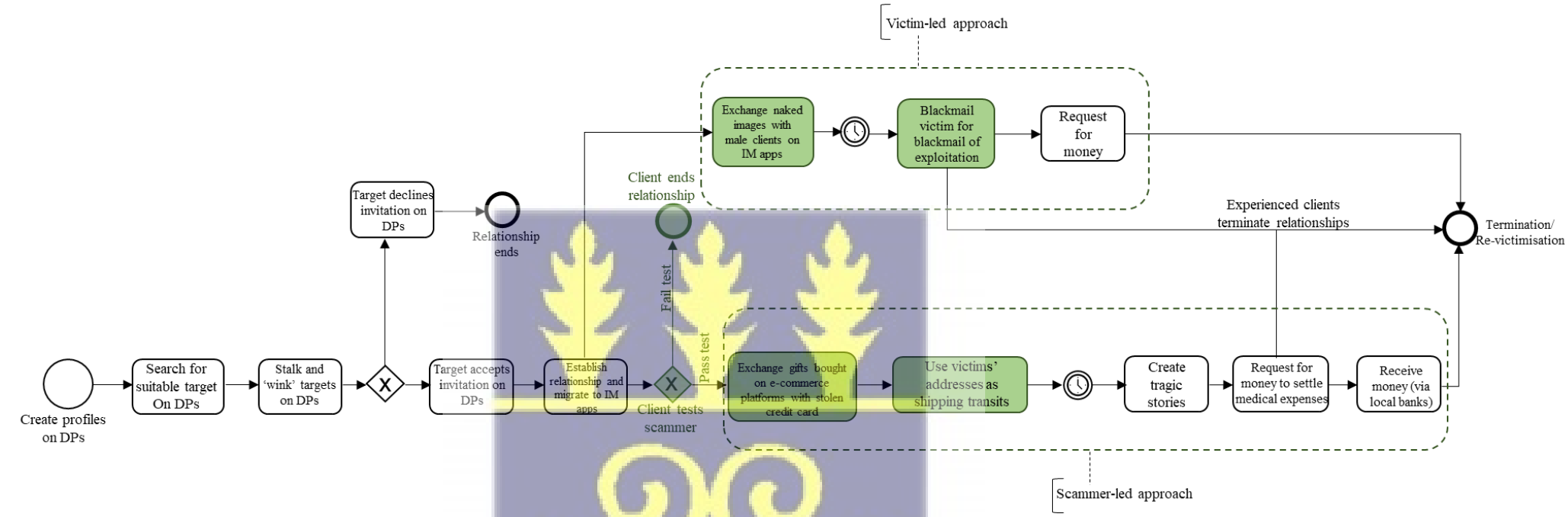
Guided by the foregoing assumptions and their reflections in the framework, data was collected, analysed, and discussed. Empirical evidence from the study revealed that for online romance scams to be committed, perpetrators put in place strategies that start from finding to stinging their victims (see Figure 8.2). This, therefore, meant an adjustment to the initial framework (Figure 3.4); hence, the post-study framework (see Figure 8.1) to address the third research question.

Figure 8.1 Revisited Conceptual Framework



Source: Author's Construct

Figure 8.2 The Online Romance Scam Pathway



Legends

DP - Dating Platforms
IM - Instant Messaging Apps (WhatsApp, Telegram etc.)

- Existing Findings
- New Findings

Source: Author's Construct

Furthermore, to achieve the purpose of this research of developing an online romance scam pathway, the study dwelt on Whitty's five-stage romance scam persuasive technique to develop a three-phase romance scam pathway (see Figure 8.2). It is essential to note that data for the development of the RFP emanated from the field data collected with the research framework as a guide in order not to lose sight of the boundaries of the framework. It is worth emphasising that the novelty of the development of the RSP stems from the fact that it was empirically developed with primary data from romance scam perpetrators.

8.3.3 Reflection on Methodology

The choice of a research method largely depends on the phenomena and issues under study, the specific context of the research, and other components of the design (Maxwell, 2012). This study was undertaken from the critical realist's (CR) philosophical position. The primary claim of CR is that a world exists independently of the researcher's knowledge of it (Sayer, 2004). Critical realists argue against empiricism and positivism, contending that science is not just about recording constant conjunctions of observable events but about objects, entities, and structures that exist (even though perhaps unobservable) and generating the events we do observe (Mingers, 2004). Mingers (2004) further asserts that critical realism enables the researcher to get beneath the surface to understand and explain why events occur as they do. This laid a strong foundation for this study to adopt CR's philosophical stance in that the study went beyond generalising IT-related crimes as cybercrime to providing a detailed exposition of the multiplicity of internet crimes committed by cybercrime perpetrators.

CR embraces a plurality of methodologies: quantitative, qualitative, and mixed methods (Easton, 2010; Scott et al., 2013; Wynn Jr & Williams, 2012). A qualitative methodology was adopted to unearth the mechanisms that underlie the commission of online romance scams in

Ghana. According to Hu (2018), the use of qualitative methods in CR-based research is more established. Further, Scott et al. (2013) argue that qualitative approaches are more capable of explaining a social phenomenon and providing situated empirical explanations, making them "epistemologically valid." It is against this backdrop that this study adopted the qualitative approach.

8.4 Contribution and Implications of the Research

As expected of every research exercise, this research's contribution can be viewed along five elements: research, theory, methodology, practice, and policy. As illustrated in Table 8.2, the study's contributions have been mapped against the research questions and findings.

8.4.1 Contribution to Research

From the perspective of the perpetrators, the aim of this study was to uncover the mechanisms that underpin the commission of online romance scams and to establish an online romance scam pathway. With this aim at the core of this study, it is instructive to outline how its achievement informs knowledge.

Drawing from the literature review, it was evident that research on online romance scams seem not to have attracted the attention of information systems researchers. A plausible reason for this may be the technical lenses with which information systems researchers approach cybercrime and arguably give less attention to socio-technical internet crimes such as romance scams. This study, in this regard, is perhaps, one of the first studies, if not the first, on romance scams in information systems, thereby contributing to addressing the paucity of socio-technical cybercrime literature in the discipline. Unsurprisingly, a portion of this thesis published in the 2020 conference proceedings of the Americas Conference on Information Systems (AMCIS

2020) appears to have been the only romance scam study in the Information Security and Privacy (SIGSEC) track. The paper was subsequently nominated for best paper at the conference. The paper was consequently selected as one of three papers reviewed by Cross (2020). Cassandra Cross is a romance scam scholar who has been cited several times in this thesis.

In addition, this research found that the perpetrators of romance scams go through three distinct stages in terms of the behavioural dynamics that they exhibit. The stages of creation, maturation, and decline were determined to exist. This study is the first to identify these dynamics because previous literature have not covered these stages. This serves as a starting point for future researchers to build on in order to better appreciate the behavioural dynamics of the cybercrime perpetrator.

Lastly, this study contributes to research by expanding the romance scam persuasive techniques (Whitty, 2013b), which have hitherto been developed using data from victims and dating platforms. This study identified a method used by scammers to defraud their victims that is also lacking in existing literature: the victim-led approach, in which scammers pose as young ladies and allow victims (mostly males) to make demands in the form of naked photographs and webcam videos in exchange for money. This strategy is used by scammers to sting their victims by blackmailing them.

8.4.2 Contribution to Theory

The study's uniqueness in terms of theoretical contribution stems from the fact that it is arguably one of the first studies in information systems research to apply the MOA framework to the study of cybercriminal behaviours. Again, this study is arguably one of the first to

combine all four dimensions. Thus, motivation, opportunity, ability and rationalisation. Previous studies that have attempted to understand the triggers of cybercrime have done so from either motivation or motivation and rationalisation. This implication cannot be overlooked as the study aims to add to the existing body of knowledge regarding cybercrime studies as well as respond to research gaps considering the sparsity of studies that employed social or criminology theories.

Additionally, considering the debate surrounding the routine activity theory's applicability in explaining cybercrimes, this study attempted to contribute to studies in efforts towards resolving this academic debate by combining the RAT, MOA and NT. Combining these theories resulted in developing a comprehensive conceptual framework for understanding the motivation, ability, and opportunity rationalisation of online romance scammers. This was also done in response to calls by scholars in the discipline to explore how existing theories could assist in understanding the behaviour and intention of perpetrators in cyberspace (Holt & Bossler, 2014; Jaishankar, 2008; Venkatraman et al., 2018).

8.4.3 Contribution to Methodology

Qualitative interviews with offenders have been a crucial method for gathering from cybercrime perpetrators. Only a few academics have successfully carried out such works, possibly due to the unique challenges regarding access to this population (Hutchings & Holt, 2018). The choice to use offenders as the primary source of evidence for this study was intended to contribute to the ostensibly narrow gap of low representation of offender-side data in cybercrime literature. That notwithstanding, this study was conducted using a longitudinal case study approach with a romance scam syndicate and other self-identified individual romance scam perpetrators who voluntarily opted to divulge information for this study after

the confidentiality of their information was explained to them. This venture demonstrates the possibility of demystifying ways to obtain offender-side data in cybercrime research. The approach was further adopted in response to a recent call in a publication in the MISQ by Hui et al. (2017) to establish direct, complementary evidence from attacker-side data in cybercrime research.

Furthermore, the consolidation of complementary evidence from online romance scam offenders led to the development of a romance scam pathway. Knowledge about the strategies employed by romance scammers seems to have been dominated by evidence from the victims' perspectives in developing frameworks to this effect. In this regard, the romance scam pathway developed in this study (see Figure 8.2) serves as a starting point towards appreciating the techniques that romance scam perpetrators employ in finding, priming and defrauding their victims, particularly from the perspective of the offenders.

8.4.4 Contribution to Practice

Concerning practice, this study's contribution can be looked at in three ways: The implications for dating platforms, patrons of the platforms and anti-romance scam campaigners.

Regarding platforms, this study presents a rich content of information that may inform managers and developers of dating platforms about the various approaches romance scammers adopt in bypassing security features put in place on their platforms. It also goes a long way to inform the managers of the platforms that not all persons on their platforms are there for the purpose for which the platforms were designed. This then requires the dating platforms to institute accommodating measures to encourage patrons to report suspected accounts for subsequent investigations.

Again, this study presents rich insights for the users of dating platforms to be abreast with the modus operandi of romance scam perpetrators. This is particularly important because thousands of individuals are victimised by online romance scammers, but many of those victims feel embarrassed to tell their stories. The few stories that get told are not enough to dissuade other love seekers. The data in this thesis, therefore, presents ample evidence ostensibly describing how the perpetrators operate. A critical take-away for date seekers on dating platforms to note is the need to engage the scammers' intellectual competencies and occasionally quiz them on pertinent issues. Such issues may be political, geographic, leisure and tourism, to mention a few.

Regarding anti-scam platforms, this study presents a rich insight for platforms engaged in educating date seekers about the dangers of romance scams. Therefore, it is essential to note that a portion of this thesis published in the 2020 Proceedings of the Americas Conference on Information Systems has been adopted on some platforms for the purpose of educating date seekers (see appendix G).

8.4.5 Contribution to Policy

Concerning policy development, it is evident that Ghana is making strides toward combatting cybercrimes in the country. This includes the development of the Ghana National Cyber Security Policy & Strategy, the passing of the Cybersecurity Act 2020 by Parliament and the observation of October as the cybersecurity month. Despite these policies, Ghana has gradually gained ground alongside Nigeria as a hotspot for the commission of online romance scams emanating from West Africa. Therefore, it is essential for policy developers to consider the attack side of affairs, as most of the policies have been defensive in nature.

Additionally, this study triangulated data from various perspectives and as a result, provided adequate information for law enforcement agencies about the modus operandi of cybercriminals in Ghana. It is instructive to note that the nature of romance scams demands collaboration between the law enforcement agencies and Internet Service Providers to fish out malicious Internet Protocols (IP) to aid in combatting the cybercrime menace in Ghana. Again, the data will aid in ongoing collaborative discussions between the ITU, Regional Development Forum and the Ghana Government to expedite any ongoing policy formulation.

Table 8. 2 Summary of Contributions and Their Indicators

Type	Contribution	Indicators
Research	1. This study in relation to the paucity of socio-technical crime studies in the IS discipline, is perhaps, one of the first studies on romance scams in information systems, thereby contributing to addressing the issue of lack of studies.	1. Two conference papers and two book chapter publications. One of the publications was • *the only romance scam paper in the AMCIS 2020 Security and Privacy Track.* • *nominated for best paper award at the AMICS 2020 conference.* • *one of three selected papers reviewed by Cross (See Cross, 2020).*
	2. This study contributes to research by expanding the romance scam persuasive techniques (Whitty, 2013b), which have hitherto been developed using data from victims and dating platforms. The pathway can be used to study cybercrime perpetrators' techniques in other forms of internet crimes.	2. The development of a romance scam pathway (See Figure 8.2).
Theory	1. Considering the debate surrounding the routine activity theory's applicability in explaining cybercrimes, this study attempted to contribute to literature in an effort toward resolving this academic debate by combining the RAT, MOA and NT.	1. Developed and empirically tested a conceptual framework on how romance scam perpetrators rationalise their motivation,

Type	Contribution	Indicators
		opportunities, and abilities (See Figure 8.1).
Methodology	1. This study contributes to methodology by aggregating primary evidence directly from romance scam perpetrators in an effort to ostensibly close the gap in offender-side data representation in cybercrime literature.	1. Interviews as quoted in some sections of this thesis (e.g., see chapters 5 and 6). 2. A trajectory of data collection phases and quotes as illustrated in Figure 5.7.
Practice	1. This study provides a wealth of information to managers and developers of dating platforms about the various methods romance scammers use to circumvent security features implemented on their platforms. The study also provides insights for platforms that educate date seekers about the dangers of romance scams.	1. Discussion of the findings of this study with practitioners (see section 8.5) 2. Adoption of a published portion of this thesis on an anti-scam platform for public education (see appendix G). 3. Invitation to join an anti-scam platform (www.romancescams.org).
Policy	1. The findings of this study will aid in ongoing collaborative discussions between the ITU, Regional Development Forum and the Ghana Government regarding cybercrime policy development.	1. A review of the various criminal and cybersecurity acts of Ghana (see section 5.4).

