Cyberstalking: A content analysis of gender-based offenses committed online

By

Nelufa Ahmed

215080766

Supervisor: Professor Shanta Balgobind Singh

Submitted in agreement for the fulfilment of the requirements for the degree of Master of Social Sciences

School of Applied Human Sciences

Criminology and Forensic Studies Discipline

University of KwaZulu-Natal

2019

DECLARATION

I, Nelufa Ahmed (215080766), declare that the work presented

in this dissertation is my own.

It was never submitted previously to any other university for any other purpose,

be it for a degree or an examination.

The references used and cited have been acknowledged.

Signature of candidate……

Date……..

ACKNOWLEDGEMENTS

Gratitude and appreciation is difficult to express and document. First and Foremost, I would like to thank the Almighty; I am truly blessed for all that has been bestowed on me, for the challenges that I have faced whilst conducting this research and for providing me with strength and courage to persevere and steam ahead with my thesis. Alhamdulillah I have become stronger than I ever have been.

I would like to thank my parents, Shaik Abdul Wahab and Zeenath Bibi Ahmed. They have both sacrificed and assisted me in every aspect of my life, I am grateful to them for the type of person that I am today. My dad, who is my pillar of strength. You will never know how important your existence has been in my life. You have done things far and beyond for your children, more than the fair share of any parent could possibly do. You have been my father, my friend, my mentor, my guide, my protector and even my babysitter. You have always been there to help me pick up the pieces and face the challenges of everything that came my way. You allowed me to accept the things I cannot change and face things in the most optimistic way imaginable. Thank you for being extraordinary.

To my children, Jauhara(15) and Hisham(3), thank you, for being understanding in these trying times of mines, for being kind in my bouts of madness and helping me with trivialities. Jauhara constantly and consistently reminding me of completing my thesis and succeeding. Hisham on having such heartwarming, melting smiles whilst you played and watched me work; without trying to interfere with my laptop. One is my sunshine and the other is my silver lining. You both mean the world to me.

Thank you to my husband, Hasan Moosa, for pushing me to the extremes, for adding to my stress and anxiety, for always testing my limits in all aspects and arrears of life. Thank you for being my love, my friend, my enemy, for giving me loads of life challenges to face and overcome. Thank you for financing me, assisting me and for believing in me in completing my studies. My love for you is like running water; it constantly flows but always runs deep. Thank you for giving us the biggest scare of all. May you remain healthy, if not for us, then for your toddler.

Thank you Brighton. Thank you for assisting me as best as you could. Thank you for giving me headaches and constantly pushing me for time.

Lastly and most importantly, I would like to thank my supervisor, Professor Shanta Balgobind Singh, for guiding, understanding and believing in me. You assisted me in confronting life's challenges and in completion of my thesis. Without your confidence and guidance in me, this research would not have been possible.

ABSTRACT

The 21st century has come up with the increased usage of technology and this has been welcomed by cyber stalkers for it has exacerbated cyberstalking. Cyberstalking therefore has grown considerably within the contemporary environment. Cyberstalking entails the inappropriate, uninvited social exchange behaviours initiated by a perpetrator via online or wireless communication technology and devices. Forms of cyberstalking includes sending threatening or obscene electronic emails, harassing in chat rooms, spamming, tracing another person's computer and internet activity, and posting threatening or harassing messages on blogs or through social media. The study utilised qualitative research methods in which documentary search was utilised as the secondary source of data collection. The study therefore gathered that gender based offences have considerably increased online. The study gathered that women (particularly young women aged 18-24) disproportionately experience severe types of cyber harassment, namely cyberstalking and online sexual harassment. The study also gathered that there are a number of ways which have been documented to deal with cybercrime. Raising awareness, setting up and supporting peer-support networks for the eradicating gender based offences committed online and there is need for industry regulations such as punishment from using twitter and YouTube if found to be offensive. The study also gathered that cyber stalkers are motivated by a number of ways. The first category are those that need to fulfil the psychological needs, wishes, or cravings regarding the victim on the part of the perpetrator and the second category are those motivated by the need to instil fear and gain control over the victim. The third group consists of those cyber stalkers who are motivated with the need to seek revenge or punish the victim. And the last group of cyber stalkers are those motivated by the need to build a relationship with the victim. The study therefore recommends for the need to implement cyber stalking regulations within South Africa for the ones that have been acted are not being efficient in combating cyberstalking.

Table of Contents

LIST OF FIGURES

LIST OF ACRONYMS AND ABBREVIATIONS

ECHO	Electronic Communication Harassment Observation
GPS	Global Positioning System
ISPs	Internet Service Providers
ITU	International Telecommunications Union
PTSD	Post-Traumatic Stress Disorder
SAPS	South African Police Service
UN	United Nations
USDOJ	United States Department of Justice

CHAPTER ONE

INTRODUCTION AND BACKGROUND OF THE STUDY

1.1 Introduction

The 21st century has seen the rapid development, evolution and transformation of cyber technology which has been rampantly advancing across the globe. In other words, the internet is a marvel. Apart from things advancing positively, there has been an emergence of a different type of crime, one that is virtual and conducted in the domain of cyberspace online Lucks (2004: 2). Advancement in technology since the 90's has allowed for a simpler, convenient and effective lifestyle within the comforts of a person's current surrounding. It has become evident that there is an escalation in the number of individuals that use the internet worldwide (Whitty & Johnson, 2009: 1, 11) this has transformed the way people communicate (Shimizu, 2013). In this day and age it is virtually impossible to survive without technology as people have become reliant on it Lucks (2004:13).

Some services that are offered online include but are not limited to:

- Individuals can perform online shopping, marketing and delivery of items;
- Banking institutions offer online services;
- Transactions can be conducted with confirmation of credit card details electronically (King-Ries, 2011).

Life has become virtually convenient and easy with almost everything done electronically. This is because the internet has made everything virtually possible at the convenience of the user. Furthermore, the availability of gadgets and devices such as computers, tablets and mobile gadgets have even made the whole process of accessing the internet easy. Society is transitioning from paper to a digital and individuals are provided with tools that increase creativity, innovations and productivity (Lunker, 2012).

Individuals have access to emails stored on an online server. Applications and tools are constantly being developed and upgraded; certain applications allow individuals to use applications that send and receive information without leaving behind a footprint. This excludes the user information which enables to perpetrator to do this in anonymity as certain privacy laws apply depending on the country (Anderson, 2010). Applications such as Drop box, Google drive, One drive and Cloud was developed to exchange documents, pictures and videos which can be accessed with any device. However these applications are not secure as hackers use their technological skills and access these accounts without consent from the individual.

The internet and social media provide opportunities for individuals to empower themselves in a variety of ways. People maintain social interactions and connections via networking applications such as Facebook, Myspace, Twitter, We chat, Whatsapp and Instagram. The social networking sites have become an integral part of society and everyday communication. It is a cost effective means of instant messaging for individuals that are living both locally and internationally (Lenhart, 2007). It is used as a means to be informed on their family's, friends', colleagues' and co–workers' activities, achievements and places that they have travelled to. Individuals enjoy uploading pictures and writing messages in virtual reality (King-Ries, 2011). As convenient as this means of communication with family and friends as it may be there is a downside to this, this leads to a more sinister type of misdemeanors where individuals harass, threaten, involvement in spamming activities, sending of viruses and flaming which is a form of online verbal abuse (Shimizu, 2013 ; Chik, 2008; Lunker, 2012).

However, the internet has come with some disadvantages. Social decay is the chief effect of widespread use of the internet as cultures are now intertwined, traditional values and ethics are disrupted. Cyber-terrorism, cyber-crime and cyber-stalking are also amongst the defects of a globalized inter-connected environment. It is the latter part of cyberstalking that gives rise to this study. Since people across all walks of life post their life status and the likes, there has been a consistent rise of cyber stalking. It is within this regard that this study seeks to discuss on cyberstalking: a content analysis of gender based offenses committed online.

1.2 Background of the Study

According to the United Nations (2013), there are 2.3 billion people that have internet access. The estimation from this report states that the above figure is total to more than one third of the world's population; further noting that 60% of internet users are from developing countries and by the year 2020 the quantity of networked devices will outnumber people by a ratio of six to 1. In a study conducted by Collin, Rahilly, Richardson & Third (2011) in Australia, it was discovered that social networking services play a positively uplifting role in the lives of individuals. Some of the benefits found in the study include educational outcomes, identity formation, forming supportive relationships and strengthening interpersonal relationships, developing self-esteem and a positive well-being.

As integral and pivotal to society as the internet has become, there is a deeper, darker, illegal side that comes along with it. The internet has also become a tool for illegal activities (Siegel, 2011: 333). Due to the process of globalization, it has become easy for an individual to commit a transnational organized crime and/or a cybercrime. There are various definitions, different forms and types of cybercrimes. Siegel (2011: 334) defines cybercrime as the following:

1. **Cyber theft:** it is the use of online cyber space that is used to distribute and provide illegal services and goods. These include illegal copyright infringements, identity theft, security fraud, pornography and prostitution.

2. **Cyber Vandalism:** is the use of cyber space for the purposes of revenge, destruction, malicious intent and defamation of another individual. Cyber stalking included here.

3. **Cyber Terrorism:** this type of cybercrime is when an enemy tries to destroy secure networks including that on a national or international level.

1.2.1 Cybercrime

Muncie, Talbot and Walters (2010: 77) define cybercrimes under the following categories:

1. **Traditional cybercrimes:** these are criminal behaviours that the justice system is familiar with. This category is still classified as a criminal activity and would still exist out of the realm of the internet. Technology has made ensured the effectiveness of this activity. These crimes included: violent and pornography, dissemination of malicious and hateful material, stalking, bullying.

2. **Hybrid cybercrimes:** similar to traditional crimes as they would exist without the internet however has created new opportunities for criminal activities in cyberspace. These cybercrimes are: fraud, identity fraud, phishing, piracy and distributions of copyrighted materials (songs, films, books).

3. **True cybercrimes:** this category of criminal activity would not exist without the internet. It is contained within cyberspace. These include: hacking, spamming and virtual reality theft that an individual has purchased in real currency.

1.2.2 Cyberstalking

Regardless of the different categories and definitions; the types of cybercrimes are still similar and is rapidly evolving. For the purpose of this research, the researcher intends to focus on one particular type of cybercrime: Cyberstalking. However certain aspects of cyber bullying maybe included in the study as the terms cyberstalking and cyber bullying are synonymously and often used interchangeably in the media. Following is an extract from the lyrics from a popular song that seeks to explain the genesis and impact of cyberstalking.

"*Every breath you take, every move you make,*
Every bond you break, every step you take, I'll be watching you.
Every single day, every word you say,
Every game you play, every night you stay, I'll be watching you.
Oh can't you see, YOU BELONG TO ME…."

The Police

Song Lyrics: Every breath you take.

The above song lyrics was popularized by the music band, The Police in the 90's describes and summarizes the actions of a traditional stalker. The song can be applied to cyber stalking as the perpetrator would be watching and stalking the victim online. Traditional stalking behavior is characterized by a direct physical threat or attack on the victim. The stalker pursues the victim in the following way: verbal and written communication; unsolicited single sided romantic involvement; surveillance; harassment and loitering to an extent that the victim suffers from psychological distress and fear (Boon & Sheridan, 2002: 201).

An article published by the Guardian Online state the British Crime Survey 2006 revealed that there are approximately 5 million people that experience stalking each year (McVeigh, 2011). According to statistics from the Pew Research Centre revealed that 73% of adult internet users have witnessed someone being harassed online and 40% have experienced some form of harassment (Duggan, 2014). Cyberstalking can be defined as an individual fearing for his/her life and safety due to online threats, harassment, privacy invasion, reputation-harming lies, including content and nude photos posted on revenge pornographic sites which publicly shames and humiliates the victim (Quarmby, 2014), the same description above is provided for cyber bullying including the terms cyber aggression, cyber violence, internet harassment and online harassment that is repeatedly inflicted on a specific person or group (Popovac & Leoschut, 2012). However cyber bullying is considered as a violent, harassing, humiliating interaction between children and young adolescents that use any device online. The difference between cyberstalking and cyber bullying to some researchers is the age demographics. Adults may be involved

in cyber bullying on their own volition or proxy (Anderson, 2010; Anon., 2016; Lipton, 2011).

According to the United Nations Broadband Comission for Digital Development (2015) states that: Women who are more active on social media experience cyber violence and cyber hate crime as compared to men. Women between the ages of 18 to 24 are more at risk of gender based violence online. There are seven types of cyberstalking/cyber violence that have been identified:

1. **Hacking:** gaining unauthorised access to computer systems for the purpose of acquiring personal information, altering or slandering the victim (Maat, 2009: 25).

2. **Impersonation:** is used to assume the identity of the victim in order to obtain more personal information regarding the victim, this includes identity theft (Roberts, 2008).

3. **Surveillance/tracking:** to stalk and monitor the victim's activities in real time. Using Global Positioning Systems (GPS) tracking via mobile phones, cameras and specifically developed and designed applications. (Stalking Resource Centre, 2009; Rosenwald, 2004).

4. **Harassment / spamming:** to constantly annoy, threaten and scare the victim, by constantly leaving voice messages or flooding their inbox with emails or messages. The other definition is Hyper-Intimacy, where the perpetrator may try to repeatedly contact the victim via cyber communication with messages of affection or pornographic messages (Welsh & Lavoie, 2012).

5. **Recruitment:** Luring victims online to violent situations. An example would be online dating sites, employment opportunities. It also provides sex offenders with unparalleled access to individuals through the anonymity that is made available to them (Finkelhor, 2014).

6. **Malicious distribution:** of the victim's intimate and private photographs and or videos. The perpetrators may even contact the victim's employers or partners in order to destroy their relationship or have the victim fired from their job (Maat, 2009: 27).

7. **Flaming:** engaging and being involved in verbal abuse and arguments online. The perpetrator may also use offensive language. (Agosto, Forte & Magee, 2012).

Two more can be added to this commonly known as "revenge porn" and "sexting" (UN Broadband Comission for Digital Development, 2015). Revenge porn consists of the following aspects: the intention to commit harm to the victim, the perpetrator is usually an ex-partner or spouse. Revenge porn falls under the category of malicious distribution above however the perpetrator sends out the material to porn sites, chat sites or any social network (Goldsworthy, Crowley, & Raj, 2015). Maple, Shart & Brown (2011) argues that revenge porn has dominated cyberstalking.

1.3 Statement of the Problem

The increased rate of cyberstalking against women has increased in South Africa and the rest of the developing countries. The evolution of internet has come with cyberstalking in which women aged 18-24 have increasingly been affected. According to Goldsworthy et al. (2015), there are increased numbers of females who have reported the phenomenon even though a vast number of cases go unreported. In other words, cyberstalking is difficult to document to a certain degree as individuals are unaware of their legal aspect hence it often goes unreported. Regardless of the overwhelming manifestation that cyberstalking has received over the recent years; cyberstalking still continues to remain a sub group and functions as a mere branch of stalking to the Criminal Justice System. The increasing number of cybercrimes and cyberstalking against women therefore need to be documented so that an enabling policy can be ratified to protect the victims of this crime (Lipton, 2011). This study therefore seeks to analyse the effects of cyberstalking amongst gender lines in South Africa. Furthermore the study seeks to critically analyse the

effectiveness of legislation and its practical application in protecting victims of cyber stalking within South Africa.

1.4 Rationale of the Study

Due to the advancement in technology, societies have seen a growing number of individuals with devices that are easily connected online. This leaves potential victims to cybercrime at risk. This study therefore seeks to analyse gender based offenses committed online. Currently there is a paucity of data in terms of cyberstalking and cyber bullying that is available in South Africa. Victims suffer in silence and are not aware of the laws that are in place to protect them. There is no accurate picture in South Africa with regards to cybercrimes. The 2014/2015 crime statistics report does not indicate any information regarding cybercrimes (South African Police Services, 2015).

This study intends to explore and briefly identify the nature, extent and prevalence of cyberstalking. The study also is significant for it explores and document existing data on cyberstalking victims and the perpetrator characteristics. The study is also significant for it seeks to examine and show how other countries have dealt with cyberstalking and the cyber law legislations.

Furthermore, the intended study will focus on females being the victim of cyberstalking. This study is relevant for it can inform policy development and education awareness programs for organisations, interested stakeholders and the government on how to combat gender based cyberstalking. Furthermore, the study will help organisations, educators, members of society and the Police force in identifying and assisting with issues relating to cybercrimes in South Africa. This study will also contribute to the field of cyber criminology as there is limited research available in South Africa.

1.5 Objectives of the Study

The study seeks to analyse the gender based offenses committed online and how best can these offenses be combatted. The other also seeks amongst the main objective:

- To briefly document the prevalence of cybercrimes.
- To determine on gender based offenses committed online and document the strategies implemented in eradicating gender-based offenses in South Africa.
- To identify the motivations of cyberstalking perpetrators
- To identify any cyber law legislations that has been implemented.

1.6 Research Questions

Main Question

- What is the nature and extent of cybercrimes?

Sub Questions:

- What are the causes of the prevalence of cybercrimes?
- What is the nature of gender-based offences online and how has been this offences combated within South Africa?
- What are the motivations behind a cyber-stalking perpetrator?
- What cyber law legislations have the government implemented?

1.7 Structure of the Dissertation

Chapter 1: Introduction and Background of the Study

The first chapter presents the introduction to the research problem. Furthermore, the chapter discusses on the background of the study first describing on the emergence of cybercrimes, cyberstalking and cyberstalking against women in particular. The chapter also presents the research problem, the rationale of the study, objectives of the study and related research questions. It provides insight on cyber-crimes and aims to acquaint the reader with the research topic.

Chapter 2: Literature Review

The second chapter presents the literature review and theoretical framework underpinning the study. Within the chapter, the overview of cybercrimes, types of cybercrimes and cyber stalking will be presented.

Chapter 3: Theoretical Framework

The theoretical framework is of importance within this study and therefore, the chapter will detail on relevant theories underpinning the study. Amongst these include the Rational Choice theory, Space Transition theory, Lifestyle Exposure theory. The reason why these theories were used is due to the fact that each theory contextualizes different aspects of cyberstalking.

Chapter 4: Research Methods

Within any study, the methodology is of fundamental importance. Chapter three in this regards presents on the research methodology utilized to be utilized within the study. Due to the nature of the study, the study utilizes the qualitative research approach structured by the descriptive research design.

Chapter 5: Research Findings

This chapter will discuss and present the results gathered from the study. The results presented are in line with the objectives of the study and seek to conform to the research problem

Chapter 6: Conclusion and Recommendations

This chapter will present the conclusions gathered from the study. Furthermore, the chapter will present the recommendations on the research problem and also identify areas for future study

1.8 Ethical Considerations

Due to the study being a content analysis of existing data in the public domain, ethical considerations of informed consent, confidentiality, non-maleficence and beneficence do not apply. There are no participants that the researcher will interview. As this is a qualitative study, the researcher need to be aware of bringing the researchers own frame of reference into the study, and the interpretation of the data. The research however was conducted after ethical clearance from the University of KwaZulu-Natal was given. All ethical procedures as prescribed by the university's ethical guidelines were followed to ensure that the study remained strictly within ethical boundaries in its execution and reportage.

1.9 Definition of Key Terms

Cybercrime: According to Verdegem, Teerlinck and Vermote (2015), cybercrime is an "umbrella term to describe different online threats such as mal-ware, scams and hacking." Within this regard, cybercrime is viewed as a criminal act dealing with computers, networks and smartphones. Additionally, cyber-crime is inclusive of traditional crimes conducted with the use of the internet (Blackwell, 2018).

Cyberstalking: Stalking entails the use of the internet and other electronic communication devices to create a criminal level of intimidation, fear or harassment in a target victim(s) (Petrocelli, 2005; Longman dictionary of Contemporary English, 2003: 390).

Cyberspace: is referred to as the "World Wide Web", a virtual reality that is only accessed by computers, mobile devices or any device that has the capability of connecting to the internet (Cambridge Dictionary, n.d).

Gender Based Offenses Committed Online: Crimes committed online influenced by the gender of an individual. According to Pathe (2002), more than 70% of crimes committed online are against women and are committed by men.

GPS: Global Positioning Systems pinpoints a user's location by triangulating the radio signals that were emitted by the device. Satellites are used in pinpointing the

exact location of the person. This allows the cyber stalker to track the victims movements (Stalking Resource Centre, 2009; Rosenwald, 2004).

Social networking site: a communication, sharing platform which allows individuals to interact with each other (Cambridge Dictionary, n.d).

1.9 Conclusion

This chapter introduced the fundamental aspects underpinning the research. Within this regards, this chapter presented on the introduction to the research problem in which an understanding on what cyber-stalking relates to and the genesis of the concept was presented on. The chapter also presented on the research problem on the content analysis of gender based offenses committed online. Research objectives and related research questions were also part and parcel of this study. The rationale for the study, ethical considerations and the definition of key terms were also constituent of this research. The following chapter therefore presents on the literature review underpinning the study.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

Within any study, the literature review is a fundamental component. This is because literature review entails reviewing relevant published texts underpinning the research problem. The importance of such is that it helps define the research problem and also helps identify the research gap. This chapter is purposively structured so that it first discusses on the overview of cybercrime and types of cybercrimes. All this is introductory to a review of what cyberstalking entails, which is the major variable within the study. This chapter therefore reveals literature underpinning cyber stalking, its determinants and how cyberstalking is committed online against women. Due to the dearth of literature on gender based cyberstalking, the chapter will therefore identify literature gaps.

2.2 Cybercrime

The evolution of technology has come about with different changes, both negative and positive. An interesting historical fact to note is that the first reported cyber-crime was in 1820, as India, China and Japan has had access to a computer device since 3500 B.C (Mshangi, Sanga & Nfuka, 2014). During the evolution of technology, there has also come the need to define and understand computer crime and how to tackle it. However, different schools of thought have come forward with their own understanding of cybercrime thus there is no unanimous understanding of the concept. Scholars highlight different characteristics of the concept and also bring about different propositions on how to tackle the phenomenon. Wall (2005) therefore stipulates that this on-going war amongst scholars and lack of a clear cut definition is problematic as it is impacting upon every need of prevention and remediation, while a lot of people are being affected by various types of perceived cybercrime.

According to Parker (1976), the literal definition of cybercrime is that of computer related crimes. In other words, cybercrime entails criminal and detrimental activities that involve the attainment or manipulation of information for personal gain.

Symantec (2012) offers a broad understanding of cybercrime. The notion is defined as crimes involving the use of computer software, network or hardware devices. Kshetri (2010) understands cybercrime from its characteristics and argues that it is the use for computer network on the purposes of committing crimes related to identity theft, spams, hacking or cyber bullying. Within all these definitions, the fundamental notion is that a crime has to be committed online for it to be classified as cybercrime.

Since cybercrimes have affected all societies, governments have defined the concept in their own ways in a bid to counter the phenomenon. The Cybercrime Act 2001 in Australia defines the term cybercrime as crimes that target computer data and systems however different acts apply to different cities (Parliamentary Joint Committee, 2004).

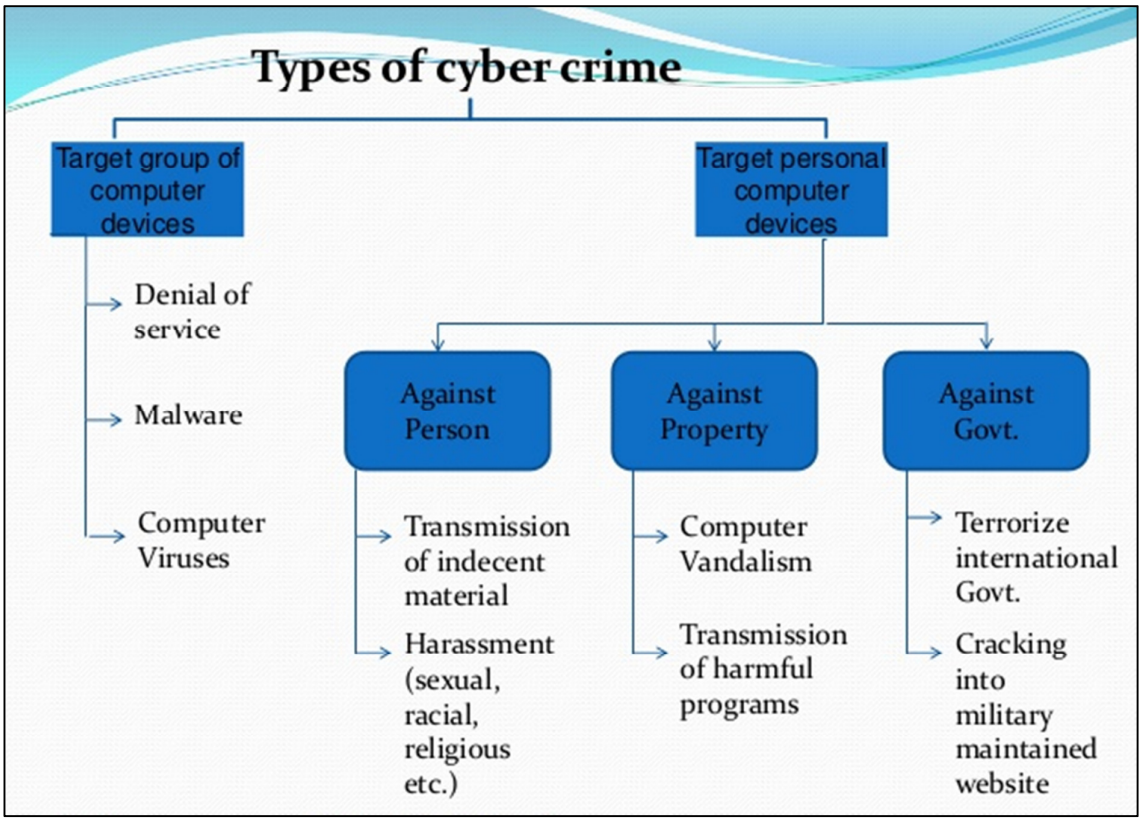
Accordingly, the United Arab Emirates (UAE) Federal Law No 2 of 2006 on The Preventive of Information Technology Crimes define cybercrime as computer related crimes including aspects such as forgery, fraud, money laundering, bullying and others that are a threat to the religion and the society at large (Gulf News, 2012).