Source: Author's Construct

8.5 Practitioners' Perspectives on the Study's Findings

Following the study's conclusion, the post-study frameworks and findings were shared with practitioners interested in cybercrime in an online group discussion. Practitioners included two lawyers, three police officers, a private security network administrator, a media practitioner and a representative from the cybercrime authority. The major outcomes of the meeting are summarised below:

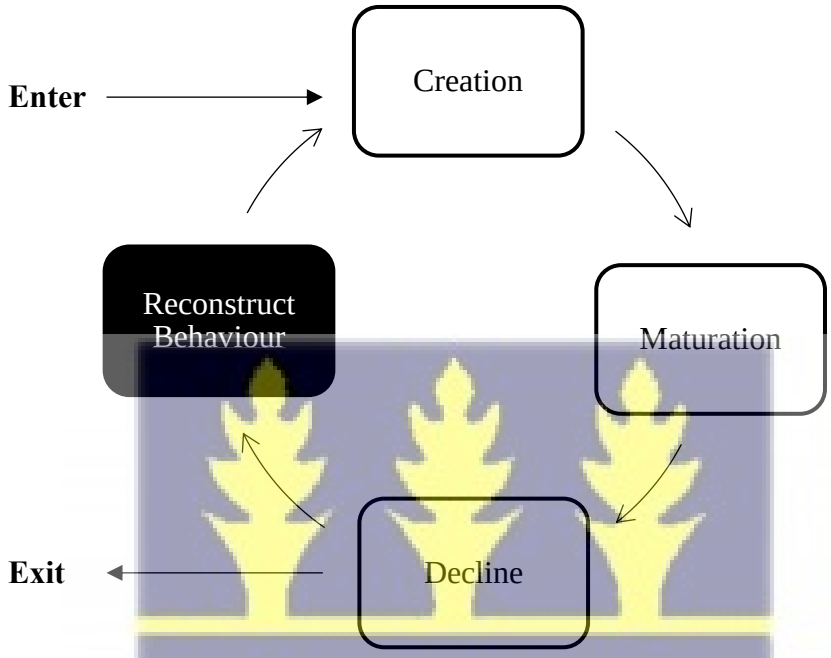
First, in terms of offender demographics, practitioners believe that there are perpetrators younger than the age range found in this study (fourteen years). However, such individuals do not usually progress from the creation to the maturation stage, according to the discussions. On curbing the menace, and especially the internet cafés' role as the hotbeds for the creation of cybercriminals, there is the need for the government to find a way to regulate internet cafés. This could include setting time limitations for specific ages and monitoring IP activities regularly.

On the regulatory front, it appears that a cybersecurity act (Act 1038) has been passed, which establishes the Cyber Security Authority, protects the country's critical information infrastructure, regulates cybersecurity activities, ensures the safety of children on the internet, and develops Ghana's cybersecurity ecosystem. Despite the act being enacted to combat cybercrime, it appears to be mute on romance scams while being emphatic on child pornography, exploitation, and other forms of internet vices. Contrary to data presented about the lack of regulatory frameworks, lawyers in the forum believed that the promulgation of Act 1038 presents an interesting starting point for prosecuting or defending individuals accused of cyber offences.

Lastly, all practitioners in the forum agreed on the romance scam pathway developed in Figure 8.2. However, the output of the behavioural dynamics model was challenged as practitioners were of the opinion that some cybercriminals do not decline. According to the practitioners, most offenders struggle with exiting while at their decline stage. The struggle is a result of maintaining the social standards they set for themselves whiles at the maturation stages. In this regard, they suggested that cyber offenders reconstruct their behaviours and return to the creation stages with other forms of crimes along with romance scams. Such may include

kidnapping and ritual killing (cyber-spiritualism) to support their romance scam efforts. The model (Figure 6.11) was thence revised to reflect the suggestions of the practitioners as illustrated in Figure 8.3.

Figure 8.3 Revised ORF Perpetrators' Behavioural Dynamics Model



Source: Author's Construct

8.6 Outputs from This Thesis

The thesis, prior to its completion, has produced a number of patentable outputs which have received considerable attention globally. The ensuing paragraphs present in chronological order the outputs from this thesis.

First among the outputs was a book chapter publication titled "Unveiling Cybercrime in a Developing Country" in the *"Encyclopaedia of Criminal Activities and the Deep Web"* published by IGI Global. The chapter presented portions of the data collected for the study and utilised one of the theories (RAT) to test its applicability within the context in which it was

adopted. The paper also exposed the researcher to the various forms of cybercrimes committed in Ghana. The DOI number for the chapter is 10.4018/978-1-5225-9715-5.ch005.

The second output was also a completed book chapter titled "Cybercrime Research: A Review of Research Themes, Frameworks, Methods, and Future Research Directions", published in the *"Handbook of Research on Managing Information Systems in Developing Economies"*, a publication by IGI Global. The chapter, which was the systematic review section of chapter two of this study, was assigned the DOI number 10.4018/978-1-7998-2610-1.ch024.

An offshoot of the systematic review was also submitted for publication at the Midwest Association for Information (MWAIS) Conference. The conference was scheduled to take place on the 28th and 29th of May, 2020, at Drakes University, Des Moines, Iowa. However, it did not come off as scheduled due to the travel ban imposed due to the Covid-19 pandemic. Nonetheless, the paper was published in the conference proceedings. The paper was titled "A Systematic Literature Review of Digital Piracy Research in Information Systems Journals (2010 – 2020): Preliminary Insights".

The fourth output of the thesis is a paper developed from the first research objective on the mechanisms that trigger cybercriminal behaviours. The paper was presented at the virtually held 2020 Americas Conference on Information Systems (AMCIS 2020) on the 13th of August, 2020. The paper, a best paper nominee at the conference, was titled "Rationalising online Romance Fraud: In the Eyes of the Offender". Since its publication in the 2020 AMCIS conference proceedings, the paper has received extensive attention from academics and practitioners at large. For instance, it was one of three papers reviewed by Cassandra Cross, a renowned romance scam scholar who has been cited on different occasions in this thesis (See

Appendix F for the full review). The paper was again adopted by SCARS™ Romance Scams & Scammers, and its content summarised into posters and infographics for public education (See Appendix G).

8.7 Research Limitations and Pointers for Future Research

During this study, some limitations were identified, which call for recommendations for future studies. First among the limitations are the unique challenges that accompany data collection in studies of this nature, as perpetrators were sceptical about divulging such vital information about their operations. They, as a result, withheld information they deemed not meant for public consumption. Another limitation regarding data collection from scammers is the leverage of convenience. Data for the study were collected at the convenience of the perpetrators. In some instances, there were *data no shows* as respondents failed to answer calls for scheduled meetings. Again, re-establishing contact with independent perpetrators was not possible as they only agreed to divulge information at the first instance of data collection. Further, the study did not consider data from minors, as it would have been interesting to know how people under eighteen years old who engage in romance scams rationalise their activities.

Furthermore, the case for this study was conducted among perpetrators who possessed all of the necessary mechanisms (i.e., motivation, opportunity, ability, and rationalisation) to commit online romance scams. However, interactions with some respondents outside of the case revealed that some offenders lack the skills required to commit online romance scams. As a result, they outsource their operations by paying others to chat with their clients and shop on their behalf. Going by the framework and its assumption, ability becomes an opportunity leveraged by the outsourcing perpetrator in this regard. Future research may look at how

abilities become opportunities in this context and how this scenario affects the framework's structure.

Furthermore, the data focused on Ghanaian romance scam perpetrators situated in Accra. It is worth noting that the rich insights into romance scammers' operations revealed in this study, though rich, are nonetheless not exhaustive. Future studies may consider the effect of migration policies and migration (e.g., AfCTA) on cybercriminal activities in Ghana. This direction has been necessitated by the fact that there were traces of neighbouring migrants during data collection and their contribution to committing internet crimes emanating from Ghana. Additionally, the research problem was addressed within a Ghanaian setting considering the emerging cyberculture of Ghanaian youth. It would be thought-provoking for future researchers to consider conducting the same research in a different context. This may produce different or similar results.

REFERENCES

Adomi, E. E., & Igun, S. E. (2008). Combating cyber crime in Nigeria. *The Electronic Library*, *26*(5), 716–725.

Akbulut, Y., & Dönmez, O. (2018). Predictors of digital piracy among Turkish undergraduate students. *Telematics and Informatics*, *35*(5), 1324–1334.

Akers, R. L. (1991). Self-control as a general theory of crime. *Journal of Quantitative Criminology*, *7*(2), 201–211.

Akers, R. L. (2013). *Criminological theories: Introduction and evaluation*. Routledge.

Alavi, M., & Carlson, P. (1992). A review of MIS research and disciplinary development. *Journal of Management Information Systems*, *8*(4), 45–62.

Alkaabi, A., Mohay, G., McCullagh, A., & Chantler, N. (2010). Dealing with the problem of cybercrime. *International Conference on Digital Forensics and Cyber Crime*, 1–18.

AlKalbani, A., Deng, H., & Kam, B. (2015). Organisational Security Culture and Information Security Compliance for E-Government Development: The Moderating Effect of Social Pressure. *Pacific Asia Conferences Information Systems*, 65. *(PACIS 2015)* (pp. 1-11).

Alli, R., Nicolaides, R., & Craig, R. (2018). Detecting advance fee fraud emails using self-referential pronouns: A preliminary analysis. *Accounting Forum*, *42*(1), 78–85.

Almerdas, S. (2014). The criminalisation of identity theft under the Saudi Anti-Cybercrime Law 2007. *Journal of International Commercial Law and Technology*, *9*(2), 80-94.

Angel, A., & Bates, B. (2014). Terministic screens of corruption: A cluster analysis of Colombian radio conversations. *Kenneth Burke Journal*, *10*(2), 1-17.

Angen, M. J. (2000). Evaluating interpretive inquiry: Reviewing the validity debate and opening the dialogue. *Qualitative Health Research*, *10*(3), 378–395.

Aransiola, J. O., & Asindemade, S. O. (2011). Understanding cybercrime perpetrators and the strategies they employ in Nigeria. *Cyberpsychology, Behavior, and Social Networking*,

14(12), 759–763.

Ardhianti, M., & Yulianto, B. (2021). Intertextuality in Cybercrime Texts as Social Reality in Indonesia. *International Journal of Innovative Science and Research Technology*, *6*(7), 1290–1295.

Argote, L., McEvily, B., & Reagans, R. (2003). Managing knowledge in organisations: An integrative framework and review of emerging themes. *Management Science*, *49*(4), 571–582.

Arief, B., & Adzmi, M. A. Bin. (2015). Understanding cybercrime from its stakeholders' perspectives: Part 2--defenders and victims. *IEEE Security & Privacy*, *13*(2), 84–88.

Arora, B. (2016). Exploring and analysing Internet crimes and their behaviours. *Perspectives in Science*, *100*(8), 540–542.

Astley, W. G., & de Ven, A. H. (1983). Central perspectives and debates in organisation theory. *Administrative Science Quarterly*, *28*(2), 245–273.

Bai, F., & Chen, X. (2013). Analysis on the new types and countermeasures of credit card fraud in mainland China. *Journal of Financial Crime*, *20*(3), 267–271.

Bai, S., & Koong, K. S. (2017). Financial and other frauds in the United States: a panel analysis approach. *International Journal of Accounting & Information Management*, *25*(4), 413–433.

Bande, L. C. (2018). Legislating against Cyber Crime in Southern African Development Community: Balancing International Standards with Country-Specific Specificities. *International Journal of Cyber Criminology*, *12*(1), 9-26.

Bankole, F. O., & Bankole, O. O. (2017). The effects of cultural dimension on ICT innovation: Empirical analysis of mobile phone services. *Telematics and Informatics*, *34*(2), 490–505.

Banville, C., & Landry, M. (1989). Can the Field of MIS be Disciplined? *Communications of*

the ACM, *32*(1), 48–60.

Barfi, K. A., Nyagorme, P., & Yeboah, N. (2018). The Internet Users and Cybercrime in Ghana: Evidence from Senior High School in Brong Ahafo Region. *Library Philosophy and Practice*, *17*(15), 1–16.

Barker, K. J., D'amato, J., & Sheridon, P. (2008). Credit card fraud: awareness and prevention. *Journal of Financial Crime*, *15*(4), 398–410.

Barn, R., & Barn, B. (2016, 12-15 June). *An ontological representation of a taxonomy for cybercrime*. 4th European Conference on Information Systems, Istanbul, Turkey.

Bartholomae, F. (2018). Cybercrime and cloud computing. A game theoretic network model. *Managerial and Decision Economics*, *39*(3), 297–305.

Baruah, S. (2019). Botnet Detection: Analysis of Various Techniques. *International Journal of Computational Intelligence & IoT*, *2*(2), 461-467.

Bay, D., Cook, G. L., Grubisic, J., & Nikitkov, A. (2014). Identifying fraud in online auctions: A case study. *Accounting Perspectives*, *13*(4), 283–299.

Benbasat, I., Goldstein, D. K., & Mead, M. (1987). The case research strategy in studies of information systems. *MIS Quarterly*, *11*(3), 369–386.

Berg, S. E. (2009). Identity theft causes, correlates, and factors: A content analysis. In F. Schmalleger & M. Pittaro (Eds.), Crimes of the Internet (pp., 225-250). Upper Saddle River, NJ: Pearson Education, Inc.

Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. C. (2011). Data mining for credit card fraud: A comparative study. *Decision Support Systems*, *50*(3), 602–613.

Bigné, E., Hernández, B., Ruiz, C., & Andreu, L. (2010). How motivation, opportunity and ability can drive online airline ticket purchases. *Journal of Air Transport Management*, *16*(6), 346–349.

Bisman, J. (2010). Postpositivism and accounting research: A (personal) primer on critical

realism. *Australasian Accounting Business & Finance Journal*, *4*(4), 3-25.

Blackburn, S. (2005). *The Oxford dictionary of philosophy*. OUP Oxford.

Blumberg, M., & Pringle, C. D. (1982). The missing opportunity in organisational research: Some implications for a theory of work performance. *Academy of Management Review*, *7*(4), 560–569.

Boateng, R. (2014). Resources, electronic-commerce capabilities and electronic-commerce benefits: Conceptualising the links. *Information Technology for Development*, *22*(2), 242–264.

Boateng, R., Olumide, L., Isabalija, R. S., & Budu, J. (2011). Sakawa-cybercrime and criminality in Ghana. *Journal of Information Technology Impact*, *11*(2), 85–100.

Bolimos, I. A., & Choo, K.-K. R. (2017). Online fraud offending within an Australian jurisdiction. *Journal of Financial Crime*, *24*(2), 277–308.

Bossler, A. M., & Holt, T. J. (2010). The effect of self-control on victimisation in the cyberworld. *Journal of Criminal Justice*, *38*(3), 227–236.

Bowles, M. (2012). The business of hacking and birth of an industry. *Bell Labs Technical Journal*, *17*(3), 5–16.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101.

Bressler, M. S. (2009). The impact of crime on business: A model for prevention, detection & remedy. *Journal of Management and Marketing Research*, *2*(1), 12–20.

Buchanan, T., & Whitty, M. T. (2014). The online dating romance scam: causes and consequences of victimhood. *Psychology, Crime & Law*, *20*(3), 261–283.

Budd, C., & Anderson, J. (2011). *Consumer fraud in Australasia: Results of the Australasian consumer fraud taskforce online Australia surveys 2008 and 2009*. Australian Institute of Criminology.

Burgoon, J. K., & Qin, T. (2006). The dynamic nature of deceptive verbal communication. *Journal of Language and Social Psychology*, *25*(1), 76–96.

Burrel, G., & Morgan, G. (2006). Sociological paradigms and organisational analysis. *Aldershot, Gower*.

Burrell, G., & Morgan, D. L. (1979). *Sociological Paradigms and Organisational Analysis*. Heinemann Educational Books Ltd.

Button, M., & Cross, C. (2017). *Cyber frauds, scams and their victims*. Taylor & Francis.

Carlson, D. E. (2014). *Debit/Credit Card Fraud Prevention Software and Smart Phone Application System and Process*. Google Patents.

Carminati, M., Caron, R., Maggi, F., Epifani, I., & Zanero, S. (2015). BankSealer: A decision support system for online banking fraud analysis and investigation. *Computers & Security*, *53*(2015), 175–186.

Carter, E. (2021). Distort, extort, deceive and exploit: Exploring the inner workings of a romance fraud. *The British Journal of Criminology*, *61*(2), 283–302.

Carter, N., Bryant-Lukosius, D., DiCenso, A., Blythe, J., & Neville, A. J. (2014). The use of triangulation in qualitative research. *Oncology Nursing Forum*, *41*(5), 545-547.

Cassim, F. (2011). Addressing the growing spectre of cyber crime in Africa: evaluating measures adopted by South Africa and other regional role players. *Comparative and International Law Journal of Southern Africa*, *44*(1), 123–138.

Cavaye, A. L. M. (1996). Case study research: a multi-faceted research approach for IS. *Information Systems Journal*, *6*(3), 227–242.

Cecez-Kecmanovic, D., Janson, M., & Brown, A. (2002). The rationality framework for a critical study of information systems. *Journal of Information Technology*, *17*(4), 215–227.

Chaudhary, K., Yadav, J., & Mallick, B. (2012). A review of fraud detection techniques:

Credit card. *International Journal of Computer Applications*, *45*(1), 39–44.

Cheng, L., Li, W., Zhai, Q., & Smyth, R. (2014). Understanding personal use of the Internet at work: An integrated model of neutralisation techniques and general deterrence theory. *Computers in Human Behavior*, *38*(2014), 220–228.

Choi, K. (2008). Computer crime victimisation and integrated theory: An empirical assessment. *International Journal of Cyber Criminology*, *2*(1), 308-333.

Choo, F., & Tan, K. (2007). An "American Dream" theory of corporate executive Fraud. *Accounting Forum*, *31*(2), 203–215. https://doi.org/10.1016/j.accfor.2006.12.004

Choo, K.-K. R. (2008). Organised crime groups in cyberspace: a typology. *Trends in Organised Crime*, *11*(3), 270–295.

Choo, K.-K. R., & Smith, R. G. (2008). Criminal exploitation of online systems by organised crime groups. *Asian Journal of Criminology*, *3*(1), 37–59.

Chua, W. F. (1986). Radical developments in accounting thought. *Accounting Review*, *61*(4), 601–632.

Clark, B. H., Abela, A. V, & Ambler, T. (2005). Organisational motivation, opportunity and ability to measure marketing performance. *Journal of Strategic Marketing*, *13*(4), 241–259.

Cohen, L. E., & Felson, M. (1979). On estimating the social costs of national economic policy: A critical examination of the Brenner study. *Social Indicators Research*, *6*(2), 251–259.

Cohn, E. G., & Farrington, D. P. (1999). Changes in the most-cited scholars in twenty criminology and criminal justice journals between 1990 and 1995. *Journal of Criminal Justice*, *27*(4), 345–359.

Coleman, J. W. (1994). Neutralisation theory: An empirical application and assessment. *Unpublished Doctoral Dissertation, Oklahoma State University, Stillwater*.

Cox, R. W., Johnson, T., & Richards, G. E. (2009). Routine Activity and Internet Crime. In F. Schmalleger & M. Pittaro (Eds.), Crimes of the Internet (pp. 302-316). Upper Saddle River, N.J: Prentice Hall.

Crang, M., & Cook, I. (2007). Participant observation. In M. Crang & I. Cook (eds.), *Doing ethnographies* (pp. 36-60). London: Sage.

Creswell, J. (2009). *Research design: Qualitative, quantitative, and mixed methods approaches*. SAGE Publications, Incorporated.

Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications.

Croasdell, D., & Palustre, A. (2019). Transnational Cooperation in Cybersecurity. *Proceedings of the 52nd Hawaii International Conference on System Sciences*.

Cross, C. (2015). No laughing matter: Blaming the victim of online fraud. *International Review of Victimology*, *21*(2), 187–204.

Cross, C. (2018). Marginalised voices: The absence of Nigerian scholars in global examinations of online fraud. In *The Palgrave handbook of criminology and the global south* (pp. 261–280). Springer.

Cross, C. (2020a). Romance fraud. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 917–937.

Cross, C. (2020b). Three Paper Thursday: Broken Hearts and Empty Wallets. *Light Blue Touchpaper, Security Research, Computer Laboratory, University of Cambridge*.

Cross, C., Dragiewicz, M., & Richards, K. (2018). Understanding romance fraud: Insights from domestic violence research. *The British Journal of Criminology*, *58*(6), 1303–1322.

Cross, C., & Holt, T. J. (2021). The Use of Military Profiles in Romance Fraud Schemes. *Victims & Offenders*, *16*(3), 385–406.

Crotty, M. (1998). *The foundations of social research: Meaning and perspective in the research process*. Sage.

Cybersecurity Ventures. (2017). *2017 Cybercrime Report*.

Danermark, B., M. Ekström, L. Jakobsen and J. C. Karlsson. 1997.'Generalisation, Scientific Inference and Models foran Explanatory Social Science.'Pp. 73–114 in Explaining Society: Critical Realism in the Social Sciences, edited by Berth Danermark. Ablingdon, Oxon: Routledge.

Danquah, P., & Longe, O. B. (2011). Cyber deception and theft: An ethnographic study on cyber criminality from a Ghanaian perspective. *Journal of Information Technology Impact*, *11*(3), 169–182.

Darke, P., Shanks, G., & Broadbent, M. (1998). Successfully completing case study research: combining rigour, relevance and pragmatism. *Information Systems Journal*, *8*(4), 273–289.

Davis, J. T. (2012). Examining perceptions of local law enforcement in the fight against crimes with a cyber component. *Policing: An International Journal of Police Strategies & Management*, *35*(2), 272–284.

Deci, E. L., & Ryan, R. M. (1987). The support of autonomy and the control of behavior. *Journal of Personality and Social Psychology*, *53*(6), 1024-1037.

Deevy, M., Lucich, S., & Beals, M. (2012). Scams, schemes & swindles. *Financial Fraud Research Center, Stanford University*.

Delisi, M. (2001). Designed to fail: Self-control and involvement in the criminal justice system. *American Journal of Criminal Justice*, *26*(1), 131–148.

Dennis, A. R., Fuller, R. M., & Valacich, J. S. (2008). Media, tasks, and communication processes: A theory of media synchronicity. *MIS Quarterly*, *32*(3), 575–600.

Dixon, D. (2012). Analysis Tool or Research Methodology: Is there an epistemology for

patterns? In *Understanding digital humanities* (pp. 191–209). Springer.

Dobovšek, B., Lamberger, I., & Slak, B. (2013). Advance fee frauds messages–non-declining trend. *Journal of Money Laundering Control*, *16*(3), 209–230.

Dobson, P. J. (2002). Critical realism and information systems research: why bother with philosophy. Information research, 7(2), 7-12.

Donalds, C., & Osei-Bryson, K.-M. (2019). Toward a cybercrime classification ontology: A knowledge-based approach. *Computers in Human Behavior*, *92*, 403–418.

Donner, C. M., Marcum, C. D., Jennings, W. G., Higgins, G. E., & Banfield, J. (2014). Low self-control and cybercrime: Exploring the utility of the general theory of crime beyond digital piracy. *Computers in Human Behavior*, *34*(2014), 165–172.

Downward, P., & Mearman, A. (2006). Retroduction as mixed-methods triangulation in economic research: reorienting economics into social science. *Cambridge Journal of Economics*, *31*(1), 77–99.

Dyer Jr, W. G., & Wilkins, A. L. (1991). Better stories, not better constructs, to generate better theory: A rejoinder to Eisenhardt. *Academy of Management Review*, *16*(3), 613–619.

Easton, G. (2010). Critical realism in case study research. *Industrial Marketing Management*, *39*(1), 118–128.

Eastwood, J. G., Jalaludin, B. B., & Kemp, L. A. (2014). Realist explanatory theory building method for social epidemiology: a protocol for a mixed method multilevel study of neighbourhood context and postnatal depression. *SpringerPlus*, *3*(1), 1–12.

Eboibi, F. E. (2017). A review of the legal and regulatory frameworks of Nigerian Cybercrimes Act 2015. *Computer Law & Security Review*, *33*(5), 700–717.

Eck, J. E., & Clarke, R. V. (2003). Classifying common police problems: A routine activity

approach. *Crime Prevention Studies*, *16*,(2003), 7–40.

Eckberg, D. L., & Hill Jr, L. (1979). The paradigm concept and sociology: A critical review. *American Sociological Review*, *44*(6), 925–937.

Edelson, E. (2003). The 419 scam: information warfare on the spam front and a proposal for local filtering. *Computers & Security*, *22*(5), 392–401.

Edwards, M., Peersman, C., & Rashid, A. (2017). Scamming the scammers: towards automatic detection of persuasion in advance fee frauds. *Proceedings of the 26th International Conference on World Wide Web Companion*, Perth, Australia.

Electronic Transactions Act. (2008). *Electronic Transactions Act*. 55.

Enticott, G. (2011). Techniques of neutralising wildlife crime in rural England and Wales. *Journal of Rural Studies*, *27*(2), 200–208.

Fadel, K. J., & Durcikova, A. (2014). Enhancing the motivation, opportunity, and ability of knowledge workers to participate in knowledge exchange. *2014 47th Hawaii International Conference on System Sciences*, 3605–3614.

Fair, J. E., Tully, M., Ekdale, B., & Asante, R. K. B. (2009). Crafting lifestyles in urban Africa: Young Ghanaians in the world of online friendship. *Africa Today*, *55*(4), 29–49.

Felson, M., & Clarke, R. V. (1998). Opportunity makes the thief. Police research series, paper 98. Policing and reducing crime unit. *Research, Development and Statistics Directorate. London: Home Office*.

Festinger, L., Pepitone, A., & Newcomb, T. (1952). Some consequences of deindividuation in a group. Journal of abnormal psychology, 47(2 Suppl.), 382-389.

Finch, E. (2013). The problem of stolen identity and the Internet. In *Crime online* (pp. 39–53). Willan.

Fitzgerald, B., & Howcroft, D. (1998). Towards dissolution of the IS research debate: from polarisation to polarity. *Journal of Information Technology*, *13*(4), 313–326.

Forbes. (2017). *The True Cost Of Cybercrime For Businesses*. Forbes. https://www.forbes.com/sites/theyec/2017/07/13/the-true-cost-of-cybercrime-for-businesses/#16c370584947

Furnell, S. M. (2001). The problem of categorising cybercrime and cybercriminals. In *2nd Australian Information Warfare and Security Conference*. Australia.

Gay, L. R., & Airasian, P. W. (2000). *Student guide to accompany educational research: Competencies for analysis and application*. Merill.