The United States of America (USA) Department of Justice (USDOJ, 1999) further defines cybercrime as computer crimes that include viruses, worms and other facets that infringe on the proper use for network systems. It is imperative to note that the definition of cybercrimes is interpreted differently according to that specific country. However, this study adopts the understanding of cybercrimes as including crimes involving the computer and internet.

2.2.1 Types of Cybercrime

In a bid to understand cybercrime and effectively come up with ways to combat this ever-widening criminal activity, there is need to understand the types or categories of cybercrime. Figure 2.1 presents on the types of cybercrime

Figure 2.1: Displays the different types of cyber crime



(Source: Telecommunication Development Sector, 2012)

- **Phishing**

The major type of cybercrime is phishing. Wall (2005) defines this cybercrime as an act of attempting to trick people into disclosing of their security information in the form of card numbers, bank details amongst others through masquerading as a trustworthy business online. Jahankhani, Nemrat & Hosseinian-Far (2014) argues that these messages sent online may ask recipients to either confirm or validate their account information. Generally, phishing goes two ways: first there is a stolen identity of the company requiring information from respondents and then the stealing of personal and confidential information from clients. The term phishing originates from the fact that Internet scammers are using progressively sophisticated lures as they “fish” for user’s financial information and password data related to these aspects

(Wall, 2005). In some cases the phishing message appears from a familiar or known recipient which enables it to be more effective (Roberts, 2008). This crime often works through the following procedures:

- Setting up a mirror image of a real web site
- Sending out a convincingly fake e-mail, luring the users to that mimic site
- Obtaining the required information thereafter redirecting users to the real site

There have been a relatively steady number of phishing cases reported however; in 2014 the United Nations reported a 12% decrease in cybercrimes related to phishing (Jahankhani et. al. 2014). According to the State of the Phish Report (2019), published by Wombat Security, 59% of an estimated 5.5 million reported emails were classified as suspicious phishing emails. Regularly these phishing sites are from a popular and familiar company, example Microsoft or UK Lottery.

- **Spam**

Another form of cybercrime is spam which is a product of the Internet's ability to place unprecedented power into the hands of a single person (Symantec, 2012). Spam measures come in the form of advertisements or investment schemes which are fraudulent. Usually sent via mail, the main purpose of spam is to offer a reduced investment deal or price to the customer whom in turn the spammer asks for money or confidential security numbers. According to Kaspersky (2012), after disclosing personal information, the customer will never hear from the spammer again.

- **Hacking**

The most popular cybercriminal activity is hacking. Yar (2006) defines hacking as unauthorized access into another user's computer system for particular items. Yar (2006) further explains that hacking is just the same as traditional robbery in which the robber will find all the relevant information of the target before carrying on with their work. This is just the same as hacking in which the hacker gathers relevant information, scans and finally enters into the hole and hack into personal computers. Hacking is often one method that a perpetrator uses in order to execute the next step, Identity theft (Roberts, 2008). Hugo Cornwell published a book in 1985 name

“The Hackers Handbook”, he is a self-proclaimed hacker and asserts that a hackers only crime is his curiosity (Maat, 2009).

- **Identity Theft**

The fastest growing cybercrime around the developed and the developing world is identity theft. Jahankhani et. al. (2014) argues that identity theft occurs when a person obtains private information about another individual without their knowledge and uses this information to carry out fraud or theft. Generally, company databases have been hacked by criminals who then impersonate their victims (Roberts, 2008). The reason why there are alarming rates of identity theft can be attributed to the ever-increasing and evolving methods of obtaining and utilizing personal information.

- **Ransomware**

According to Yar (2006), ransomware is also another form of cybercrime. “Ransomware is a subset of crime ware that in most cases infects a victim's computer via phishing attacks. Upon successful infection, the ransomware commonly encrypts the victim's data. The perpetrator then demands a ransom payment in exchange for the safe return of their data. There's no guarantee victims will ever receive data back. There has been a decrease in this type of cybercrime. The State of the Phish Report (2019) has reported that 10% of respondents had experienced ransomware attacks in 2018 worldwide.

- **Malware**

Another form of cybercrime is malware. Accordingly, malware takes on many different forms. Some are designed to specifically target users' financial information by installing key loggers onto victims' computers (Kaspersky, 2012). Malware samples are spread to users in a variety of delivery methods, including phishing attacks and malicious software packages that exploit unpatched software vulnerabilities. Once installed, attackers can use the malware to spy on online activities, steal personal and financial information or hack into other systems. Malware is one of the leading online threats and it’s been used in some of the world’s largest cyber-attacks including Cryptlocker, NotPetya and WannaCry.

2.3 Cyberstalking

The rapid increase in the use of the internet has brought about with it a new breed of individuals known as cyber stalkers. Generally, a cyber-stalker is that individual who uses the internet as a tool to intimidate, threaten, harass, and generate fear upon their victims through stalking tactics (McFarlane & Bocij, 2003). It is evident that the use of internet via any connected device is the prerequisite to cyberstalking (DreBing, Bailer, Anders, Wagner & Gallas, 2012). A question therefore arises, what is cyberstalking?

There is no generally accepted definition of cyberstalking as the phenomenon relatively lacks detailed knowledge. Most studies and laws have detailed on cybercrimes in detail, with a little focus on its categories. Mustaine and Tewksbury (1999) therefore laments that lack of the precise definition of this concept has often made it difficult to document and structure the behaviour of cyber stalkers. Petrocelli (2005) argues that cyberstalking entails the use of the internet and other electronic communication devices to create a criminal level of intimidation, fear or harassment in a target victim(s). This study concurs that there is relatively dearth information on the whole concept of cyberstalking but there is a general understanding that the phenomenon that the behaviour of the perpetrators of this crime vary from non-threatening emails and texts to a potentially deadly encounter between the perpetrator and the victim (Hutton & Haantz, 2003).

Hutton and Haantz (2003) are of the view that in trying to determine what cyberstalking entails, there is need to study the behaviour of cyber stalkers. Cyber stalkers primarily rely on the internet and other electronic related devices to threaten, intimidate and harass intended targeted victims. Therefore, the first characteristics of cyberstalking are the use of internet and the methods of cyberstalking include threats and intimidation (Petrocelli, 2005). Furthermore, cyber stalkers have inherent behaviour tendencies which are premeditated, repetitive and aggressive and they are illegal. This kind of behaviour is regarded as illegal under statutory and constitutional law in many countries, rendering cyberstalking, illegal (Hutton & Haantz, 2003). However according to King-Ries (2011) law enforcement

investigators are not trained and equipped with the necessary skills. Within this regard, cyberstalking is a criminal offence motivated by interpersonal hostility and aggressive behaviours stemming from power and control issues.

Campbell (2005) asserts that the whole notion of cyber harassment has often used cyberstalking and cyber bullying as interchangeable terms; Roberts (2008) is of the same view as there is no clear definition for these terms. In defining cyberstalking and cyber bullying, Campbell (2005) argues that three distinct characteristics of stalking behaviour helps determine the impact and understanding of the concept. The first one is hyper-intimacy. Spitzberg, Marshall and Cupach (2001) are of the view that aspects of hyper-intimacy include repeated, unsolicited efforts by the perpetrator at cyber communication with the victim. This aspect therefore is characterised by sending messages of affection, obsessive behaviour and at times sending explicit messages (Spitzberg *et al.,* 2001; Welsh & Lavoie, 2012). The other form of cyberstalking is threats which in this regard includes invasion of privacy through emails, messages and other forms of electronic sabotage. The last characteristic is real-life transfer in which the initial contact was through online contact but it would evolve to physical intrusions (Spitzberg *et al.,* 2001).

Cyberstalking can be defined as an individual fearing for his/her life and safety due to online threats, harassment, privacy invasion, reputation-harming lies, including content and nude photos posted on revenge pornographic sites which publicly shames and humiliates the victim (Quarmby, 2014). The same description is provided for cyber bullying including the terms cyber aggression, cyber violence, internet harassment and online harassment that is repeatedly inflicted on a specific person or group (Popovac & Leoschut, 2012). However cyber bullying is considered as a violent, harassing, humiliating interaction between children and young adolescents that use any device online. The difference between cyberstalking and cyber bullying to some researchers is the age demographics. Adults may be involved in cyber bullying on their own volition or proxy.

Suarez (2014) argues that cyber stalkers utilize a number of tools to perpetrate on this crime. Amongst the tools include Global Positioning systems (GPS), cellphone monitoring chips, spyware computer programmes and tracking devices to the locations, activities and communications of their victims that are unwanted (DreBing et. al. 2012; King-Ries, 2011). At the disposal of cyber stalkers is also the use of technologies such as social-networking, chat rooms, e-mail and mobile phones (Lenhart, 2009). Suarez (2014) and Bocij (2004) both argue that both traditional and cyber stalkers have one desired intention, that is to accomplish having control and power over a victims through all means necessary.

Cyber-harassment or bullying or stalking according to Wall (2005) “is the use of electronic information and communication devices such as e-mail, instant messaging, text messages, blogs, mobile phones, pagers, instant messages and defamatory websites to bully or otherwise harass an individual or group through personal attacks or other means.” Cyber-bullying and stalking according to Early (2010), comes in the form of , “taunts, insults and harassment over the Internet or text messages sent from mobile phones” and this phenomenon has become widespread among young generation, in some cases with tragic disastrous consequences.

In understanding the concept of cyberstalking, the academic community has come with different types of cyber stalkers. Eterovic-Soric, Choo, Ashman, & Mubarak (2017) present that cyber stalkers can be placed into three categories. The first group is those that are influenced by simple obsession. These have a prior relationship with the victim, mostly being a co-worker, ex-lover or ex-spouse. The second group of cyber stalkers are those that are love obsessional driven by the belief that contact with the victim will lead to a love involvement of some sought (Eterovic-Soric et al, 2017). The last group of stalkers are erotomanic stalkers who in the same sense with obsessional stalkers are motivated by love but however the difference between the groups is that; these stalkers are deluded to think the victim is in love with them. Generally, the erotomanic stalker is likely to be female as different to other two categories.

Mullen (2018) is of the view that cyber stalkers can be classified into non-mutually exclusive categories based on their motivations. Mullen (2018) therefore stipulates that the categories rank from those that are rejected by the victim, those that seeking intimacy, those that incompetent, those that are influenced by resentfulness and those that are predatory. Basically, this typology of cyberstalking approaches the categorisation of stalkers from a psychological perspective and is intended for use in treatment of the stalker.

Mohandie, Meloy, McGowan & Williams (2006) argues that since the internet has exacerbated the issue of cyberstalking, the RECON (Relationship and Context-Based) typology can be utilised to understand the motivation of cyber stalkers. This typology categorises cyberstalking based on the context of stalking and the relationship between the victim and the stalker. If these two have had any prior relationship, these can be understood as either intimacy or acquaintance and cases in which the two have no prior relationship in one of “Public figure” and “Private stranger” (Mohandie et al., 2006). Mullen (2018) further asserts that this typology therefore addresses some concerns with the typology as proposed and developed by Eterovic-Soric et al. (2017) on aspects such as observation of stalkers transitioning from the Love Obsessional category to the Erotomanic category.

2.3.1 Online Cyberstalking vs. Traditional Offline Stalking

There is need to distinguish between online cyber stalking vs. traditional offline cyber stalking, for a clear and precise appreciation of cyberstalking and its characteristics in the modern society. Petherick (2007) argues that cyberstalking relatively is an extension of the traditional mode of stalking where the perpetrator utilises a set of skills in committing the offence. Generally, cyberstalking behaviours are more of the same with traditional stalking behaviours though the former represents a comprehensive new form of deviant, criminal behaviour (Bocij & McFarlane, 2002). Within these types of stalking, what is inherent is that offenders intend to harass, threaten in some cases and intimidate the victims. Furthermore, Bocij (2005) further states that both these stalkers have the same reaction when they are confronted,

scorned, rejected or belittled by a victim that is an aggressive reaction. The only difference within these stalkers is that cyber stalkers are more are white collar and established members of the community whereas traditional stalkers are conventional criminal offenders from all walks of life (Bocij, 2005).

Hutton and Haantz (2003) argue that the similarity between a traditional stalker and a cyber-stalker is that both these perpetrators are driven by the desire to have power, control and influence over their victim. Even though law enforcement agents believe cyber stalking to be harmless, if left unattended, this crime has the potential, just as the traditional stalking crime to lead to physical confrontation between the offender and the victim. However, Bocij (2005) argues that the traditional stalker has an intimate relationship or prior relationship with their victims and this is a distinctive feature with a cyber-stalker who chooses their victims at random.

As far back as the 90's, it was reported that nearly 50% of all cyberstalking incidents involved complete strangers who were initially contacted in some perceivably innocent manner via the Internet. What a cyber-stalker needs is a computer or internet connection therefore the geographical proximity is not of effect. There are cases in which cyberstalking is reported from people who live in different countries (Reno, 1999). In the case of Gary Dellapenta, the victim had repeatedly rejected him and he turned to social media. This case is off utmost importance as the above person was the first person in history to be charged with cyberstalking. California was the first state to ban cyberstalking or stalking with any electronic communications in 1999 (History, 2019).

Cyberstalking however has drastically changed from the conventional traditional stalking means. The reason for this is that traditional stalking is easy and effortless at times for law enforcement agents to solve. Bocij and McFarlane (2002) argue that perpetrators of traditional stalking follow their victims from work, school, shopping malls and other related areas in which they leave a signature which is easy to track. Furthermore, there cases where traditional stalkers leave notes or threatening messages that are easy for law enforcement to analyse and apprehend the offender. However, this is different when it comes to cyberstalking.

Bocij (2005) is of the view that people search website such as Google, host a plethora of sites that promote revenge and retaliation, which is always a welcome harbour for cyber stalkers. An example of this is that cyber stalkers often send anonymous emails and messages through websites such as Payback, a page which also hides the sender's details. Bocij (2005) further highlights that there a numerous radical sites which cyber stalkers utilise, such as the Avenger's web page which encourages visitors to seek revenge, and in some cases, incite violence.

2.3.2 The distinction between Stalking and Cyberstalking

Baum, Catalano, Rand & Rose (2009) and Spitzberg & Cupach, (2007) assert that in majority of stalking cases reported, the stalker and victim had shared a certain degree of acquaintance. As stated prior, a victim and a cyber stalker does not need to be within close proximity. Social networking sites are the ideal places to find information online about their victim, or even to post harassing pictures and messages (Singh, 2008). According to the Stalking Resource Centre (2009), stalkers obtained information from cyberspace and social networking sites; not all stalkers may never engage in physical stalking behaviour outside the boundaries of cyber space, therefore cyberstalking should not be regarded as an extension to stalking (Sissing, 2016).

The main differentiation between stalking and cyberstalking are the main methods used by perpetrators of these crimes. From the definitions stated above of stalking vs. cyberstalking, it was established that the former represents a form of harassment in close and physical proximity of the victim whereas the latter entails victimisation through the use of technological and computer related systems. The downfall of cyberstalking is that there are no restrictions and boundaries in terms of cyberstalking a victim.

Reyns (2010:16) is of the view that there are focal determinants that distinguish between stalking and cyberstalking. One way towards a clear understanding of the difference between these crimes, one has to understand it from that specific country, as different government's legislations define the concept differently. Sissing (2016)

stipulates that within the United States (US) for example, uses the American case studies where different states that have both the cyberstalking legislation, apart from the traditional physical stalking legislation. There is therefore the need to investigate cyberstalking as a phenomenon in its own right not as an extension of stalking as there are current gaps in the research and literature regarding the different types of cybercrime and most importantly cyberstalking.

2.3.3 Behaviours linked to Cyberstalking

The study highlighted that there is dearth of information allied with the concept of cyberstalking meaning that there is little information documented on the behaviours of cyber stalkers. However, from the common publications, this section details on the behaviours of cyber stalkers for understanding the behaviours of these perpetrators helps craft policies and initiatives that counter the crime.

- **Sending consistent undesirable communications**

Mullen, Pathe & Purcell (2009) is of the view that the sending of repetitive unwanted messages is one of the methods utilised by cyber stalkers. Applications on social networks such as Twitter, Facebook, Whatsapp, Instagram have created virtual communities that allow people to share a plethora of information about their daily lives and activities (Lenhart, 2007). Cyber stalkers overload a victim's inboxes on any type of networking site with unwanted and at times provocative messages.

A more traditional way is the flooding of emails in which victims become overwhelmed to use those services (Mullen *et al*, 2009). Miller and Morris (2012) argue that this type of method is utilised by cyber stalkers who have a competency in technological services. The use of social network systems is mostly utilised by cyber stalkers because it is relatively cheap and perpetrators can utilise fake accounts and names so that their true identity is concealed. Other websites such as "The Payback" are some websites utilised for it protects the perpetrators name and contact information.

- **Terrorising and Intimidating**

Another form of behaviour exhibited by perpetrators of cyberstalking is consistently making threats. These threats can be made against the victim's family, friends and colleagues (Bocij, 2004:12). All social network platforms in recent days are utilised to make threats. There are cases where victims have received offensive threats with improper materials or pornographic materials attached. Mullen *et al.* (2009) argues that the advent of technology which helps conceal the identity of cyber stalkers has made it easy for them to attach such files and make consistent threats towards their victims. As stipulated by Pittaro (2011:282), cyber stalkers aspire to create and cause constant distress for the victim through a variety of intimidating and threatening behaviours.

- **Spreading fabricated allegations**

Another form of cyber stalking behaviour is through the spread of false information and accusations about the victim. Bocij (2004) identifies a number of cases where cyber stalkers have even contacted the family, friends and colleagues of the victim with false information. All this is intended to cause harm and humiliation towards their victim.

- **Impersonating the victim**

Another behaviour associated with cyber stalkers is that they can attempt to impersonate the victim through various social networks. Bocij (2004) argues that the rationale of doing this by the cyber stalker is to gather information on the victim, embarrass the victim and further encourage other people to participate in the abuse. Bocij (2004) attaches an example of a situation where the cyber stalker will enter a chat room, Facebook group and the likes using the identity of the victim and post degrading invitations to the audience. There have been cases also of identity theft through impersonating the victim.

- **Distributing Private/ Embarrassing Information**

As established within the study on cybercrime and perpetrators of such crimes, these perpetrators are often close people to their victim. Within this regard, the behavior of publishing embarrassing information is often associated with stalkers who act in

revenge. This is enhanced through circulating emails, pictures, videos and even establishing websites containing the private information of victims (Mullen *et al.,* 2009). The recent case of the South African Home Affairs Minister Mr Malusi Gigaba and the distribution of the video of his indiscretion can be utilized as a case study.

- **Identity Theft**

Identity theft is also another form of behavior associated with perpetrators of cyberstalking. According to Willard (2006), to bring humiliation, grief and stress towards the victim, accounts can be created online that are used to order merchandise and services on behalf of the victim. An example of identity theft is that of Australian businessman Tim Beban and Andrew Meagher, that had ringleader Klaara Kodu use their stolen information to purchase goods for resale purposes worth $17 000(A current affair, 2019). The perpetrator has admitted to the crime however no charge has been laid as there is no clear current law to curb this type of crime. This behavior is different from the usual identity theft due to reasons of cyberstalking. For example, traditional identity theft is all about monetary gain whereas identity theft under cyberstalking frameworks is more related to cause grief and humiliation towards the victim.

Thomas (2019) published an article online about cyberstalking victim Alexis Moore. As far back as 2004 law enforcement ridiculed her and did not take her seriously when she complained of a physical and cyber stalker. An ex-partner of hers had stolen her identity and went about humiliating her and causing grief and destruction. The perpetrator had displayed the traits listed below.

2.3.4 Profiling a Cyber Stalker

There has been a general elusion on the classification of cyber stalkers, even though there has been extensive research on the traits and characteristics of stalkers in general. Bocij (2005) argues that the normal stalkers that have been characterised around the globe include obsessive, psychotic, non-domestic or domestic stalkers. Since there is no original study that describes the characteristics of a stalker, this study therefore utilise elements that can be taken out from the general definition of cyber stalkers. Anonymity is regarded as the attribute of cyber stalkers as this act is

conducted in a private manner (Willard, 2006). Therefore, cyber stalkers are criminals who are detached from societal norms and ethics and are unable to deal with reality. These stalkers therefore are paranoid and self-absorbed in themselves.

Lucks (2014: 36) argue that cyber stalkers use the internet and related technologies to perfect their wildest fantasises and deviant behaviours. The goal is to gain power through manipulation, exploiting and trapping their prey. Smoker and March (2017) and Spitzberg and Cupach (2007) are of the view that some offenders experience rejection and seek revenge on the character of the victim through threats and harassment. Bocij (2005) argues that the whole notion of stalking comes from the feeling of being wronged thus cyber stalkers engage in a process of damaging, destructive and detrimental restoration. These stalkers therefore cause havoc whenever the opportunity presents itself.

Due to the nature of the digital world, the cyber stalker operates in a virtual office, with the potential of causing harm to victims far away from them geographically (Spitzberg *et al.,* 2001). Lucks (2014) argue that the more far away the perpetrator is from the victim, the more efficient they are for they feel comfortable physically distanced from their victims so that they cannot get attached by the harm they cause. Therefore, aspects such as violence, abnormal fantasy and aggression are encouraged and practised within the cyber reality. In the context of virtual cyber reality, aspects of aggression and abnormal behaviour are not condoned within this world thereby giving a growing concern of ever combating this crime. Lucks (2014) further mentions that anonymity plays a major role in the commission of cyberstalking as the cyber stalker has the ability to avoid detection – fuelling their destructive behaviour.

This study therefore utilises the classification of cyber stalkers as presented by Bocij and McFarlane (2005). The first category comprises of vindictive cyber stalkers. Within this category, threats, harassment and even violence are key methods, as vindictive stalkers are malicious and spiteful. The second category is that of composed cyber stalkers who prioritise on making the life of the victim difficult. Bocij and McFarlane (2005) also identify the third category of cyber stalkers as including

obsessive and infatuation behaviour with their victims, a group known as intimate cyber stalkers. Lastly, the collective cyber stalker operates in such a way that there is more than one individual cyber stalker. It often includes two or more offenders stalking one individual Bocij and McFarlane, 2005).

2.3.5 Reasons why Cyber Stalking is Difficult to Document

As established within the study, cyberstalking lacks a precise understanding and effective counter measures because there is dearth of information about the phenomenon. This is partly caused by the fact that cyberstalking is difficult to document. Following, are the reasons why cyberstalking is difficult to document

2.3.5.1 Nature and Extent of Stalking

Jenkins (2015) argues that within societies, there have been few if not at all, studies measuring on the extent and nature of stalking. In a study conducted by the U.S Bureau of Justice Statistics in 2010 as reported by Jenkins (2015), it was discovered that current trends and evidence suggest that cyberstalking has become a serious issue that will grow in scope and complexity as more people take advantage of the internet and other telecommunications technologies. This has lived to be fulfilled in present times as cyberstalking is increasing in frequency and most countries are still struggling on the reality of this crime and how it can be stopped. Cyberstalking according to Jenkins (2015) therefore comes in the form of unwanted phone calls, sending unwanted letters and emails, spying on the victim, posting information or spreading rumours about someone on the internet amongst other forms (King-Ries, 2011; Anderson, 2010; Ghasem, Frommholz & Maple, 2015). However, these forms are far too conclusive in determining cybercrime and these actions are difficult to comprehend due to the complex nature of the internet.

2.3.5.2 Digital Society

Another reason why cyberstalking is difficult to document is the increasing nature of a digitalised society. Generally, a digitalised society therefore means that it is easy to monitor and gather information about certain individuals or persons of interest. It is generally easy therefore for a cyber-stalker to gather all the relevant information on

their victim for all the general information is easily accessible on the internet. Individuals freely divulge information. Thompson (2014) argues that there is an increasing number of mobile phones equipped with GPS, the stalker can use the easily accessible tools such as Foursquare, Google Buzz and SnapChat to determine the exact location of their victim and track whatever they are doing. Currently SnapChat uses a bitmoji (which is the actual replica of the individual but in animation form). This bitmoji is created by the user and enables other users to see their exact location. Facebook and Instagram have sections that allow the user to "check inn" to their current location which is then displayed for followers/ friends to see. Cyberstalking is linked to the popularity of some of the social media sites listed above (Hill, 2010).

The increasing number of offline trade has also exacerbated cyberstalking. Today, one can shop online, make travel plans amongst other things. A cyber stalker can therefore keep track of every financial transaction, every correspondence, and every website visited by their victim. In a case study in South Africa in 2015, one particular lady told the courts that the ex-husband who had been stalking her online, he had produced her travel documents, plans and all her activities showing the potential capability of harming her, despite residing in a different province (Thompson, 2014). Therefore, the digital nature of society has made cyberstalking difficult to document.

2.4 Cyberstalking from a South African Perspective

Cyberstalking is a phenomenon that has affected both developed and developing societies. South Africa is one of those communities in which there have been an increasing number of cases of cyberstalking. Pretoria News (2015) is of the view that South African statistics about the phenomenon are a bit patchy for studies have been few and beyond on this crime. However, the enactment of the Protection from Harassment Act which came into effect in 2013, stipulates that authorities have taken the emergence of this crime seriously. The law generally stipulates that if an individual is being relentlessly targeted with abuse on social media or via email, that particular individual can apply for a protection order under the provisions of the act.