Gerry, F. Q., & Moore, C. (2015). A slippery and inconsistent slope: How Cambodia's draft cybercrime law exposed the dangerous drift away from international human rights standards. *Computer Law & Security Review*, *31*(5), 628–650.

Gibbons, M. T. (1987). Introduction: The politics of interpretation. *Interpreting Politics*, Oxford, Basil Blackwell.

Glickman, H. (2005). The Nigerian "419" advance fee scams: prank or peril? *Canadian Journal of African Studies/La Revue Canadienne Des Études Africaines*, *39*(3), 460–489.

Goldman, Z. K., & McCoy, D. (2016). Deterring financially motivated cybercrime. *Journal of National Security Law & Policy*, *8*(3), 1-22.

Goodman, M. c D. (1997). Why the police don't care about computer crime. *Harvard Journal of Law & Technology*, *10*, 466–494.

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, *2*(1), 13–20.

Gottschalk, P. (2010). Categories of financial crime. *Journal of Financial Crime*, *17*(4), 441–458.

Government of Ghana (2008). Electronic Transactions Act *2008* No 772 (Gh). Retrieved from

https://www.researchictafrica.net/countries/ghana/Electronic_Transactions_Act_no_772:2008.pdf

Government of Ghana (2012). Criminal Offences (Amendment) Act *2012* No 849 (Gh). Retrieved from https://www.refworld.org/pdfid/44bf823a4.pdf

Government of Ghana (2012). Data Protection Act *2012* No 843 (Gh). Retrieved from https://nita.gov.gh/wp-content/uploads/2017/12/Data-Protection-Act-2012-Act-843.pdf

Government of Ghana (2012). Cybersecurity Act *2020* No 1038 (Gh). Retrieved from https://csdsafrica.org/wp-content/uploads/2021/08/Cybersecurity-Act-2020-Act-1038.pdf

Gray, D. E. (2013). *Doing research in the real world*. London: Sage.

Gross, M. L., Canetti, D., & Vashdi, D. R. (2016). The psychological effects of cyber terrorism. *Bulletin of the Atomic Scientists*, *72*(5), 284–291.

Gruen, T. W., Osmonbekov, T., & Czaplewski, A. J. (2005). How e-communities extend the concept of exchange in marketing: An application of the motivation, opportunity, ability (MOA) theory. *Marketing Theory*, *5*(1), 33–49.

Guba, E & Lincoln, Y. (1994). Competing paradigms in qualitative research. *Handbook of Qualitative Reseach*, *2*(163–194), 105–117.

Harbinson, E., & Selzer, N. (2019). The risk and needs of cyber-dependent offenders sentenced in the United States. *Journal of Crime and Justice*, *42*(5), 582–598.

Harris, L. C., & Daunt, K. L. (2011). Deviant customer behaviour: A study of techniques of neutralisation. *Journal of Marketing Management*, *27*(7–8), 834–853.

Harrison, A. (2018). The effects of media capabilities on the rationalisation of online consumer fraud. *Journal of the Association for Information Systems*, *19*(5), 408-440.

Hassard, J. (1995). *Sociology and organisation theory: Positivism, paradigms and postmodernity* (Issue 20). Cambridge University Press.

Healy, M., & Perry, C. (2000). Comprehensive criteria to judge validity and reliability of qualitative research within the realism paradigm. *Qualitative Market Research: An International Journal*, *3*(3), 118–126. https://doi.org/10.1108/13522750010333861

Heron, J., & Reason, P. (1997). A participatory inquiry paradigm. *Qualitative Inquiry*, *3*(3), 274–294.

Hillman, H., Hooper, C., & Choo, K.-K. R. (2014). Online child exploitation: Challenges and future research directions. *Computer Law & Security Review*, *30*(6), 687–698.

Hirschheim, R., Klein, H. K., & Lyytinen, K. (1995). *Information systems development and data modeling: conceptual and philosophical foundations*. Cambridge University Press.

Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior*, *35*(1), 20–40.

Holt, T. J., & Schell, B. H. (2011). *Corporate hacking and technology-driven crime*. IGI Global Snippet.

Holtfreter, K., Reisig, M. D., & Pratt, T. C. (2008). Low self-control, routine activities, and fraud victimisation. *Criminology*, *46*(1), 189–220.

Horkheimer, M. (1972). *Critical theory: Selected essays* (Vol. 1). A&C Black.

Hoyer, W. D., MacInnis, D. J., & Pieters, R. (2012). *Consumer Behavior* (6th ed.). South-Western.

Hu, X. (2018). Methodological implications of critical realism for entrepreneurship research. *Journal of Critical Realism*, *17*(2), 118–139.

Hua, J., & Bapna, S. (2013). The economic impact of cyber terrorism. *The Journal of Strategic Information Systems*, *22*(2), 175–186.

Huang, J., Stringhini, G., & Yong, P. (2015). Quit playing games with my heart: Understanding online dating scams. *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, vol *9148*. 216–236. Springer, Charm.

Huey, L., Nhan, J., & Broll, R. (2013). 'Uppity civilians' and 'cyber-vigilantes': The role of the general public in policing cyber-crime. *Criminology & Criminal Justice*, *13*(1), 81–97.

Hui, K.-L., Kim, S. H., & Wang, Q.-H. (2017). Cybercrime deterrence and international legislation: Evidence from distributed denial of service attacks. *Mis Quarterly*, *41*(2), 497-523.

Hung, K., & Petrick, J. F. (2012). Testing the effects of congruity, travel constraints, and self-efficacy on travel intentions: An alternative decision-making model. *Tourism Management*, *33*(4), 855–867. https://doi.org/10.1016/j.tourman.2011.09.007

Hunt, S. D. (1991). Positivism and paradigm dominance in consumer research: toward critical pluralism and rapprochement. *Journal of Consumer Research*, *18*(1), 32–44.

Hunton, P. (2011). A rigorous approach to formalising the technical investigation stages of cybercrime and criminality within a UK law enforcement environment. *Digital Investigation*, *7*(3–4), 105–113.

Hunton, P. (2012). Data attack of the cybercriminal: Investigating the digital currency of cybercrime. *Computer Law & Security Review*, *28*(2), 201–207.

Hutchings, A., & Holt, T. J. (2018). Interviewing cybercrime offenders. *JQCJC*, 75.

Ibrahim, S. (2016). Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. *International Journal of Law, Crime and Justice*, *47*, 44–57.

Iivari, J. (1991). A paradigmatic analysis of contemporary schools of IS development. *European Journal of Information Systems*, *1*(4), 249–272.

Iivari, J., & Hirschheim, R. (1996). Analysing information systems development: A comparison and analysis of eight IS development approaches. *Information Systems*, *21*(7), 551–575.

Inuwa, I., Ononiwu, C., Kah, M. M. O., & Quaye, A. K. M. (2019). Mechanisms fostering

the misuse of information systems for corrupt practices in the Nigerian public sector. *International Conference on Social Implications of Computers in Developing Countries*, Dar es Salaam, Tanzania. (122–134).

Irwin, A.S, Slay, J., Raymond Choo, K.-K., & Lui, L. (2014). Money laundering and terrorism financing in virtual environments: a feasibility study. *Journal of Money Laundering Control*, *17*(1), 50–75.

ITU. (2012). *Understanding Cybercrimes: Phenomena, Challenges and Legal Response*. International Telecommunication Union.

Jaishankar, K. (2008). Space transition theory of cyber crimes. *Crimes of the Internet*, Pearson, ISBN-13:978-0-13-231886-0, 283–301.

Jamil, Z. (2012). Global Fight Against Cybercrime: Undoing the Paralysis. *Georgetown Journal of International Affairs*, 109–120.

Jansen, J., & Leukfeldt, R. (2015). How people help fraudsters steal their money: An analysis of 600 online banking fraud cases. *Socio-Technical Aspects in Security and Trust (STAST), 2015 Workshop On*, (24–31). IEEE.

Jeong, O.-R., Kim, C., Kim, W., & So, J. (2011). Botnets: threats and responses. *International Journal of Web Information Systems*, *7*(1), 6–17.

Jonker, J., & Pennink, B. (2010). *The essence of research methodology: A concise guide for master and PhD students in management science*. Springer Science & Business Media.

Ju, J., Cho, D., Lee, J. K., & Ahn, J.-H. (2016). *An Empirical Study on Anti-spam Legislation*.

Kaplan, B., & Duchon, D. (1988). Combining qualitative and quantitative methods in information systems research: a case study. *MIS Quarterly*, *12*(4), 571–586.

Kaplan, B., & Maxwell, J. (2005). Qualitative research methods for evaluating computer information systems. In James G. Anderson, Carolyn Aydin*Evaluating the Organisational Impact of Healthcare Information Systems*, (pp. 30–55.

Kassem, R., & Higson, A. (2012). The new fraud triangle model. *Journal of Emerging Trends in Economics and Management Sciences*, *3*(3), 191–195), Springer.

Kigerl, A. (2012). Routine activity theory and the determinants of high cybercrime countries. *Social Science Computer Review*, *30*(4), 470–486.

Kincheloe, J. L., & McLaren, P. (2002). Rethinking critical theory and qualitative research. In E. Trueba & Y. Zou (Eds.), *Ethnography and Schools: Qualitative Approaches to the Study of Education* (87–138). Rowman & Littlefield Publishers.

Kling, R. (1980). Computer Abuse and Computer Crime as Organisational Activities, 2 Computer LJ 403 (1980). John Marshall Journal of Information Technology & Privacy Law, 2(1), 403-427.

Klockars, C. B. (1974). *The professional fence*. Free Press New York.

Kopp, C., Layton, R., Sillitoe, J., & Gondal, I. (2015). The Role of Love stories in Romance Scams: A Qualitative Analysis of Fraudulent Profiles. *International Journal of Cyber Criminology*, *9*(2), 205-216.

Kraemer-Mbula, E., Tang, P., & Rush, H. (2013). The cybercrime ecosystem: Online innovation in the shadows? *Technological Forecasting and Social Change*, *80*(3), 541–555.

Krauss, S. E. (2005). Research paradigms and meaning making: A primer. *The Qualitative Report*, *10*(4), 758–770.

Kshetri, N. (2009). Positive externality, increasing returns, and the rise in cybercrimes. *Communications of the ACM*, *52*(12), 141–144.

Kshetri, N. (2013a). Cybercrime and cyber-security issues associated with China: some economic and institutional considerations. *Electronic Commerce Research*, *13*(1), 41–69.

Kshetri, N. (2013b). *Cybercrime and cybersecurity in the global south*. Springer.

Kshetri, N. (2017). *Cybercrime Firms' Internationalisation Strategy and Tactics: An Exploratory Framework.*

Kuhn, T. S. (1970). *The Structure of Scientific Revolutions (Unabridged).*

Laue, C. (2011). Crime potential of metaverses. In *Virtual Worlds and Criminality* (pp. 19–29). Springer.

Lee, A. S. (1991). Integrating positivist and interpretive approaches to organisational research. *Organisation Science*, *2*(4), 342–365.

Leukfeldt, E. R. (2014a). Cybercrime and social ties. *Trends in Organised Crime*, *17*(4), 231–249.

Leukfeldt, E. R. (2014b). Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimisation. *Cyberpsychology, Behavior, and Social Networking*, *17*(8), 551–555.

Leukfeldt, E., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, *37*(3), 263–280.

Leung, X. Y., & Bai, B. (2013). How motivation, opportunity, and ability impact travelers' social media involvement and revisit intention. *Journal of Travel & Tourism Marketing*, *30*(1–2), 58–77.

Levi, M., & Leighton Williams, M. (2013). Multi-agency partnerships in cybercrime reduction: Mapping the UK information assurance network cooperation space. *Information Management & Computer Security*, *21*(5), 420–443.

Li, D., Xu, X., Chen, C., & Menassa, C. (2019). Understanding energy-saving behaviors in the American workplace: A unified theory of motivation, opportunity, and ability. *Energy Research & Social Science*, *51*, 198–209.

Li, W., Chen, H., & Nunamaker Jr, J. F. (2016). Identifying and profiling key sellers in cyber carding community: AZSecure text mining system. *Journal of Management Information*

Systems, *33*(4), 1059–1086.

Li, W., Yin, J., & Chen, H. (2016). Identifying high quality carding services in underground economy using nonparametric supervised topic model, *International Conference on Information Systems, ICIS 2016,* Dublin, Ireland.

Li, X., & Qin, Y. (2018). Research on Criminal Jurisdiction of Computer cybercrime. *Procedia Computer Science*, *131*(C), 793–799.

Lickiewicz, J. (2011). Cyber Crime psychology-proposal of an offender psychological profile. *Problems of Forensic Sciences*, *2*(3), 239–252.

Lincoln, Y. S., & Denzin, N. K. (1994). The fifth moment. *Handbook of Qualitative Research*, *1*, 575–586.

Lindsay, J. R. (2017). Restrained by design: the political economy of cybersecurity. *Digital Policy, Regulation and Governance*, *19*(6), 493–514.

Liu, S.-D. (2013). The cyberpolitics of the governed. *Inter-Asia Cultural Studies*, *14*(2), 252–271.

Longe, O. B., & Chiemeke, S. C. (2008). Cyber Crime And Criminality In Nigeria: What Roles Are Internet Access Points In Playing? *European Journal of Social Sciences*, *6*(4), 132-139.

Longe, O., Ngwa, O., Wada, F., Mbarika, V., & Kvasny, L. (2009). Criminal uses of information & communication technologies in sub-Saharan Africa: trends, concerns and perspectives. *Journal of Information Technology Impact*, *9*(3), 155–172.

MacInnis, D. J., & Jaworski, B. J. (1989). Information processing from advertisements: Toward an integrative framework. *Journal of Marketing*, *53*(4), 1–23.