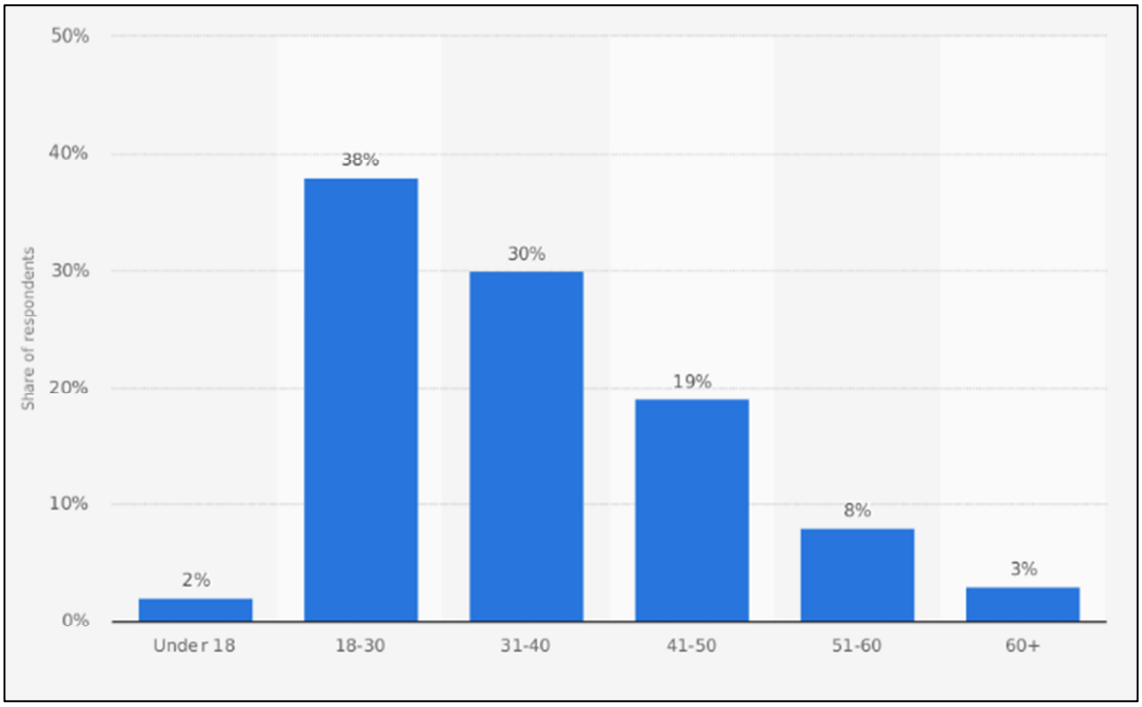
Generally, the protection from Harassment Act provides civil remedy for cases of cyber harassment and provides recourse for both domestic and non-domestic relationships. Section 1 of the Act defines harassment as broadly including cyberstalking and any other related electronic information that maybe be harmful. This Act specifically target cyber stalkers, which were previously eluded from prosecution under the 1999 Domestic Violence Act. Amongst the provisions of the Act includes aspects such as lodging a complaint against being cyber harassed, and to obtain the credible evidence that can be used to identify the offender. Ideally, Section 4 of the Act stipulates that Internet Service Providers (ISPs) to help law enforcement agencies by providing the relevant information to identify offenders within five days of the request. Section 4 (6) of the Act obliges the ISPs to inform the offender that information about their identity has been passed to relevant authorities. Generally, this Act has been welcomed as it has certainly eased the burden of proof placed on the complainant.

Accordingly, Section 5 of the Act stipulates that gives a court the mandate to investigate and acquire the relevant information of the perpetrator. Conversely, Section 6 of the Act empowers the South African Police Service (SAPS) to help in tracking down the offender and for the laying of formal charges. The Act therefore seeks to prove that the perpetrator by their actions ought to know that their actions would cause harm to the complainant. Manyame (2018) argues that this makes it easier for the accuser to prove non-patrimonial maltreatment, such as pain and suffering, which are usually difficult to prove in harassment matters. Therefore, the victim must establish that the communication caused an extent of psychological impairments such as fear of bodily harm to person, property or serious mental anguish. Finally, an objective harm must reasonably arise from the circumstances. Manyame (2018) argues that even though the legislative arm of the South African has done so well in combating cyber harassment even through there is need for constant ratification of this Act due to changes in the digital sphere.

2.4.1 Victims of Cyberstalking

According to Manyame (2018), there are different ways in which perpetrators of cyberstalking identify their victims from. Generally, there similarities between the victims of online stalking and those from traditional stalking, and these will be utilised to generate themes on broad categories of victims of cyberstalking within South Africa. The following figure presents on the general overview of the age relations of victims of cyber stalking within the South African perspective

Figure 2.2 Victims of Cyberstalking by Age in South Africa



(Source: Statistica Research Department, 2013)

Figure 2.2 presents on the proportion of victims of cyberstalking within South Africa. The higher proportionate is that between the ages of 18-30 years followed by those between 31-40 years. Within this regard, Manyame (2018) therefore analysed cases of cyberstalking and gathered the following precepts as victims of cyberstalking.

2.4.1.1 Ex-Partners

As established from the characteristics of cyber stalkers, rejection and denial often stems up to cause this crime. Generally, there is no one best suited for that crime other than previous partners. This form of cyberstalking therefore comes from a break up in relationship. Manyame (2018) is of the view that signs of harassment often show when the relationship is starting to be dysfunctional and aspects such as jealousy, loss of control and intrusiveness starts to show. Since previous partners often have in their possession personal information of their ex-partners, stalking is often made easy. Lucks (2014: 36) argue that stalking comes in form of repeated and excessive phone calls, e-mails and text messages that are threatening. All these can be attributed to cyberstalking from previous partners. The South African Domestic Violence Act however addresses this crime in effect. According to Electronic Communication Harassment Observation (ECHO) (2011), an analysis of the study that was conducted only revealed that 11% of cyber stalkers were ex-partners and 18% was a previously dated ex, which totals 29% in this category.

2.4.1.2 Casual associates and friends

Victims of cyberstalking are also prone to be stalked by their friends or acquaintances. Generally, the victim is identified when they have had some sort of social and interactive encounter with the cyber stalker as either acquaintances or friends. In most cases, victims may get the attention of the cyber stalker due to an interaction they may have engaged into. The cyber stalker therefore would feel that maybe there has been a connection between them and the victim. According to a study conducted by Electronic Communication Harassment Observation (ECHO) (2011), it was gathered that apart from cyberstalking from loved ones, this is the most common form of stalking as the cyber stalker would have felt affection for their victim, and feel that this affection is not mutual. Therefore, Sissing (2013) argues that mostly, the other kind of cyber stalker may feel that their affections are not returned and may therefore resorts to cyber harassment. ECHO (2011) reveals that 25% of cyber stalkers fall under this category.

2.4.1.3 Work colleagues

The phenomenon of cyberstalking is also not limited to office mates, but also includes customers and clients (Sissing, 2013). Manyame (2018) argues that this form of stalking often comes from resentment, jealousy and rejection. Within the work environment for example, the offender closely monitors the work performance of their victim so that empowers them create victimization against that individual. In most cases, a victim has either been fired, suspended or fined for an offence that they have not committed.

Sissing (2013) stipulates that there are different types of stalking that may arise within the workplace setting. Amongst these include cyberstalking intruding into the workplace from victimization outside work. In most cases, the victim may even lose their job as the stalker will ensure that they attack on the work credibility. Another form of cyberstalking that occurs in the work context includes that of clients stalking staff. Upon their meeting with the staff, Manyame (2018) argues that there may arise a form of interaction that topples the mind of the cyber stalker. Within the frameworks of cyberstalking that ensues within the workplace, another form is of clients stalking clients and lastly that of staff stalking co-workers. ECHO (2011), has revealed that work colleagues fall under 6% in this category.

2.4.1.4 Strangers

The study established on the definition of cyberstalking that some offenders are satisfied when they are victimizing strangers. Therefore, strangers are also a potential target of cyberstalking. Victims therefore have no previous engagement with their stalker (Sissing, 2013). Victims are usually targeted based on their social status or attractiveness. Ideally, a stalker generally is an online stranger and they may be anonymous and solicit involvement of other people online who do not even know the target. Pitarro (2011: 280) therefore states that there has been an surge in the number of cyberstalking cases perpetrated by strangers, as the Internet permits cyber stalkers access to a relatively large amount of personal information whilst still concealing the cyber stalkers identity. Strangers were classified as 22% by ECHO (2011).

2.4.1.5 Celebrities

Generally, celebrities due to the nature of their work and their popularity are victims of cyberstalking. Celebrities in all walks of life including politicians, sportsperson, actors, singers and the likes are targeted due to their fame. These victims are tormented by cyber stalkers who have intimacy and psychologically obsessive issues which results in dangers such as threats, defamation and incessant harassment (Sissing, 2013). Ideally, stalking of celebrities is as old as the concept of celebrities itself. In 1980, for example, fervent Beatles fan Mark David Chapman who shot John Lennon dead on the outside of his Manhattan apartment building. This is not the only case as there has been a surge in the number of malicious threats and texts that have been forwarded to celebrities demanding that they either stop with their career or they will face ultimate death.

To name a few of this celebrities are: Sandra Bullock, Miley Cyrus, Taylor Swift, Madonna and Catherine Zeta-Jones. This has resulted in some celebrities petrified to even conduct their day-to-day businesses. These stalkers had access to their social media pages hence most of them had identified how to know the location and whereabouts of their intended victim. According to Watt and Mclean (2012), the Internet makes it easier with Youtube, Twitter and Instagram which leaves behind a location tag; and because the cyber stalkers believe that the celebrities are actually talking directly to them. Stalkers therefore think that they have a relationship, and there's a lot more information out there about the victim thus ensuring cyberstalking. Cramer (2014) brings to light the new trend amongst celebrities called Mean Tweets.

2.5 The Impact of Cyberstalking on Victims

Since there are limited studies based on the notion of cyberstalking, researchers have alternatively adopted the impacts of stalking as detailing on the impact on cyberstalking (Turvey, 2012). There is no bracket phase on determining the impact of cyberstalking for it varies within the constitution of the victim as well as the seriousness and extent of cyberstalking. Pathe (2002) is of the view that cyber security produces psychological effects on the victims. This is because cyber security consists of repetitive and consistent harassment from the cyber stalker.

According to Bocij (2005), victims of cyber stalking experience numerous forms of harassment and the stress related to this is more likely to occur when victims feel like they are cornered and suffocated and there is no way of escaping. Pathe (2002) argues that the consistencies and persistence of cyber stalkers create a phase in which the victim feels helpless and powerless. Bocij (20004) therefore posits that victims of cyberstalking often suffer from depression, anxiety, guilt, helplessness, shame and post-traumatic stress disorder (PTSD).

Furthermore, victims of cyber stalking are subject to loss of control, seclusion, self-blame, hyper vigilance and over activity (Bocij, 2004). This is because cyberstalking has the potential and the capacity to produce distress and forceful sense of infringement amongst victims. There is also a notion of secondary victimization since the victims would not have had professional help and this lead to possible detrimental dangers experienced by the victims. Although these effects are not extended to all the victims of cyberstalking, when they do occur, they disrupt lifestyles and create havoc in their intended victim's life.

The impact of cyberstalking is not limited to psychological effects, but also produces sociological consequences among its victims (Pathe, 2002). Another impact of cyber stalking on victims is that it alters the lifestyle of victims in terms of interpersonal, professional and general social functioning. There are cases where victims have been forced to change their email addresses, telephone numbers, social media usernames and in extreme cases, names in a bid to move away from the tarnishing images created by cyberstalking. Pathe (2002) also argue that in some cases, victims have even changed the schedules they used to enjoy and even relocate to different locations. Bocij (2005) highlight that the effects caused by these changes also translate into financial costs as the victim will have to spend a lot of money in trying to effect these changes. Within cases of cyber stalking, victims may also resort to restricted or discontinued access to online activities such as social networks, chat rooms or e-mail services.

The impact of cyberstalking may also transform into physical and tangible effects. Insomnia is considered as one of the main physical effects of cyberstalking. Bocij (2004) argues that in some cases, victims may stay awake for long hours and other victims suffer from nightmares. In some instances, victims develop intimacy and issues. Certain cases, victims may be exposed and left vulnerable to substance abuse as a means of achieving relief from a hopeless situation. Pathé (2002: 52) point outs physical effects such as weariness or panic and anxiety attacks, poor concentration, feebleness, fatigue, nausea and headaches. Many physical symptoms start to manifest in the victim. It is evident that such physical symptoms are likely to interfere in all aspects of a victim's life.

2.6 Cyberstalking: An International Perspective

This section seeks to present on the cyber-stalking within the international perspective. This section seeks to present on how other countries are facing challenges in relation to cyber stalking and the regulations on cyber stalking as presented within these countries. This section is ideal for it presents a lesson that South Africa can learn from these challenges and how cyber stalking is being regulated. It has been argued that existing cyber stalking laws within countries need to be revisited for the existing laws are not ideal in combating cyber stalking.

2.6.1 The United States

According to Valentino-DeVries (2018), there have been increasing calls for the U.S to enact legislation that details with cyberstalking. This is because cyberstalking has increased with the evolving nature of technology and therefore victims are not adequately protected as current laws are too uncompromising to cover on-line harassment. All the States within the U.S have passed legislation to detail with real-life stalking but however, the implementation and maintenance of these laws have proved to be difficult to achieve (Jensen, 2013). California was the first state to pass cyberstalking laws in 1990 and other nations followed suit. For example, the Michigan Criminal Code defines harassment as relating to:

"Conduct directed toward a victim that includes repeated or continuing unconsented contact, that would cause a reasonable individual to suffer emotional distress, and that actually causes the victim to suffer emotional distress. "

Within the Michigan's state understanding of cyber harassment, aspects such as sending mail or electronic communication, sending uncontested text messages and any other unwanted electronic communication relate to cyberstalking.

However, from a constitutional perspective, there are challenges in anti-stalking legislation. According to Jensen (2013), cyberstalking legislation from a constitutional perspective is too vague and too broad. The major challenge is that there is need to prove physical contact in order for cyber stalking to generally become effective. However, within the increasing nature of the internet by individuals, most of their social security amongst other things is affected online thereby making cyber stalking a major challenge yet laws are not effective in countering this phenomenon. Jensen (2013) further postulates that in some instances, legal statutes also require a "credible threat of serious physical injury or death." In such cases, e-mail harassment is unlikely to meet this standard, thereby making cyber stalking difficult to combat.

2.6.2 The United Kingdom

The U.K system is however different from that of South Africa and that of the U.S. this is because the U.K laws are flexible and is effective in countering cyberstalking. For instance, the "Telecommunications Act of 1984 in section 43 makes it an offence to send by means of a public telecommunications system a message or other matter that is grossly offensive or of an indecent, obscene or menacing character." This Act is explicit for it covers the means of electronic communication such as the sending of offensive email messages and text messages as part of cyberstalking. Even though the Act covers communication sent through public networks and not on private area networks, the Act is still relevant as most cyberstalking is committed through the use of public networks.

Another important piece of legislation within the U.K system in combating cyber stalking is the Protection from Harassment Act which was enacted in 1997.

According to Reidenberg (2006), this Act can also be invoked in cases of on-line harassment. This Act is ideal in fighting against cyber stalking for it prevents on both civil and criminal measures in dealing with cases of cyberstalking. The Act stipulates on two criminal offences namely criminal harassment and indictable offence. The latter presents on cases involving fear of violence emanating from cyberstalking.

"Under Section 2 of the Act, it is an offence if one commits online harassment of another where the accused knew or ought to have known that the course of conduct amounts to harassment. Section 4 of the Act stipulates that it is an offence if an individual pursues a course of conduct which causes another to fear, on at least two separate occasions, that an act of violence might be used against them." The Act further explains that it is sufficient that the accused ought to have known that his course of conduct would cause the other to so fear on each of those occasions. This vivid explanation goes further in trying to combat cyber stalking within the U.K perspective.

Furthermore, the Protection from Harassment Act gives power to the courts to execute restraining orders on convicted defendants, prohibiting the offender from further conduct which may be injurious to the victim. If one is found guilty of breaching that law amounts to a potential sentence of more than five years. The Act therefore covers a number of factors that amount to cyberstalking. Amongst these measures include:

- The sending of abusive messages
- The sending of threatening e-mails
- The distribution of aggressive offensive material (Chik, 2008).

All these cases whether knowingly and unknowingly constitute an offence under section 2 of the Act.

It is important to note however that proving a case against cyberstalking within both the U.K and the U.S system is difficult even though legislation on these acts exists. Reidenberg (2006) argues that the use of these laws will necessarily be limited to

relatively straightforward cases of an identifiable offender sending obscene, offensive or threatening e-mails within the UK. This is because of the unique enforcement problems involved in the legal regulation of the Internet.

2.6.3 Challenges in regulating cyberstalking

Reidenberg (2006) argues that:

> *Even with the most carefully crafted legislation, enforcing a law in a virtual community creates unique problems never before faced by law enforcement agencies.*

This is indeed true when the internet can be used as a medium to commit a certain crime. A computer as a modem ensures that an internet related crime can be committed from any part of the world, thereby making it difficult for law enforcement agencies to maintain prescribed laws. The following are challenges faced when regulating cyberstalking

- **International Stalker**

The internet as stipulated by Reidenberg (2006) is a medium that can be accessed by anyone who possesses a computer and modem from any part of the world. This means that a potential offender may not be within the jurisdiction where an offence is committed. Generally, the increased availability of smartphones and the cheap nature of data and access to free Wi-Fi mean that distance is no obstacle to the cyber-stalker. The Internet is not a “lawless place” but there are difficulties in applying laws that are made for specific nation states and this would be also true of applying national harassment and stalking laws to the Internet.

- **The Anonymous Stalker**

Another challenge in a swift regulation of cyberstalking is the potential that most cases are perpetrated through the use of anonymous accounts. Known as an anonymous stalker, the identity of a cyber-stalker may, therefore, not be revealed or found. Cyber stalkers therefore are attracted by the fluidity of the internet to perpetrate their criminal offence. Offenders therefore may adopt an on-line persona

which bears little, or resemblance to his or her real identity. This therefore makes it difficult to combat cyberstalking.

2.7 Gender Based Offenses Committed Online

The study has established that cyber stalking knows no boundaries as perpetrators use the internet to carry out their threats and actions. Bocij (2005) argues that anyone has the potential of becoming a stalking victim whether by intentionally or non-intentionally divulging their personal information online. Accordingly, Purcell, Pathe, and Mullen (2001) even though many related information is subjective, most cyber stalkers are males and victims being women. There have been relative studies of women being the perpetrators of this crime or cases of same sex harassment, but there is an unprecedented growth of male stalkers against women. Purcell *et al.* (2001) therefore argues that male stalkers in most cases have a history of criminal offending or substance abuse.

The Working to Halt Online Abuse in 2002 conducted a study in which it was discovered that 71% of cyberstalking victims were women. Furthermore, Hutton and Haantz (2003) discovered that within this scenario, 59% of those women had a prior relationship with the stalker. Within this regard, the motivational cause of cyberstalking against women is motivated by the prior relationship of some sort. According to Shackson (2016), there has been an increased in gender offenses online. Within Sub Saharan Africa, 81% of the reported cases of stalking are also motivated against women, with a healthy percentage of these crimes conducted by ex-lovers. This specification therefore outlines that four out of five victims of cyberstalking are females and females are eight times as likely to be the stalking victims of ex-partners or acquaintances.

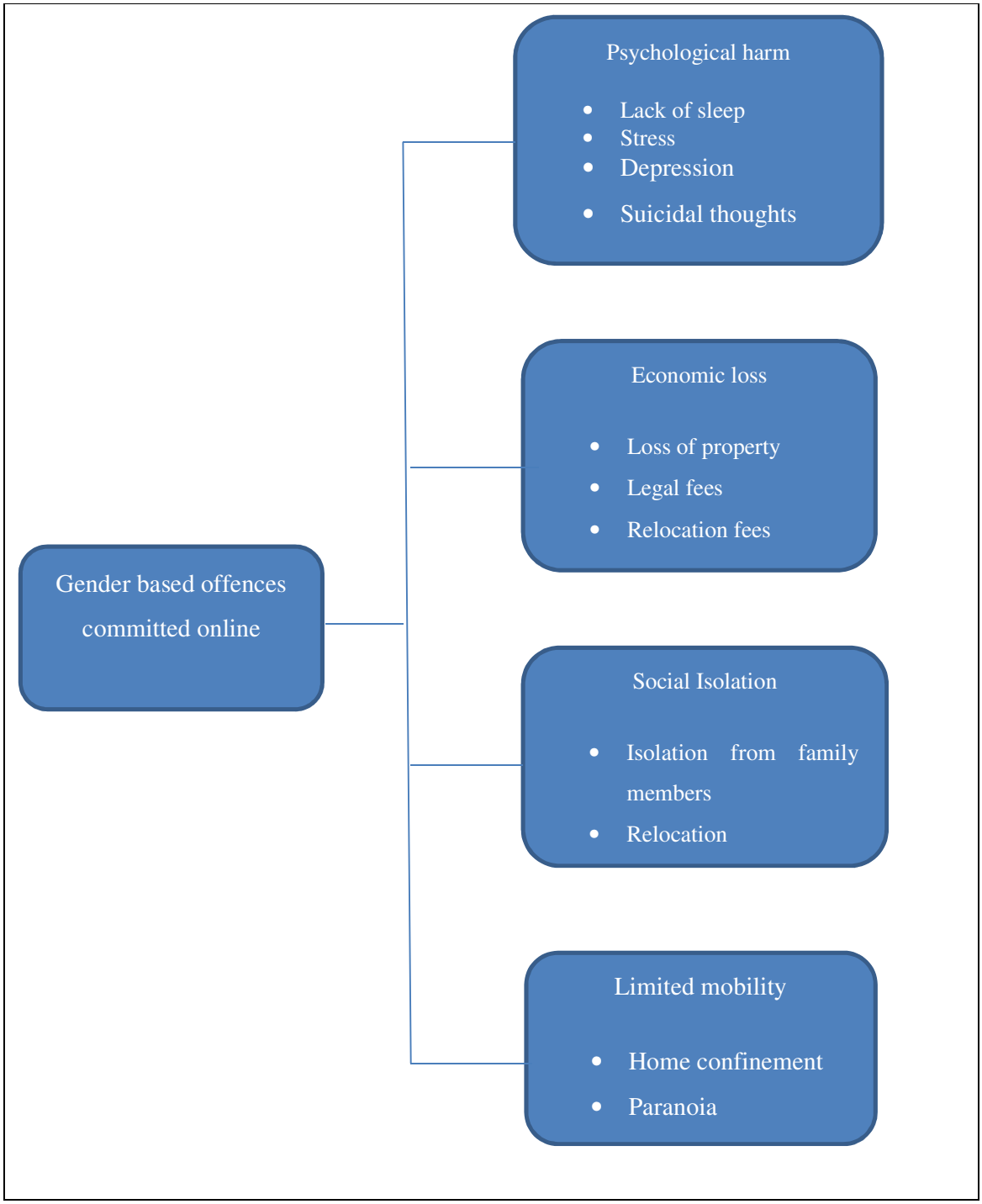
Accordingly, in a study conducted by Suarez (2014), there is a centrality of cyberstalking with domestic violence and the relationship between cyberstalking and the risk of physical violence against women. This stems from the fact that 80% of the women who are victims of cyberstalking from their ex-partners at one point or many cases had been physically assaulted by the partner. Suarez (2014) further states

that 31% of these victims were once sexually assaulted by that partner. The worrying figure is that of the reported gender based murders, 76% of these victims were once stalked by their partners prior to the murder.

2.7.1 Effects of Gender Based Offenses Committed Online

Cyberstalking based on gender has different effects on the part of the woman. According to Savait (2014), Gender based offenses infringes on the civil liberties of women in the right to self-determination and bodily integrity. Furthermore, this type of offence affects the free movement of women without fear and surveillance. Suarez (2014) further states that cyberstalking of women denies them the opportunity to create their own identity online and engage in social and political meaningful interactions. Even though studies have concluded that the chances of physical harm emanating from cyberstalking are minimum, women suffer from other forms of harassment including emotional distress.

Figure 2.3: Effects of Gender Based Offenses Committed Online



Source: Nyast, 2015)

Figure 2.3 presents on the various types of harm that are as a result of gender based cyberstalking. Accordingly, Nyast (2015) identifies in general the types of harm caused by gender based cyberstalking. Amongst the effects includes:

- **Psychological harm**

The first type of harm caused by online gender based offenses can be understood as psychological harm. Nyast (2015) argues that within this form, victims experience depression, fear and anxiety. At times, there have been records of victims being suicidal especially when things such as revenge pornography and nude pictures are shared online. According to Vitelli (2013), victims of gender based cyberstalking suffer more fear and take more actions to protect themselves over time than those who are stalked in the physical world. This is indeed a form of psychological harm. Vitelli further posits that victims of gender based offences committed online report psychological effects such as depressive and somatic symptoms, sleep problems, and generally lower well-being than non-victims. Furthermore, these victims are also far more likely to take defensive actions, such as taking time off from work or school, changing jobs or schools, and even moving away from family and friends to avoid contact with their stalker.

Effects on mental health are also another important aspect of psychological harm that impact on victims of gender based offences committed online. Vitelli (2013) is of the view that inherent with women that have been victims of cyberstalking include denial, confusion, self-doubt, questioning if what is happening is unreasonable, wondering if they are over-reacting, frustration, guilt, embarrassment and self-blame. All these signs ideally lead to agoraphobia (frightened to leave the house and never feeling safe).

Furthermore, victims of gender based offences committed online tend to find it difficult to sleep. Nyast (2015) is of the view that nightmares and ruminating are the critical psychological effects of cyberstalking. Furthermore, victims are easily irritated, angry and have homicidal thoughts. Savait (2014) states, victims also suffer from symptoms of post-traumatic stress disorder, mostly hyper vigilance (always on the lookout), and flashbacks of frightening incidents and are easily

startled. The effects may prolong into insecurity and inability to trust others and problems with intimacy.

- **Economic loss**

Another form of harm caused by gender based offenses is loss of economic income on the part of the victim. There are reports in which women have lost employment because of their perceived behaviour which would have been posted online. Vitelli (2013) is of the view that victims of cyberstalking take more self-protective measures, pay higher out-of-pocket costs to combat the problem and experience greater fear over time and all this impact on their financial status. According to Nyast (2015), there are a number of financial costs that are as a result of gender based offences committed online. Amongst these include legal fees which are unparalleled as well as damage to property.