Maclnnis, D. J., Moorman, C., & Jaworski, B. J. (1991). Enhancing and measuring consumers' motivation, opportunity, and ability to process brand information from ads. *Journal of Marketing*, *55*(4), 32–53.

Malgwi, C. A. (2005). Fraud as economic terrorism: the efficacy of the Nigerian Economic and Financial Crimes Commission. *Journal of Financial Crime*, *12*(2), 144–164.

Manicas, P. T., & Secord, P. F. (1983). Implications for psychology of the new philosophy of science. *American Psychologist*, *38*(4), 399.

Marcum, C. D., Higgins, G. E., Ricketts, M. L., & Wolfe, S. E. (2014). Hacking in high school: cybercrime perpetration by juveniles. *Deviant Behavior*, *35*(7), 581–591.

Marcum, C. D., Higgins, G. E., Ricketts, M. L., & Wolfe, S. E. (2015). Becoming someone new: identity theft behaviors by high school students. *Journal of Financial Crime*, *22*(3), 318–328.

Marenin, O., & Reisig, M. D. (1995). "A general theory of crime" and patterns of crime in Nigeria: An exploration of methodological assumptions. *Journal of Criminal Justice*, *23*(6), 501–518.

Margaret, A., Bhaskar, R., Collier, A., Lawson, T., & Norrie, A. (1998). Critical realism: essential readings. *London and New York: Routledge*.

Marshall, M. N. (1996). Sampling for qualitative research. *Family Practice*, *13*(6), 522–526.

Martin, N., & Rice, J. (2011). Cybercrime: Understanding and addressing the concerns of stakeholders. *Computers & Security*, *30*(8), 803–814.

Martin, W. E., & Bridgmon, K. D. (2012). *Quantitative and statistical research methods: From hypothesis to results* (Vol. 42). John Wiley & Sons.

Maslow, A. H. (1981). *Motivation and personality*. Prabhat Prakashan.

Mason, J. (2002). Sampling and selection in qualitative research. *Qualitative Researching*, Volume 2, *120*, 144.

Maxwell, J. A. (2012). *Qualitative research design: An interactive approach* (Vol. 41). Sage publications.

McAulay, L., Doherty, N., & Keval, N. (2002). The stakeholder dimension in information

systems evaluation. *Journal of Information Technology*, *17*(4), 241–255.

McDermott, R. (2011). Internal and external validity. *Cambridge Handbook of Experimental Political Science*, 27–40.

McGee, J. A., & Byington, J. R. (2013). How to counter cybercrime intrusions. *Journal of Corporate Accounting & Finance*, *24*(5), 45–49.

McGrath, J. E., & Johnson, B. A. (2003). *Methodology makes meaning: How both qualitative and quantitative paradigms shape evidence and its interpretation.*

McQuade, S. C. (2006). *Understanding and managing cybercrime*. Pearson/Allyn and Bacon Boston.

Menon, S., & Guan Siew, T. (2012). Key challenges in tackling economic and cyber crimes: Creating a multilateral platform for international co-operation. *Journal of Money Laundering Control*, *15*(3), 243–256.

Mertens, D. M. (2007). Transformative paradigm: Mixed methods and social justice. *Journal of Mixed Methods Research*, *1*(3), 212–225.

Meyer, S. B., & Lunnay, B. (2013). The application of abductive and retroductive inference for the design and analysis of theory-driven sociological research. *Sociological Research Online*, *18*(1), 86–96.

Miles, M. B., & Huberman, A. M. (1984). Drawing valid meaning from qualitative data: Toward a shared craft. *Educational Researcher*, *13*(5), 20–30.

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook*. sage.

Mingers, J. (2004). Real-ising information systems: critical realism as an underpinning philosophy for information systems. *Information and Organisation*, *14*(2), 87–103.

Mingers, J., Mutch, A., & Willcocks, L. (2013). Introduction [special issue: Critical realism in information systems research]. *MIS Quarterly*, *37*(3), 795–802.

Mingers, J., & Stowell, F. (1997). *Information systems: an emerging discipline?* McGraw-Hill.

Minor, W. W. (1981). Techniques of neutralisation: A reconceptualisation and empirical examination. *Journal of Research in Crime and Delinquency*, *18*(2), 295–318.

Mohamed, N. A., Jantan, A., & Abiodun, O. I. (2018). Protect Governments, and organisations Infrastructure against Cyber Terrorism (Mitigation and Stop of Server Message Block (SMB) Remote Code Execution Attack). *International Journal of Engineering*, *11*(2), 261–272.

Mohurle, S., & Patil, M. (2017). A brief study of wannacry threat: Ransomware attack 2017. *International Journal of Advanced Research in Computer Science*, *8*(5).

Moon, B., McCluskey, J. D., & McCluskey, C. P. (2010). A general theory of crime and computer crime: An empirical test. *Journal of Criminal Justice*, *38*(4), 767–772.

Moore, R., & McMullan, E. C. (2009). Neutralisations and rationalisations of digital piracy: A qualitative analysis of university students. *International Journal of Cyber Criminology*, *3*(1), 441-451.

Morgan, D. L. (1996). *Focus groups as qualitative research* (Vol. 16). Sage publications.

Mthembu, M. A. (2012). High road in regulating online child pornography in South Africa. *Computer Law & Security Review*, *28*(4), 438–444.

Mueller, M. (2017). Is cybersecurity eating internet governance? Causes and consequences of alternative framings. *Digital Policy, Regulation and Governance*, *19*(6), 415–428.

Mui, G., & Mailley, J. (2015). A tale of two triangles: comparing the Fraud Triangle with criminology's Crime Triangle. *Accounting Research Journal*, *28*(1), 45–58.

Mumford, E., Hirschheim, R., Fitzgerald, G., & Wood-Harper, A. T. (1985). *Research methods in information systems*. North-Holland Publishing Co.

Murphy, P. R., & Dacin, M. T. (2011). Psychological pathways to fraud: Understanding and

preventing fraud in organisations. *Journal of Business Ethics*, *101*(4), 601–618.

Myers, M. D. (1997). Qualitative research in information systems. *Management Information Systems Quarterly*, *21*(June), 1–18. https://doi.org/10.2307/249422

Myers, M. D., & Avison, D. (2002). *An introduction to qualitative research in information systems*.

Näsi, M., Oksanen, A., Keipi, T., & Räsänen, P. (2015). Cybercrime victimisation among young people: a multi-nation study. *Journal of Scandinavian Studies in Criminology and Crime Prevention*, *16*(2), 203–210.

National Communications Authority. (2017). *Workshop on Cybercrime Statistics Opens in Accra*. Press Release.

Navarro, J. N., & Jasinski, J. L. (2012). Going cyber: Using routine activities theory to predict cyberbullying experiences. *Sociological Spectrum*, *32*(1), 81–94.

Neuman, W. L. (2014). *Social Research Methods: Qualitative and Quantitative Approaches: Pearson New International Edition*. Pearson Education Limited.

Ngafeeson, M. (2010). Cybercrime classification: a motivational model. *College of Business Administration, The University of Texas-Pan American*, 1201 West University Drive, Edinburg, Texas 78541, USA.

Ngo, F., & Jaishankar, K. (2017). Commemorating a Decade in Existence of the International Journal of Cyber Criminology: A Research Agenda to Advance the Scholarship on Cyber Crime. *International Journal of Cyber Criminology*, *11*(1), 216–236.

Ngo, F., & Paternoster, R. (2011). Cybercrime Victimisation: An examination of Individual and Situational level factors. *International Journal of Cyber Criminology*, *5*(1), 773-793.

Nissen, H.-E., Klein, H. K., & Hirschheim, R. (1991). *Information systems research: contemporary approaches and emergent traditions*. Elsevier North-Holland, Inc.

Nycum, S. (1976). The criminal law aspects of computer abuse: Part I–state penal laws. *RUTGERS J. COMPUTERS & L., 5*, 271–276.

Offei, M., Andoh-Baidoo, F. K., Ayaburi, E. W., & Asamoah, D. (2020). How Do Individuals Justify and Rationalise their Criminal Behaviors in Online Romance Fraud? *Information Systems Frontiers*, 24, 475–491.

Ofulue, C. I. (2010). A digital forensic analysis of advance fee fraud (419 scams). In R. Taiwo (Ed.), *Handbook of research on discourse behavior and digital communication: Language structures and social interaction* (pp. 296–317). IGI Global.

Okpan, S. O., & Anigbogu, K. C. (2016). Declining social values and internet crime in owerri municipal, imo state, Nigeria. *Social Science Research, 3*(2), 67-83.

Olaiya, T. A., Lamidi, K. O., & Bello, M. A. (2020). Narrative of illicit money:'Yahoo'Boy (Format) of cyber scams and governance challenges in Africa. *DOI, 10*, 2155–6156.

Olayemi, O. J. (2014). A socio-technological analysis of cybercrime and cyber security in Nigeria. *International Journal of Sociology and Anthropology*, *6*(3), 116-125.

Orlikowski, W. J., & Baroudi, J. J. (1991). Studying information technology in organisations: Research approaches and assumptions. *Information Systems Research, 2*(1), 1–28.

Paek, S. Y., & Nalla, M. K. (2015). The relationship between receiving phishing attempt and identity theft victimisation in South Korea. *International Journal of Law, Crime and Justice*, *43*(4), 626–642.

Papadopoulos, A., & Brooks, G. (2011). The investigation of credit card fraud in Cyprus: reviewing police "effectiveness." *Journal of Financial Crime*, *18*(3), 222–234.

Paquet-Clouston, M., Décary-Hétu, D., & Bilodeau, O. (2018). Cybercrime is whose responsibility? A case study of an online behaviour system in crime. *Global Crime*, *19*(1), 1–21.

Park, Jiyong, Cho, D., Lee, J. K., & Lee, B. (2019). The Economics of Cybercrime: The Role

of Broadband and Socioeconomic Status. *ACM Transactions on Management Information Systems (TMIS)*, *10*(4), 1–23.

Park, JiYoung, Levy, J., Son, M., Park, C., & Hwang, H. (2018). Advances in Cybersecurity Design: An Integrated Framework to Quantify the Economic Impacts of Cyber-Terrorist Behavior. In *Security by Design* (pp. 317–339). Springer.

Parker, D. B. (1976). Computer abuse perpetrators and vulnerabilities of computer systems. *Proceedings of the June 7-10, 1976, National Computer Conference and Exposition*, 65–73.

Parra-López, E., Gutiérrez-Taño, D., Diaz-Armas, R. J., & Bulchand-Gidumal, J. (2012). Travellers 2.0: Motivation, opportunity and ability to use social media. In *Social media in travel, tourism and hospitality: Theory, practice and cases*. Ashgate Publication.

Patton, M. Q. (1990). *Qualitative evaluation and research methods*. SAGE Publications, inc.

Pereira, F., Spitzberg, B. H., & Matos, M. (2016). Cyber-harassment victimisation in Portugal: Prevalence, fear and help-seeking among adolescents. *Computers in Human Behavior*, *62*, 136–146.

Phau, I., Lim, A., Liang, J., & Lwin, M. (2014). Engaging in digital piracy of movies: a theory of planned behaviour approach. *Internet Research*.

Ponterotto, J. G. (2005). Qualitative research in counseling psychology: A primer on research paradigms and philosophy of science. *Journal of Counseling Psychology*, *52*(2), 126.

Pope, C., Ziebland, S., & Mays, N. (2000). Qualitative research in health care: Analysing qualitative data. *British Medical Journal*, *320*(7227), 114-116.

Prabowo, H. Y. (2011). Building our defence against credit card fraud: a strategic view. *Journal of Money Laundering Control*, *14*(4), 371–386.

Prabowo, H. Y. (2012). A better credit card fraud prevention strategy for Indonesia. *Journal of Money Laundering Control*, *15*(3), 267–293.

Pratt, T. C., & Cullen, F. T. (2000). The empirical status of Gottfredson and Hirschi's general theory of crime: A meta-analysis. *Criminology, 38*(3), 931–964.

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency, 47*(3), 267–296.

Prichard, J., Watters, P. A., & Spiranovic, C. (2011). Internet subcultures and pathways to the use of child pornography. *Computer Law & Security Review, 27*(6), 585–600.

Puspitosari, H., & Bidari, A. S. (2017). Ethic cyber strengthening ascriminal law policy formulations in response cyberporn. *UNTAG Law Review, 1*(2), 30–37.

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

Raj, S. B. E., & Portia, A. A. (2011). Analysis on credit card fraud detection methods. *2011 International Conference on Computer, Communication and Electrical Technology (ICCCET)*, 152–156.

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.

Reingold, N. (1980). Through paradigm-land to a normal history of science. *Social Studies of Science, 10*(4), 475–496.

Reyns, B. W. (2013). Online routines and identity theft victimisation: Further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency, 50*(2), 216–238.

Reyns, B. W. (2015). A routine activity perspective on online victimisation: Results from the Canadian General Social Survey. *Journal of Financial Crime, 22*(4), 396–411.

Reyns, B. W., & Henson, B. (2016). The thief with a thousand faces and the victim with none: Identifying determinants for online identity theft victimisation with routine

activity theory. *International Journal of Offender Therapy and Comparative Criminology*, *60*(10), 1119–1139.

Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being pursued online: Applying cyberlifestyle–routine activities theory to cyberstalking victimisation. *Criminal Justice and Behavior*, *38*(11), 1149–1169.

Richet, J.-L. (2022). How cybercriminal communities grow and change: An investigation of ad-fraud communities. *Technological Forecasting and Social Change*, *174*(2022), 1-9.

Riek, M., & Böhme, R. (2018). The costs of consumer-facing cybercrime: an empirical exploration of measurement issues and estimates. *Journal of Cybersecurity*, *4*(1), 1-16.

Robey, D. (1996). Research commentary: diversity in information systems research: threat, promise, and responsibility. *Information Systems Research*, *7*(4), 400–408.

Rodgers, W., Söderbom, A., & Guiral, A. (2015). Corporate social responsibility enhanced control systems reducing the likelihood of fraud. *Journal of Business Ethics*, *131*(4), 871–882.

Rotich, E. K., Metto, S. K., Siele, L., & Muketha, G. M. (2014). A survey on cybercrime perpetration and prevention: A review and model for cybercrime prevention. *European Journal of Science and Engineering*, *2*(1), 13–28.

Ryan, R. M., & Deci, E. L. (2000). Intrinsic and extrinsic motivations: Classic definitions and new directions. *Contemporary Educational Psychology*, *25*(1), 54–67.

Safa, N. S., Maple, C., Furnell, S., Azad, M. A., Perera, C., Dabbagh, M., & Sookhak, M. (2019). Deterrence and prevention-based model to mitigate information security insider threats in organisations. *Future Generation Computer Systems*, *97*, 587–597.

Salleh, N. M., Selamat, S. R., Yusof, R., & Sahib, S. (2016). Discovering Cyber Terrorism Using Trace Pattern. *IJ Network Security*, *18*(6), 1034–1040.

Salu, A. O. (2005). Online crimes and advance fee fraud in Nigeria-are available legal

remedies adequate? *Journal of Money Laundering Control*, *8*(2), 159–167.

Santanna, J. J., van Rijswijk-Deij, R., Hofstede, R., Sperotto, A., Wierbosch, M., Granville, L. Z., & Pras, A. (2015). Booters—An analysis of DDoS-as-a-service attacks. *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, 243–251.

Saunders, M., Lewis, P., & Thornhill, A. (2003). Research methods for business students. *New Jersey*, *4*, 100–109.

Sayer, A. (2004). Why critical realism. In *Critical Realist Applications in Organisation and Management Studies*, *11*(6), 6-20.

Schell, B. H., Martin, M. V., Hung, P. C. K., & Rueda, L. (2007). Cyber child pornography: A review paper of the social and legal issues and remedies—and a proposed technological solution. *Aggression and Violent Behavior*, *12*(1), 45–63.

Scotland, J. (2012). Exploring the philosophical underpinnings of research: Relating ontology and epistemology to the methodology and methods of the scientific, interpretive, and critical research paradigms. *English Language Teaching*, *5*(9), 9-16.

Scott, C., & Medaugh, M. (2017). Axial coding. *The International Encyclopedia of Communication Research Methods*, *10*, 1-2.

Scott, S. V, Zachariadis, M., & Barrett, M. (2013). Methodological implications of critical realism for mixed-methods research. *MIS Quarterly: Management Information Systems*, *37*(3), 855–879.

Sharma, S. (2020). I want it my way: Using consumerism and neutralisation theory to understand students' cyberslacking behaviour. *International Journal of Information Management*, *53*, 2-12.

Siemsen, E., Roth, A. V, & Balasubramanian, S. (2008). How motivation, opportunity, and ability drive knowledge sharing: The constraining-factor model. *Journal of Operations*

Management, *26*(3), 426–445.

Siggelkow, N. (2007). Persuasion with case studies. *Academy of Management Journal*, *50*(1), 20–24.

Simon, M., & Choo, K. (2014). Digital forensics: challenges and future research directions. In I.S. Kim, & J. Liu, *Contemporary Trends in Asian Criminal Justice: Paving the Way for the Future* (pp. 105-146). Seoul, South Korea: Korean Institute of Criminology.

Singleton, T. (2013). Fighting the Cybercrime Plague. *Journal of Corporate Accounting & Finance*, *24*(5), 3–7.

Siponen, M., Vance, A., & Willison, R. (2012). New insights into the problem of software piracy: The effects of neutralisation, shame, and moral beliefs. *Information & Management*, *49*(7–8), 334–341.

Smith, G. S. (2015). Management models for international cybercrime. *Journal of Financial Crime*, *22*(1), 104–125.

Soliman, M., & Azer, M. A. (2018). Web Application API Blind Denial of Service Attacks. *14th International Computer Engineering Conference (ICENCO)*, 249–253.

Solomon, D. J. (2007). The role of peer review for scholarly journals in the information age. *Journal of Electronic Publishing*, *10*(1).

Sorell, T., & Whitty, M. (2019). Online romance scams and victimhood. *Security Journal*, *32*(3), 342–361.

Soudijn, M. R. J., & Zegers, B. C. H. T. (2012). Cybercrime and virtual offender convergence settings. *Trends in Organised Crime*, *15*(2–3), 111–129.

Strauss, A., & Corbin, J. (1990). *Basics of qualitative research: Grounded theory procedures and techniques.* Sage publications.

Strong, D. M., & Volkoff, O. (2010). Understanding Organisation—Enterprise system fit: A path to theorising the information technology artifact. *MIS Quarterly*, *34*(4), 731–756.

Sukhai, N. B. (2004). Hacking and cybercrime. *Proceedings of the 1st Annual Conference on Information Security Curriculum Development*, 128–132.

Sun, J.-R., Shih, M.-L., & Hwang, M.-S. (2015). Cases study and analysis of the court judgement of cybercrimes in Taiwan. *International Journal of Law, Crime and Justice, 43*(4), 412–423.

Sykes, G. M., & Matza, D. (1957). Techniques of neutralisation: A theory of delinquency. *American Sociological Review*, *22*(6), 664–670.

Tade, O. (2013). A spiritual dimension to cybercrime in Nigeria: The 'yahoo plus' phenomenon. *Human Affairs*, *23*(4), 689–705.

Tan, H. K., & David, Y. (2017). Preying on lonely hearts: A systematic deconstruction of an internet romance scammer's online lover persona. *Journal of Modern Languages*, *23*(1), 28–40.

Teddlie, C., & Tashakkori, A. (2010). Overview of contemporary issues in mixed methods research. *Sage handbook of mixed methods in social and behavioral research*, *2*, 1-44.

Tehrani, P. M., Manap, N. A., & Taji, H. (2013). Cyber terrorism challenges: The need for a global response to a multi-jurisdictional crime. *Computer Law & Security Review*, *29*(3), 207–215.

Tillyer, M. S., & Eck, J. E. (2009). Routine activities. *21st Century Criminology: A Reference Handbook*, *1*, 279–287.

Trauth, E. M. (2001). The choice of qualitative methods in IS research. In Qualitative research in IS: issues and trends (pp. 1-19). IGI Global.

Tseloni, A., Wittebrood, K., Farrell, G., & Pease, K. (2004). Burglary victimisation in England and Wales, the United States and the Netherlands: A cross-national comparative test of routine activities and lifestyle theories. *British Journal of Criminology*, *44*(1), 66–91.

Tzeng, C.-H. (2018). How foreign knowledge spillovers by returnee managers occur at domestic firms: An institutional theory perspective. *International Business Review*, *27*(3), 625–641.

Vahdati, S., & Yasini, N. (2015). Factors affecting internet frauds in private sector: A case study in cyberspace surveillance and scam monitoring agency of Iran. *Computers in Human Behavior*, *51*, 180–187.

Valasik, M. (2014). Self-Control Theory. *The Encyclopedia of Criminology and Criminal Justice*, 1–5.

Vallerand, R. J. (1997). Toward a hierarchical model of intrinsic and extrinsic motivation. In *Advances in experimental social psychology* (Vol. 29, pp. 271-360). Academic Press.

Van Baak, C., Hayes, B. E., Freilich, J. D., & Chermak, S. M. (2018). Honor crimes in the United States and offenders' neutralisation techniques. *Deviant Behavior*, *39*(2), 187–202.

Van de Weijer, S. G. A., & Leukfeldt, E. R. (2017). Big five personality traits of cybercrime victims. *Cyberpsychology, Behavior, and Social Networking*, *20*(7), 407–412.

Van der Meulen, N. S. (2013). You've been warned: Consumer liability in Internet banking fraud. *Computer Law & Security Review*, *29*(6), 713–718.

Van der Wagen, W., & Pieters, W. (2015). From cybercrime to cyborg crime: Botnets as hybrid criminal actor-networks. *British Journal of Criminology*, *55*(3), 578–595.

Varey, R. J., Wood-Harper, T., & Wood, B. (2002). A theoretical review of management and information systems using a critical communications theory. *Journal of Information Technology*, *17*(4), 229–239.

Vazsonyi, A. T., Jiskrova, G. K., Ksinan, A. J., & Blatný, M. (2016). An empirical test of self-control theory in Roma adolescents. *Journal of Criminal Justice*, *44*, 66–76.

Vazsonyi, A. T., Machackova, H., Sevcikova, A., Smahel, D., & Cerna, A. (2012).

Cyberbullying in context: Direct and indirect effects by low self-control across 25 European countries. *European Journal of Developmental Psychology*, *9*(2), 210–227.

Venkatraman, S., Cheung, C. M., Lee, Z. W. Y., Davis, F. D., & Venkatesh, V. (2018). The "Darth" Side of Technology Use: An Inductively Derived Typology of Cyberdeviance. *Journal of Management Information Systems*, *35*(4), 1060–1091.

Verdinelli, S., & Scagnoli, N. I. (2013). Data display in qualitative research. *International Journal of Qualitative Methods*, *12*(1), 359–381.

Verma, A. (2012). Cyber pornography in India and its implication on cyber cafe operators. *Computer Law & Security Review*, *28*(1), 69–76.

Vlachos, V., Minou, M., Assimakopouos, V., & Toska, A. (2011). The landscape of cybercrime in Greece. *Information Management & Computer Security*, *19*(2), 113–123.

Wada, F., Longe, O., & Danquah, P. (2012). Action speaks louder than words-understanding cyber criminal behavior using criminological theories. *The Journal of Internet Banking and Commerce*, *17*(1), 1–12.

Wahyuni, D. (2012). The research design maze: Understanding paradigms, cases, methods and methodologies. *Journal of applied management accounting research*, *10*(1), 69-80.

Wall, D. (2001). *Crime and the Internet.(1st ed)*. Routledge.

Wall, D. (2015). Dis-organised crime: Towards a distributed model of the organisation of cybercrime. *The European Review of Organised Crime*, *2*(2), 1–20.

Wall, D. S. (2007). Policing cybercrimes: Situating the public police in networks of security within cyberspace. *Police Practice and Research*, *8*(2), 183–205.

Wall, D. S. (2015). The Internet as a conduit for criminal activity. In A. Pattavina (Ed.), *Information Technology and the Criminal Justice System* (pp. 77–98). Sage.

Wall D (2017) Crime, security and information communication technologies: The changing cybersecurity threat landscape and implications for regulation and policing. In:

Brownsword R, Scotford E and Yeung K (eds) *The Oxford Handbook on the Law and Regulation of Technology*. Oxford: Oxford University Press, 1075–1096

Walsham, G. (1995). The emergence of interpretivism in IS research. *Information Systems Research*, *6*(4), 376–394.

Warikoo, A. (2014). Proposed methodology for cyber criminal profiling. *Information Security Journal: A Global Perspective*, *23*(4–6), 172–178.

Warner, J. (2011). Understanding cyber-crime in Ghana: A view from below. *International Journal of Cyber Criminology*, *5*(1), 736.

Webster, J., & Drew, J. M. (2017). Policing advance fee fraud (AFF) Experiences of fraud detectives using a victim-focused approach. *International Journal of Police Science & Management*, *19*(1), 39–53.

Whittemore, R., & Knafl, K. (2005). The integrative review: updated methodology. *Journal of Advanced Nursing*, *52*(5), 546–553.

Whitty, M. T. (2013a). Anatomy of the online dating romance scam. *Security Journal*, *28*(4), 443–455.

Whitty, M. T. (2013b). The scammers persuasive techniques model: Development of a stage model to explain the online dating romance scam. *British Journal of Criminology*, *53*(4), 665–684.

Whitty, M. T. (2018a). 419-It's just a Game: Pathways to Cyber-Fraud Criminality emanating from West Africa. *International Journal of Cyber Criminology*, *12*(1), 97–114.

Whitty, M. T. (2018b). Do you love me? Psychological characteristics of romance scam victims. *Cyberpsychology, Behavior, and Social Networking*, *21*(2), 105–109.

Whitty, M. T. (2019). Who can spot an online romance scam? *Journal of Financial Crime*, *36*(2), 623–633.

Whitty, M. T., & Buchanan, T. (2012). The online romance scam: A serious cybercrime. *CyberPsychology, Behavior, and Social Networking*, *15*(3), 181–183.

Whitty, M. T., & Buchanan, T. (2016). The online dating romance scam: The psychological impact on victims–both financial and non-financial. *Criminology & Criminal Justice*, *16*(2), 176–194.

Wilhelm, C. (2020). Investigating Neutralisation Strategies in Digital Piracy: The Role of Content Preferences and Social Norms. *Journal of Broadcasting & Electronic Media*, *64*(2), 320–340.

Williams, M. L. (2015). Guardians upon high: an application of routine activities theory to online identity theft in Europe at the country and individual level. *British Journal of Criminology*, *56*(1), 21–48.

Winder, R. L., Probert, S. K., & Beeson, I. A. (1997). *Philosophical Issues In Information Systems*. (R. L. Winder, S. K. Probert, & I. A. Beeson (eds.)). CRC Press.

Wu, Y., Balasubramanian, S., & Mahajan, V. (2004). When is a preannounced new product likely to be delayed? *Journal of Marketing*, *68*(2), 101–113.

Wynn, D., & Williams, C. (2008b). Critical Realm-Based Explanatory Case Study Research in Information Systems. In *Proceedings of the International Conference on Information Systems (ICIS)* (pp.1-20) Paris, France (Vol. 202).