Furthermore, child care costs and moving expenses are also part of the financial implications that come with cyberstalking of women. Of importance to note is that in general, South Africa is the third highest country that loses money due to cybercrime in general. According to the South African Banking Risk Information Centre (SABRIC), South Africa is currently ranked as the third highest number that has cybercrime victims. An estimated loss of about R2.2 billion a year is attributed to cyber-attacks. Ideally, there is a significant amount that can be related to cyberstalking, which amongst the forms of cybercrime, ranks highly in South Africa (IOL, 2018).

- **Social Isolation**

Another related effect on gender based offences committed online is social isolation**.** According to Nyast (2015), a common feature associated with victims of cyberstalking is isolation from family members, loved ones and the community at large. Women who have had their photos and videos circulated online without their consent have at times been publicly humiliated and ridiculed. This therefore impact on their confidence leading them to live a life of isolation (Nyast, 2015).

According to Vitelli (2013), in most cases, women who have been stalked and their personal information shared online suffer from isolation as the people around them at times withdraw their company because they don't have faith in the victim, they are unable to cope with the victim's psychological state or as a direct consequence of third-party victimisation. Understandably, social isolation also comes through the victim trying to isolate themselves in a bid to protect their loved ones from the shame. Therefore in most cases, victims end up relocating to a new area where they are unknown; changing their phone number, name or even their outward appearance. Within this regard, social isolation is also another effect of gender based offences committed online. Alexis Moore had been one of the many victims that have experienced social isolation by losing everything listed above as others have isolated her (Thomas, 2019).

- **Limited Mobility**

As discussed above, limited mobility is an effect of gender based cyberstalking. Savait (2014) is of the view that victims of cyberstalking are not able to move freely around and they are also limited to participate in online initiatives due to fear. Maple, Shart and Brown (2011) emphasises that cyberstalking has repeated incidents which aid in the victims sense of safety which cause, distress, anxiety and fear. In most cases, victims tend to change their usual routine for they cannot cope with the shame and embarrassment that would have been as a result of gender based offences committed online.

Nyast (2015) is of the view that victims tend up avoiding their usual activities such as going to the gym or going out amongst other routines. Victims therefore tend to be confined in their comfort zones such as homes and work place and they tend to be highly paranoid. According to Mullen (2018), victims of cyberstalking also have a tendency of holding dear their personal belongings or loved ones such that they do not want them out of their sight and tend to be highly paranoid if the normal routine such as a child coming back from school is missed. Within this regard, limited mobility is also an effect of gender based violence committed online.

- **Self-censorship**

Defined as fear of further use of the internet and associated media, victims tend up limiting their use of internet (Nyast, 2015). The major effect of removal of one-self from the internet has wide and diverse effects including lack of access to information, e-services, and social or professional communication. Self-censorship can also result into personality changes as the victim may become more suspicious, introverted or aggressive. Victims may also resort to self-medication, alcohol abuse and in some cases; there have been suicidal thoughts and attempts.

- **Effects on work and School**

Gender based offences committed online also have an effect on school and work performances of victims. The common effect is that of the deterioration of work and school performance. Mullen (2018) argues that due to the effects, a victim may increasing take sick leave or be absent from school which in turn risks on their productivity. They are a number of victims who have been stalked online that have lost their jobs due to under performance (Mullen, 2018). Some have even taken different career paths for their reputation would have been hurt and thus they will be facing challenges of sustaining within their career. Victims have also dropped from school due to poor education results.

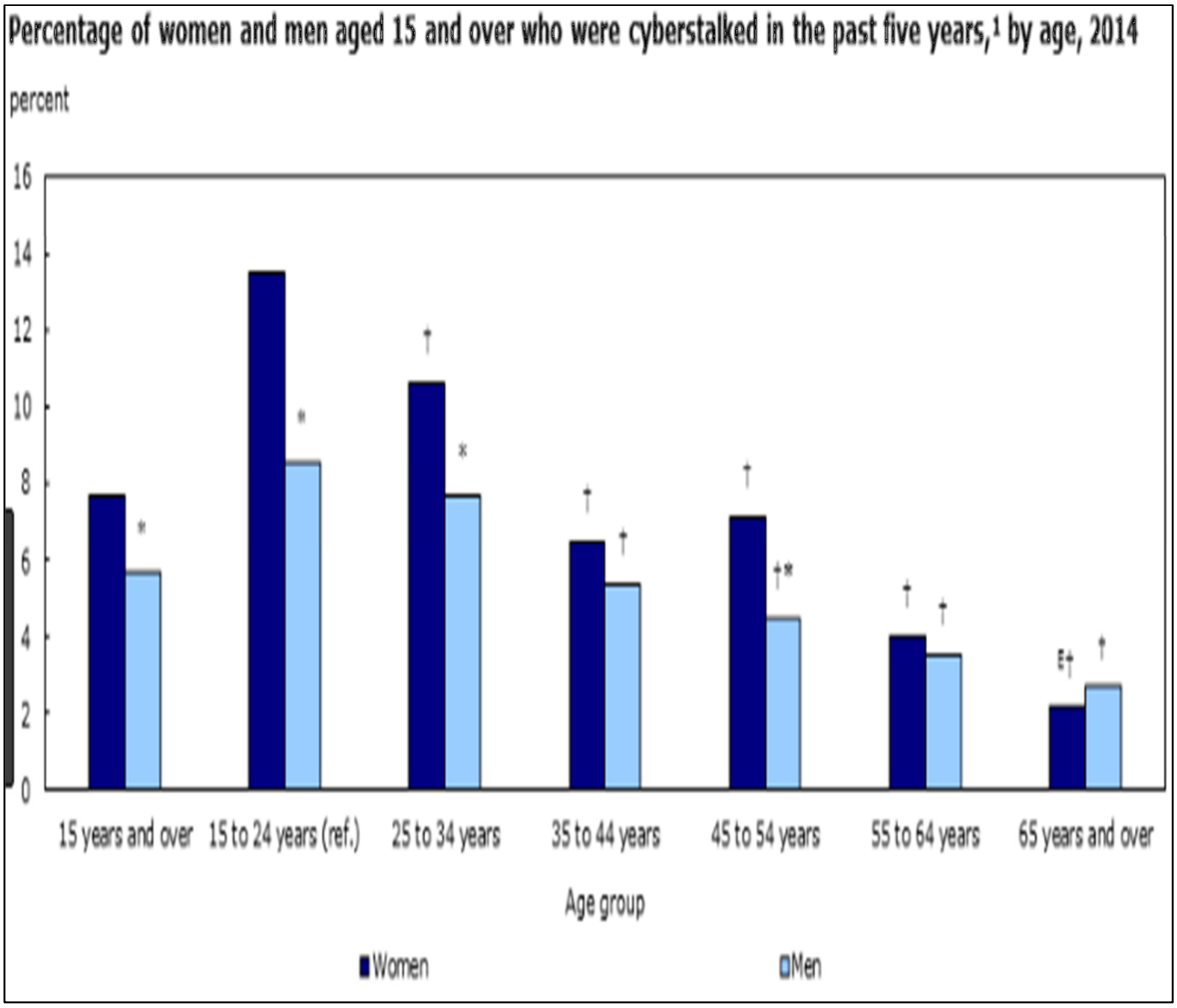
2.7.2 Female vs. Male Cyberstalking

There is generally a wide difference between male and female cyberstalking. Following is a discussion on the causes, factors and other factors that contribute to the difference between female and male cyberstalking. Accordingly, Mullen (2018) conducted a study within the U.S on the difference between male and female victims of cyberstalking. Mullen (2018) therefore gathered that more than one million women and 370,000 men are stalked annually in the United States. This rate therefore stipulates that women are prone to cyberstalking generally more than men. Mullen (2018) further stipulated that an astonishing one in twelve women and one in forty-five men will be stalked in their lifetimes. There is drastically a wide gap between men and women in relation to cyberstalking. Mullen (2018) further stipulates that the

average duration of stalking is nearly two years and even longer if the stalking involves intimate partners.

Nyast (2015) further explained on the varying differences between male and female cyberstalking from the US perspective but referencing them globally. Nyast (2015) therefore gathered that female victims of cyberstalking tend to be females during their college phase aged between 18-29 years but women are not the only targets. A survey of 765 students at Rutgers University and the University of Pennsylvania found 45% of stalkers to be female and 56% to be male (Saivat, 2015). Global figures however presents on the fact that most stalkers to be male by overwhelming margins (87%). The following figures presents on the history of cyberstalking between male and females.

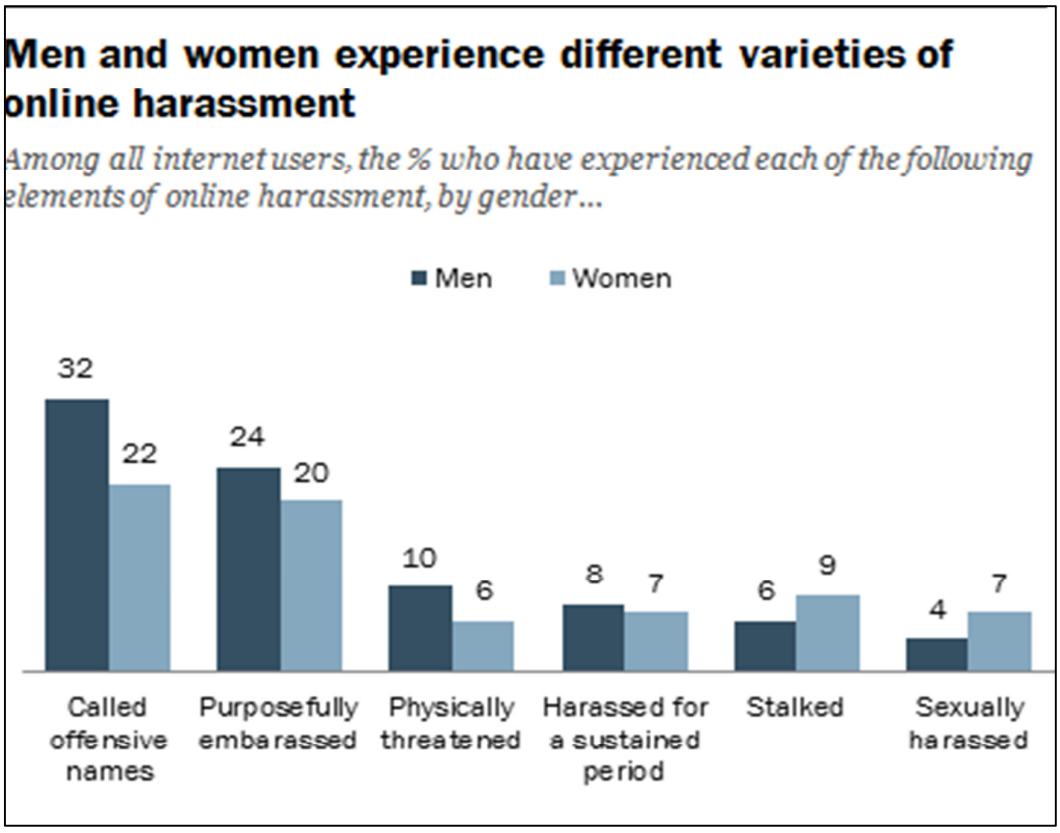
Figure 2.4: 2014 Statistics on the percentage of women and males who were cyber stalked in Canada



(Source: Statistics Canada, 2014)

Figure 2.4 stipulates that there are varying figures between male and females who are being cyber stalked. The figure confirms with the study conducted by Mullen (2018) who argued that those aged between 15-34 years are mostly affected by cyber stalking. The figures significantly drop however with the growing age of an individual. The following figure presents on the varying reasons why men and women are cyber stalked and the percentages related thereof.