Wynn Jr, D., & Williams, C. K. (2012). Principles for conducting critical realist case study research in information systems. *MIS Quarterly*, 36(3), 787–810.

Xiao, B. S., Chan, T. K., Cheung, C., & Wong, R. Y. M. (2016). An investigation into cyberbullying perpetration: a routine activity perspective. In *Proceedings of the Pacific Asia Conference on Information Systems (PACIS), Chiayi, Taiwan* (Vol. 370).

Yan, Q., Yu, F. R., Gong, Q., & Li, J. (2016). Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A

survey, some research issues, and challenges. *IEEE Communications Surveys & Tutorials*, *18*(1), 602–622.

Yar, M. (2005). The Novelty of Cybercrime: An Assessment in Light of Routine Activity Theory. *European Journal of Criminology*, *2*(4), 407–427.

Yilma, K. M. (2014). Developments in cybercrime law and practice in Ethiopia. *Computer Law & Security Review*, *30*(6), 720–735.

Yin, R. (2002). *Case study research and applications: Design and methods* (3rd ed.). California: Sage Publications.

Yin, R. K. (2015). *Qualitative research from start to finish* (2nd ed.). New York: The Guilford Press.

Yin, R. K. (2018). *Case study research and applications. Design and methods* (6th ed.). California: Sage publications.

Yogi Prabowo, H. (2011). Building our defence against credit card fraud: a strategic view. *Journal of Money Laundering Control*, *14*(4), 371–386.

Yogi Prabowo, H. (2012). A better credit card fraud prevention strategy for Indonesia. *Journal of Money Laundering Control*, *15*(3), 267–293.

APPENDICES

Appendix A: Publications

Book Chapter Publications:

Boateng, R., & **Barnor, J. N.** (2020). Unveiling Cybercrime in a Developing Country. In M. Khosrow-Pour D.B.A. (Ed.), *Encyclopaedia of Criminal Activities and the Deep Web* (pp. 66-92). Hershey, PA: IGI Global. doi:10.4018/978-1-5225-9715-5.ch005

Barnor, J. N., & Patterson, A. A. (2020). Cybercrime Research: A Review of Research Themes, Frameworks, Methods and Future Research Directions. In R. Boateng (Ed.), *Handbook of Research on Managing Information Systems in Developing Economies* (pp. 480-502). Hershey, PA: IGI Global. doi:10.4018/978-1-7998-2610-1.ch024

Conference Paper(s):

Barnor, J.N., Boateng, R., Kolog, E. A., Afful-Dadzie, A., Entee, E., & Patterson, A. (2020). "A Systematic Literature Review of Digital Piracy Research in Information Systems Journals (2010 – 2020): Preliminary Insights" (2020). MWAIS 2020 Proceedings. 11.

Barnor, J. N. B., Boateng, R., Kolog, E. A., & Afful-Dadzie, A. (2020). "Rationalizing Online Romance Fraud: In the Eyes of the Offender". AMCIS 2020 Proceedings. 21. https://aisel.aisnet.org/amcis2020/info_security_privacy/info_security_privacy/21

Best Paper Nominee at the Americas Conference on Information Systems (AMCIS 2020).

Appendix B: Interview Guides

INTERVIEW GUIDE (PERPETRATORS)

I am a PhD student at the University of Ghana Business School, and I am researching into the triggers of online romance scams in Ghana. This research is part of the requirements for a Doctorate Degree in Information Systems. You can be confident that any information you provide will be kept strictly confidential and used for academic purposes only.

Thank you.

Date: ____/____/_____
Duration: ____hours, _____minutes

1. Please tell me about yourself (Remind respondent not to mention his/her name)
2. What is your educational background?
3. If yes, what is the nature of the job?
4. Do you know what cybercrime is?
5. Have you been engaged in cybercrime before?
6. How long have you been in the act?
7. **Kindly describe the process to me.**
   [ ] romance scam [ ] identity theft [ ] credit card fraud [others]_____

Motivation

8. How did you get into the business of cybercrime?
9. Have you ever been employed? If yes, why did you stop working?
10. Would you describe yourself as someone from a well to do family? If no, probe further.
11. What satisfaction to you gain in doing cybercrime?
12. On average how much do you make in a month?
13. Compared to your earnings when you were employed, which one is better?

Opportunity

Technology ownership

14. Do you own a computer or related devices that you use?
15. How did you come by the devices?
16. How do you access the internet?

Absence of capable guidance

17. Are you aware of any cybercrime laws in Ghana?
18. What are your thoughts on the legal implications?
19. Have you ever been pursued by the law enforcement agencies?
20. Are your parents, friends or people close to you aware of what you do/
21. How do they take it?

Gang Culture

22. Do you have friends who are also engaged in this?
23. How is your relationship with them like?
24. Do you help each other or you all operate independently?
25. Do you have partners you do this with? Both in and outside Ghana.
26. Would you say they are more successful than you or you are better off?

Victims' routine activities

27. Are your victims aware you are Ghanaian?

28. How do you find victims?
29. Which criteria do you use to choose your victims?
30. How do you describe yourself to them?
31. How do you keep them?
32. Please describe some of the techniques you utilised to persuade your client.

Miscellaneous

33. How do you receive the monies sent by your clients?
34. How are you able to circumvent the laws?
35. What do you do with the money?

Ability

36. How did you learn to use computers?
37. Have you had any formal IT training?
38. How are you able to achieve anonymity in cyberspace?
39. What are some of the applications you use in achieving your objectives?

Rationalisation

40. What kind of people do you usually target?
41. Have you ever targeted a local victim? Why?
42. How would you compare what you do to traditional crimes?
43. What is the difference between what you do and sakawa?

INTERVIEW GUIDE (POLICE OFFICIAL)

I am a PhD student at the University of Ghana Business School, and I am researching into the triggers of online romance scams in Ghana. This research is part of the requirements for a Doctorate Degree in Information Systems. You can be confident that any information you provide will be kept strictly confidential and used for academic purposes only.

Thank you.

Date: ____/____/_____

Duration: ____hours, _____minutes

Background of Respondent

1. Kindly enlighten me on your unit and position within your organisation.
2. Kindly enlighten me on your job details.
3. How long have you been working with this unit of the police department?
4. In your own words, how would you define cybercrime?
    a. *So, what actions or inactions constituent cybercrime?*
5. Has the Ghana Police Department identified, created, or established a unit or entity specifically charged with dealing with cybercrime incidents response?
    i. *If yes, please provide the following information:*
    The exact name of the unit/entity:
    ii. *The number of officers or experts in the unit/entity:*
    iii. *The regional and international organisations that unit/entity collaborate with:*
6. Is the police department technologically equipped to combat cybercrimes and other forms of technological crimes?
7. What is the computer literacy level of the cybercrime combat unit of the police service if there is any?
8. How do you employ ICT tools to detect cybercrimes?
9. What are the top 3 to 5 cybercrime offenses that Ghana suffers from most?

REPORTING

10. Which industries are most exposed to cyber-attacks and why?

11. Do they report cybercrimes to you?
    If no, are there any plausible reasons why they don't?
    If yes, what actions did the police take?

    Do defrauded victims report to you? If they do, are there nationality, gender and age breakdown of defrauded victims? *what actions did the police take?*
    If no, are there any plausible reasons why they don't?
12. Do you feel some cybercrime cases get unreported?
    If yes? Why do you think so?
13. Can you enlighten me on the categorisation of reported internet fraud cases?

APPREHENSION

14. The insurgence of mobile internet usage has made it easier for individuals to undertake internet services at their comfort. This in effect means cybercriminals can also be mobile. What laid down plans do you have in tracing cyber criminals?
15. What are some of the strategies that the police employ to clampdown cyber criminals?
16. What roles do intelligence play in fighting cybercrime?
17. What are the main problems with regard to a successful investigation of cybercrimes in Ghana?

LAW ENFORCEMENT

18. Are there domestic laws on arresting and prosecuting cybercriminals?
19. Is incarceration a possible consequence for crimes committed online?
20. Under which laws are suspected cybercriminals charged?

PROSECUTION

21. What are the processes of prosecution of cybercriminals?
22. Are there breakdowns of nationalities of arrested and prosecuted cybercriminals?
23. What are the main problems with regard to a successful prosecution of cybercrime in Ghana?

COLLABORATION

24. Are there enough logistics to aid in tracking cybercriminals?
25. Does the Ghana Police have any concrete experiences with respect to strengthening the relationship between the authorities responsible for investigating and/or prosecuting cybercrimes, and internet service providers?
    Yes ___ *No* ___
    Please explain:

INTERVIEW GUIDE (BANKERS)

I am a PhD student at the University of Ghana Business School, and I am researching into the triggers of online romance scams in Ghana. This research is part of the requirements for a Doctorate Degree in Information Systems. You can be confident that any information you provide will be kept strictly confidential and used for academic purposes only.

Thank you.

Date: ____/____/_____

Duration: ____hours, _____minutes

1. Kindly enlighten me on your position and job details in your organisation.
2. How long have you been working in this organisation?
3. How will you describe your ICT literacy level?
4. Did your organisation train you in ICT during your recruitment process?
5. Do you perceive that as a necessary venture?

   Why do you think so?
6. In your own words, how would you define cybercrime?
   a. *So, what actions or inactions constituent cybercrime?*
7. Do you have laid down measures on addressing cybercrime issues?
8. Do you have any training in dealing with cybercrime?
9. Does your organisation have a current Policy on cybercrime?

   If yes, please list such policy documents.
   If no, why?
10. Ghana is ranked 2nd on cyber fraudulent countries in Africa, does that make Ghana a safe haven for cybercriminals and subsequently blacklisting?
    How does this affect your nature of business?

INTERVIEW GUIDE (LEGAL PRACTITIONERS)

I am a PhD student at the University of Ghana Business School, and I am researching into the triggers of online romance scams in Ghana. This research is part of the requirements for a Doctorate Degree in Information Systems. You can be confident that any information you provide will be kept strictly confidential and used for academic purposes only.

Thank you.

Date: ____/____/_____

Duration: ____hours, _____minutes

1. Kindly enlighten me on your position and job details in your organisation.
2. How long have you been working as a legal practitioner?
3. Which type of law do you practice?
   common. criminal. civil. administrative.
4. In your own words, how would you define cybercrime?
   a. *So, what actions or inactions constituent cybercrime?*
5. Do you have any training in dealing with cybercrime?
6. Why will/won't you defend a cybercriminal?
7. How do you determine the jurisdiction within which cybercrimes are committed?
8. Are cyberlaws captured in the Ghanaian laws?
   If yes, kindly refer us to any documentation
   If no, what are the hindrances to the enactment of such laws?
9. Under which laws are suspected cybercriminals charged?
10. Does cybercrime have a designated legislation or it is covered by general legislation?
11. Does Ghana have a current Policy on cybercrime?
    If yes, please list such policy documents.
    If No, please set the reasons why there is no policy on cybercrime in Ghana?
12. Are cybercrimes punishable by jail time?
13. Ghana is ranked 2nd on cyber fraudulent countries in Africa, does that make Ghana a safe haven for cybercriminals and subsequently blacklisting?

INTERVIEW GUIDE (CAFÉ OWNERS/OPERATORS)

I am a PhD student at the University of Ghana Business School, and I am researching into the triggers of online romance scams in Ghana. This research is part of the requirements for a Doctorate Degree in Information Systems. You can be confident that any information you provide will be kept strictly confidential and used for academic purposes only.

Thank you.

Date: ____/____/_____

Duration: ____hours, _____minutes

1. How long have you been operating this café?
2. Can you give an estimated breakdown of gender, age and nationality of people who patronize your café?
3. Do you have any idea of what patrons use your internet for?
   How do you know?
4. How do you monitor activities of your clients?
5. Do you allow patrons of the café to install app/programs on your computers?
   Why do/don't you allow app installation on your systems?
6. Have you in any way come across VPNs installed on your client systems?
7. In your own words, how would you define cybercrime?
   a. *So, what actions or inactions constituent cybercrime?*
8. Which periods constitute the peak moments at your café?
9. Do patrons of the café seem related or seem to know themselves?
   How do you know?
10. Do you report suspected cybercrimes to authorities?
    Why do/don't you report?
11. Do your ISP contact you over suspected cybercrime emanating from your IP?

Appendix C: Ethical Clearance

UNIVERSITY OF GHANA
ETHICS COMMITTEE FOR THE HUMANITIES (ECH)
P. O. Box LG 74, Legon, Accra, Ghana

My Ref. No...ECH 038/ 20-21 ...

October 30, 2020

Jonathan Nii Barnor Barnor
Department for Operations and MIS
University of Ghana
Legon

ETHICAL CLEARANCE
(ECH 038/ 20-21)

The protocol tittle below has been reviewed and approved by the ECH Committee.

TITLE OF PROTOCOL: **UNDERSTANDING ABILITY, OPPORTUNITY AND MOTIVATION RATIONALISATION IN ONLINE ROMANCE SCAMS**

PRINCIPAL INVESTIGATOR: **JONATHAN NII BARNOR BARNOR**

Please note that the final review report must be submitted to the Committee at the completion of the study. Your research records may be audited at any time during or after the implementation. Any modification of this research project must be submitted to ECH for review and approval prior to implementation.

Please report all serious adverse events related to this study to ECH within seven (7) days verbally and in writing within fourteen (14) days.

This certificate is valid till October 29, 2021. You are to submit annual reports for continuing review.

Please accept my congratulations.

Yours Sincerely,

Professor C. Charles Mate-Kole
ECH Chair

Cc: Prof. Richard Boateng, Department of Operations and MIS, UG

Tel: +233-303933866 Email: ech@ug.edu.gh

Appendix D: Protocol Consent Form

UNIVERSITY OF GHANA

Official Use only Protocol number

Ethics Committee for Humanities (ECH)

PROTOCOL CONSENT FORM

Section A- BACKGROUND INFORMATION

Title of Study:	**Understanding Ability, Opportunity and Motivation Rationalisation in Online Romance Scams**
Principal Investigator:	**Mr.Jonathan Nii Barnor Barnor**
Certified Protocol Number	

Section B– CONSENT TO PARTICIPATE IN RESEARCH

General Information about Research

In this study, I aim to study the motivations behind the commission of online dating frauds, the opportunities that were provided and the technical and social abilities of the perpetrators.The study goes further to assess existing policies formulated towards combating cybercriminal activities in Ghana by interviewing law enforcement agents, lawyers and bankers. The ultimate goal of the study is to uneveil the social and economic motivations behind the commission online crimes which will inturn inform practice and policy decisions. The study's population apart form the ones aforementioned will also include cybercafe owners, cybercafe operators and people who have previously been engaged in cybcercriminal activities. Participants of the study must agree for interview sessions for periods between 30 to 45 minutes.

Benefits/Risks of the study

There are no identifiable risks associated with this project, i.e. physical, social nor psychological. The project rather contributes to theory, research and practice that will be beneficial to cybercrime policy development in Ghana.

Confidentiality

All data collected on and from participants will be only accessible to the researcher. The data collected will be confidential and no name will be attached to a record. Data collected will be stripped off personal identifiers and will be replaced by codes. Data will be saved only on the computer of the researcher.

Compensation

There is no compensation package for participants; there is no cash nor in kind compensation for participating in this research project.

Withdrawal from Study

Participation in this research project is voluntary and participants may withdraw at any time without penalty. There is no adverse effect on any participants who decline to partake in this project.
In the event that information become available that may be relevant to a participant's wiliness to continue participation, the participant will be duly informed and continuance consent obtained before the participant will be allowed to continue participation. Participants can withdraw participation at any point in time and whenever they feel they cannot continue participation.

Contact for Additional Information

For more information, questions and concerns about this research project, and research related injury, please contact the researcher:

Mr. Jonathan Nii Barnor Barnor, University of Ghana Business School, Department of Operations and Management Information systems, Main campus, Box LG 78, University of Ghana, Legon, Accra.

Email: jnbbarnor@st.ug.edu.gh

Mobile Phone Number: +233 24 365 8609

If you have any questions about your rights as a research participant in this study you may contact the Administrator of the Ethics Committee for Humanities, ISSER, University of Ghana at ech@isser.edu.gh / ech@ug.edu.gh or 00233- 303-933-866.

Section C- PARTICIPANT AGREEMENT

"I have read or have had someone read all of the above, asked questions, received answers regarding participation in this study, and am willing to give consent for me to participate in this study. I will not have waived any of my rights by signing this consent form. Upon signing this consent form, I will receive a copy for my personal records."

Name of Participant I.S.K

Signature or mark of Participant

10 November 2020
Date

If participant cannot read and or understand the form themselves, a witness must sign here:

I was present while the benefits, risks and procedures were read to the volunteer. All questions were answered and the volunteer has agreed to take part in the research.

Name of witness

Signature of witness / Mark

Date

I certify that the nature and purpose, the potential benefits, and possible risks associated with participating in this research have been explained to the above individual.

Name of Person who Obtained Consent

Jonathan Nii Barnor Barnor

8th May 2020
Date

Signature of Person Who Obtained Consent

Data collection sign sheet

Date	Pseudonyms/Initials	Sign
18/10/2017	Zack	
06/11/2017	Franklyn	
06/11/2017	John	
06/11/2017	CHRIS	
02/10/2018	Caleb	
2 NOV 18	Noah	
02/11/18	Razak	
15/03/2020	Esmond	

Mr Barnor Jonathan Barnor

Appendix E: Patrick's Experience
Received: 15th September, 2019

I started doing it somewhere around 2005/2006.
I come from a family of 4 who had moved to Accra from Kumasi around 2000. I completed Senior Secondary School in Accra in 2005 after which I started working in an internet café. After working there for a while, I began to realise how the young boys were making money form the whites. I asked them why they were doing that and they told me, it was the money for those who died in the 9/11 disaster. That is to say, the cards that they shopped on were for the dead. I got interested in this because after all, who is guilty for stealing from a dead person?
I remember very well that the first person I asked to teach me was a Nigerian patron of the café I worked in. he walked me through the process for some time and gave me a text documents with a list of sites to generate credit card credentials. I was then set up and ready to start what I was not ready for. But with the availability of the internet and the computers at my disposal as an attendant, I decided to while away time by engaging in the act.
In my first experience, I started chatting with someone in a yahoo Messenger Chatroom randomly. I introduced myself as an African woman seeking a relationship and the person on the other side introduced himself as a white old man seeking also seeking a relationship. He asked me to send him a picture of me. I was not ready at the time, so, I quickly downloaded a picture online and sent it to him. He began laughing at me in the text and pointed it out to me that the picture I had sent was not a single woman. It was a married woman because the woman in the picture was wearing a wedding ring. It did not end there. The person on the other side introduced himself again as Samuel from Cameroon who was also in the same business of finding victims online. We became friends and by the help of Sam, I had become knowledgeable in the act of making friends online.
With the tutorials from my friends, I started making friends on the popular social media platforms available i.e. myspace, Hi5, Facebook, Yahoo Messenger, Kiss.com etc. But one thing that I was doing it that the rest were not doing is that, I use my real identity to make friends with the people and after I have gathered enough information about them, I went through the backdoor with another account (identity) not necessarily to make friend with them but to use them for shipping items to Ghana. I was posing as a mines worker but most of the big shops do not ship to Ghana so I used them (the clients).
Ideally, it took between three to six months to gain the trust of a friend. In my case, most of my clients came to me to verify the legitimacy of the backdoor account so for example, If I'd told her in the backdoor account that I work in a goldmine in Ghana, she will verify the truth of this matter with me in my real account. So, when I tell them that 'yes, there is a goldmine in Ghana like the one she is describing, she then tends to believe the backdoor account". There were instances, where the moves didn't fall through but most of them did.
I then began to shop in the popular shops to them to ship to Ghana for me. For example, one day I was able to shop items worth $4000 but because I could not ship everything through one person (client) so, I shared it among them. But of course with different identities. When the items got here in Ghana, the postal guys began to suspect me. They even threatened to report me but I tipped them and they made me go through. This was a usual practice but this was huge.

Things got bad for me somewhere around 2009. Fraud news in Ghana began to enjoy popularity and for that matter, the shops began to tighten their security holes. The cards I used to generate were no more functional on these shops. While things got worse for me, my friends were really making it big. Some even suggested it was a spiritual matter and for that matter suggested consulting spiritual agents like Mallams but I refused. Instead, I began to intensify my friendship with my real identity. But the difference here is that I aimed at finding relationships with sugar mummies. After all, I saw some of my friends migrate outside of the country to go and start life with their relationships. After getting there, and making some money off them, they run away and leave them. I tried severally for this one too but to no avail.

Prior to starting perpetrating cybercrime, the society within which I lived had a reproving attitude towards cybercrime due to the spirituality associated with it. Many were those who had sacrificed their bodies to make money, others also went as far as Benin to go and look for spiritual backings towards the act. So, I was stigmatised against in my area. Though I was in touch with my friends while I made it, all began to fade gradually.

After rejecting the Mallam appointment, I decided to stop, re-join my church and go back to school. I was an active member at my church before I started the act of cybercrime. It has not been easy but gradually I have incorporated back into society. I have new friends now and a new life for myself. I am currently working with an IT firm in Accra and also doing my masters.

Appendix F: Cassandra Cross' Review of an Output from This Thesis

Barnor, J., Boateng, R., Kolog, E. and Afful-Dadzie, A. (2020)Rationalizing Online Romance Fraud: In the Eyes of the Offender AMCIS 2020 Proceedings 21.

Research examining romance fraud is overwhelmingly based on victim perspectives of this offence. Notably, most studies seek to understand one or more aspects of the factors that contribute to why victims are susceptible; the techniques used by offenders to perpetrate their deception; and the various impacts of romance fraud victimisation in the aftermath of incidents.

However, it is equally important to understand romance fraud from an offender's perspective. This article uses interviews with 10 self-identified romance fraud offenders in Ghana. It combines the motivation-opportunity-ability framework with the rationalisation dimension of the fraud triangle to gain insights into how these offenders understand their actions and the impacts of their offending.

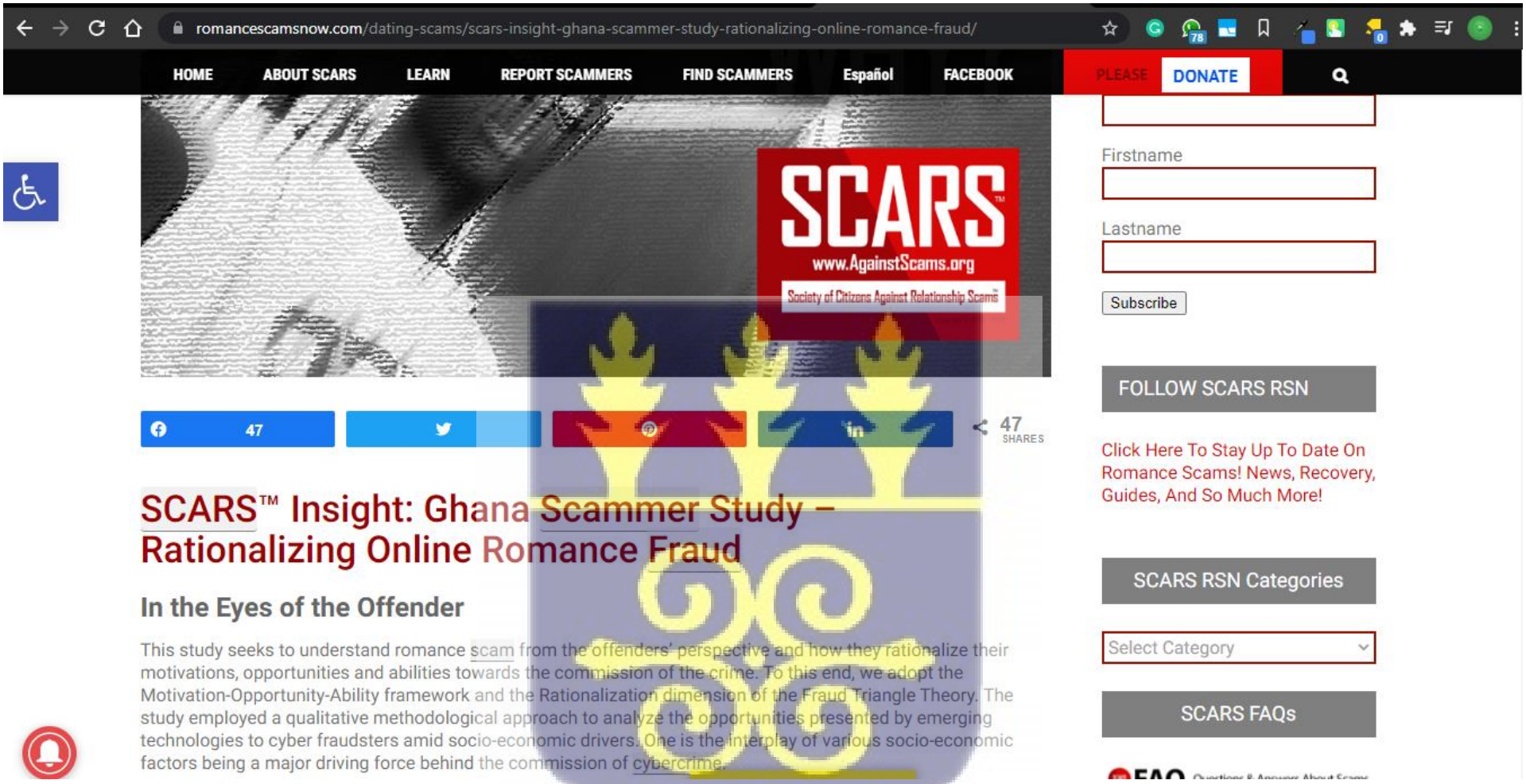
In outlining their results, the authors detail the reasons why offenders partake in romance fraud. One factor stems from their individual need to provide for their families, and high levels of unemployment which restrict their ability to access legitimate job opportunities. There is a plethora of opportunities available to conduct these activities, and a strong belief in the inability of police to be able to catch them. In terms of abilities, offenders note the combination of social and technical skills needed to perpetrate romance fraud, and the allocation of these tasks to individuals as appropriate.

The ability of offenders to rationalise and/or justify their actions is clear. There is a belief that what they are doing is not criminal, and that online offending (as evident in romance fraud) is better than committing violent offences (such as robbery). There is also a belief that victims are greedy, gullible and unintelligent, and that victimisation is justified (particularly against Westerners) in terms of colonial transgressions of the past.

The results of these interviews are challenging to read, having interviewed so many victims whose lives have been devastated by romance fraud. However, it is critical to understand the cultural lens through which romance fraud is perpetrated and the assumptions that underpin both offender and victim behaviours. While it is important to note that romance fraud is a global phenomenon crossing all geographical boundaries, there is arguably a concentration of offenders in West Africa who focus their efforts on romance fraud. The social, economic, political and cultural context of these nations lays the foundations for offenders to engage in romance fraud as a means of making money. One cannot address the root causes of romance fraud without acknowledging this and seeking to address these wider societal issues.

Overall, this article provides important insights into the motivations and justifications of romance fraud offenders as well as some of the logistics involved in their offending behaviour.

Appendix G: A Snapshot of a Publication from this Thesis Used for Public Education



Funding

This research was financially supported by the Carnegie Corporation of New York (CCNY) BANGA Project to the University of Ghana.