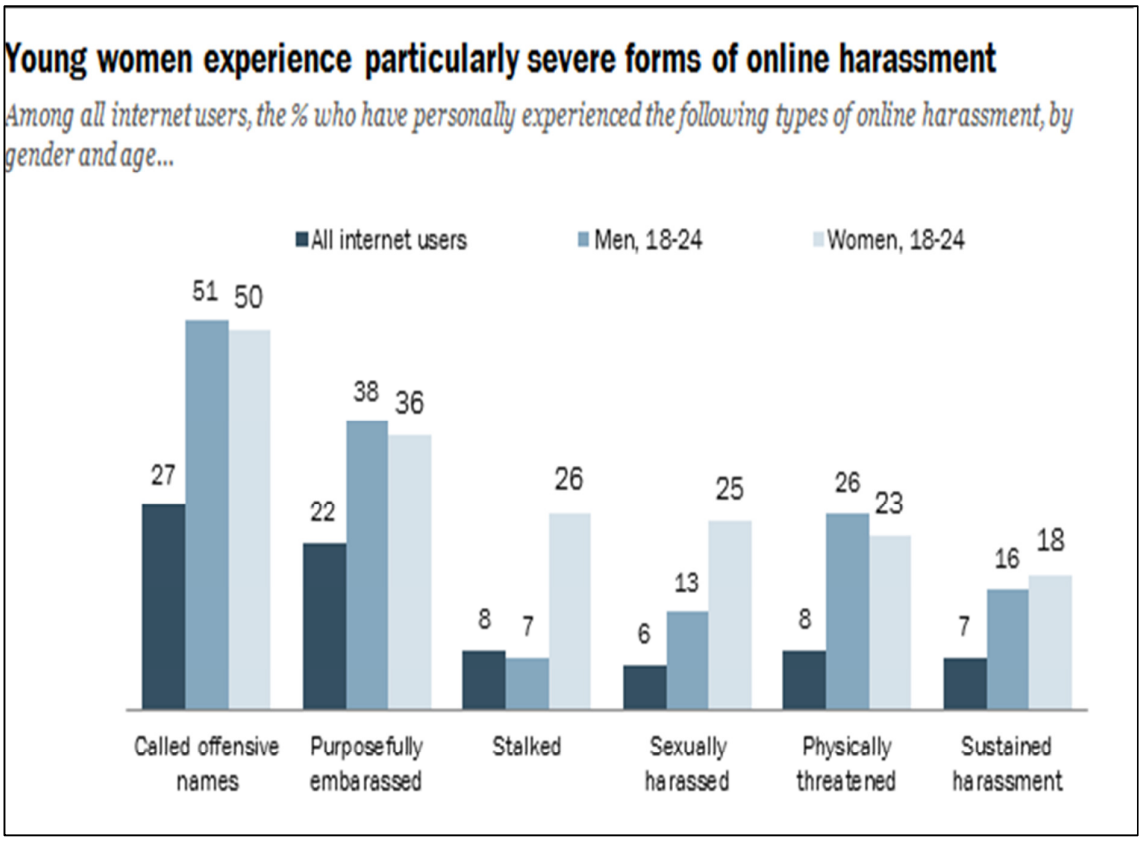
Figure 2.5: Men and Women experience different varieties of online harassment



(Source: Duggan, 2014)

Figure 2.5 stipulates that even though women have the considerable numbers in being cyber-stalked, men also suffer from other forms of online harassment in their high numbers. For example, the percentage of men who have been called offensive names is significantly higher than that of women. Furthermore, those who have been purposively embarrassed, men rank slightly higher than women. The important part however is that women have been stalked more than men on the internet thereby attesting to the fact that women are victims of cyberstalking rather than men. The following figure therefore presents on the men and women between the ages of 18-24 who experience different varieties of online harassment.

Figure 2.6: Women and Men Aged 18-24 and the different forms of online harassment they face



(Source: Duggan, 2014)

The figure above presents on the fact that women between the ages of 18-24 are more prone to stalking than any other forms of online harassment. Saivet (2015) argued that these increasing numbers are probably due to the fact that these women are in their discovery age and by nature, they attract attention. This explains the reason why a large proportionate of women is cyber stalked as compared to men.

2.8 Conclusion

This chapter discussed on the relevant literature underpinning the study. This chapter therefore started by investigating on the concept of cybercrime. Developed from investigations of this concept, the study reviewed relevant literature on what cyberstalking entails its nature and relevant legislation underpinning the concept in South Africa. Just like most studies, this study chapter is premised by the objectives set out in chapter one therefore, the study did not exceed these boundaries. This chapter therefore gathered that cyberstalking is a relatively new phenomenon that requires extensive literature, for an understanding of the concept. Since the study aims at understanding cyberstalking against women, the study aims to contribute to the knowledge production of contemporary crimes such as cyberstalking and the empowerment of past, present and future victims of cyberstalking.

CHAPTER THREE

THEORETICAL FRAMEWORK

3.1 Introduction

Within any study, a theoretical framework is of great significance. This is because a related theory helps understand the research problem and concepts underpinning the study. Within this case, this study identifies the rational choice theory which details on the assumption on human behavior, lifestyle exposure theory which is premised on how people live their lives, space transition theory which detail on the effects of cybercrime and the routine activity theory which details on the routine of the life of individuals will be discussed in a bid to understand cyberstalking: a content analysis of gender based offenses committed online. The study utilizes a number of theories so as to have different insights and perspectives on the research problem. The theoretical framework is essential for it seeks to explain from a theoretical standpoint on how these theories helps to validate on the research problem. In general, these theories therefore function as possible explanations for cyber stalking against women.

3.2 The Rational Choice Theory

The rational choice theory is of fundamental use within this study. According to Wright (2009), the rational theory and its assumptions about human behaviour is useful in the study of criminology. Cesare Beccaria is attributed to have propounded the theory and ever since its emergence in the 18th Century, there has been an expansion of the theory to cover wide areas such as situational crime prevention, routine activity theory, deterrence and crime analysis (Wright, 2009). Within this regard, the rational choice perspective has been applied to a wide range of crimes, including robbery, drug use, vandalism, and white-collar crime. In addition, neuropsychological literature shows that there are neurobiological mechanisms involved in our “rational choices.”

Wright (2009) argues that the fundamental aspect underpinning the rational choice theory is that of individual preferences, beliefs and constraints. Preferences in this case include the positive and negative outcomes that may come out of any situation, beliefs entails the cause-effect relationship which translates into the cost-benefit of doing a certain task and the constraints define the limits to the set of feasible actions. As stipulated by Bransen (2001), the rational theory therefore stipulates the rational behavior that is suitable for the realization of specific goals given the limitations that is imposed by the given situation.

Acheson (2002) is of the view that the rational choice theory stipulates that in their preferences, human beings are driven by selfish desires and the goal is attain maximization of their goals. This relate to this study as cyber stalkers are all but concerned with their ego and coming out on top in every situation (Bocij, 2004). Furthermore, the rational choice theory prescribes that selfish act in the form of opportunism lead individuals to break laws if only their objectives are met. This is in relation with cyber stalker who breaks a plethora of legislation in trying to achieve their goal of bringing suffering and embarrassment towards their victims.

Furthermore, the rational choice theory is premised on the fact that human beings through their nature of being selfish, egocentric and brutal do things that maximize their benefits (Siegel, 2011: 83). Bransen (2001) is of the view that the aim of the rational choice theory is to explain and predict human actions in terms of laws that causally relate expected utility numbers and ensuing actions. Adopted from the economic field where organisations seek to maximize their profits with relative loss, the rational choice theory assumes that human beings behave in a way that best suit their interest.

Initially classical criminology was believed to be the works of sins and demons which was later replaced by explanations of rationality (Siegel, 2011: 85). Cornish (2010) argue that criminals rationalize and weigh the benefits and consequences of a crime before they commit it. Cyber stalkers therefore are argued to weigh their prospective benefits against the potential risks and act upon it. In the case of cyber stalking the benefits are destruction. The use of the Rational Choice Theory in this study

therefore helps since the study attempts to understand and explain social phenomenon regarding cyberstalking and cyber bullying against women.

The theory understands that for a crime to happen there should be a motivated offender or perpetrator. According to Davis (2005), a motivated offender is an individual who has the motive to commit a crime and is capable of doing so. There are reasons why an individual is motivated to commit a crime and relevant to this study, in cyberstalking, perpetrators are motivated by one of the many factors such as rejection, obsession, vengeance or power (Mullen et al., 2009). These reasons therefore motivate people to commit cybercrimes such as cyberstalking.

Secondly, another element that helps understands this theory and its relationship with cyberstalking is that of a suitable target. When the theory was propounded, value comes in the form of financial and material gains but in cyberstalking, value of the crime comes in harassment and embarrassment of the victim. Furthermore, in cyberstalking, there is no physically visibility of the stalker, but may have originated its shape in an online encounter such as in a chat room. Davis (2005) describes accessibility as an idea where an offender approaches the victim without suspicion and cyber stalkers are highly intellectual beings when it comes to cyber technologies and can thus effortlessly find and approach their victims in order to exploit and manipulate them, often remaining unidentified due to the anonymity and concealment of cyber space. Cyber stalkers can access information about their victims effortlessly due to factors such as careless distribution of personal details as well as the absence of protective software.

The last attribute is that of absence of capable guardian. Within any sphere, the absence of a guardian makes the victim prone to attack. Guardianship is not only related to people surrounding a person but refers to modern ideals such as security system or alarm system. Therefore, Davis (2005) argues that the presence of a guardian weakens the possibility of a crime ever happening. In relation to cyberstalking, guardianship may come in the form of protective software or responsible awareness of the dangers within the cyber

3.3 Space Transition Theory

The study also utilizes the space transition theory in a bid to understand the research problem. Accordingly, Professor K. Jaishankar (2008) a Criminologist that has researched cybercrimes and cyber bullying proposed for a theory, “Space Transition Theory.” The theory ever since its development in 2008, it has gained widespread attention in criminology and as off date, the theory is the most frequently cited theories in cyber criminology. According to Jaishankar (2008), the development of the space transition theory brought about the new understanding on cybercrime and the development of this model helped ease the understanding of cybercrime and how it can be countered. All of this is related to the fact that the Space transition theory was propounded where no other scientist could explain the overall discourse on cybercrime.

The theory aims to explain and understand the causation of crime, nature of behavior in terms of conforming and non-conforming behavior in cyber space and in reality. Jaishankar (2008) stipulates that the space transition theory explains the nature of individuals who bring out their conforming and non-conforming behaviours in cyberspace and their actual physical space.

The first assumption of the theory is that a person with repressed criminal behavioural tendencies may have a higher inclination to commit the act in cyber space whereas they would not commit it in the physical space due to status quo and position in society. In this proposition, Jaishankar (2008) borrows the assumptions of Arbak’s (2005) model of crime and social status to explain that:

- “Individuals feel varying degree of self-reproach on engaging in criminal activities,
- They are generally concerned with their social status in the society, based on others’ perceptions of their values and,
- In making their decision, they calculate the social and material risks of being a criminal against the comfort of living as a law-abiding citizen. “

To say in other words, people who are more sensitive to guilt may not endorse a criminal lifestyle. The anticipation of the harm to one's social status and the subsequent embarrassment it will cause to them, generally inhibit the individuals to act as if 'they are moral'.

The second assumption of the Space Transition Theory is that identity flexibility, dissociative anonymity and a lack of the deterrence factor contribute towards committing a cybercrime. Jaishankar (2008) is of the view that aspects such as anonymity lead people to sometimes act in unpleasant manner including cyberstalking and cyber bullying. As stipulated by Suler (2005), when people are under the bracket of anonymity, they are influenced to commit acts of crime in which they have a feeling that it won't be traced back to them. Apparently, one of the key factors that urge most members in the society to carry themselves in an honest, non-violent manner, is the fear of being caught – a deterrence factor. However, this deterrence, however, is diminishing largely in the cyberspace thus leading to cybercrime.

The third assumption within the Space Transition Theory is that if a criminal displays behaviours that are criminal in nature in the physical space, then they would be most likely commit it in cyber space as well. This is also true in the fact that criminals can start exhibiting their behaviour online and then transform that behaviour into the physical world (Jaishankar, 2008). For example, during the early 2000s, individuals would operate on their own whilst scheming and committing cybercrime but in recent past, there has been an increase in organisations which have since seen the cyberspace as an avenue to make money. This is enhanced by the fact that cyber space allows criminal gangs to facilitate and cover up their criminal activities. Today, the ease with which the cyber criminals transfer money from one account to other, it seems fairly difficult for the law enforcement to follow the financial transactions of criminal gangs.

Another assumption within this theory is that strangers are most likely to unite together in cyber space to commit a crime than in a physical space, these include associates working together to commit a cyber space criminal act. Moore (2012) are

of the view that the past few years have seen an increase in the use of the internet as a recruiting platform of criminals. For example, ISIS has used this platform to reach a wide number of youth within the Islamic State. This highlights the fact that in real time scenario where like-minded people merge online to spread criminal violence in physical space.

Furthermore, the Space transition theory posits that individuals that form part of a closed society are more likely to commit a cybercrime as compared to individuals from an open society. Within this aspect, Jaishankar (2008) argues that people who live in open societies have the opportunity to express their feelings in demonstrations and strikes. However, this is different from people who live in closed societies where their feelings are suppressed. Such people, Jaishankar (2008) argued find solace in the cyber space, as they engage in all sorts of criminal activities including but not limited to ordinary online hate messages in social media, cyber terrorist activities, and posting revenge porn images of ex-partner amongst others.

The last assumption underpinning the space transition theory is that due to differences in norms and conforming behaviour in cyber space and physical reality, this may create a conflicting matter for the individual committing the crime. Within the cyberspace, people from different dimensions meet and conflicts that arise from the cyberspace lead to the intention of committing cybercrimes.

This research believes that in cyberspace, individuals that harass other individuals online do freely as they feel secure in the anonymity associated with being connected online. A person can create any persona online, including multiple accounts that aid them in cyberstalking and online harassment. There is a lack of research and stringent laws regarding cybercrimes. Individuals make a rational choice to commit these activities with the security of knowing their identity is private. These individuals do not act out impulsively but rather in a well-planned and calculating manner in order to disrupt, destroy and dehumanize, instilling fear in their intended victims.

3.4 Lifestyle Exposure Theory

The study also utilises the lifestyle exposure theory. The theory was developed by Hindelang, Gottfredson and Garofalo in 1978. Generally, this theory was formulated on data gathered during victimisation surveys conducted across America. In general, lifestyle may be defined as "patterned ways in which individuals channel their time and energy by engaging in a number of activities" (Fattah, 1991:319). However, Hindelang et al (1978) define lifestyle as "routine daily activities, both vocational (work, school, keeping house) and leisure activities."

The general notion underpinning the lifestyle exposure theory is that the probability of victimisation is dependent on the lifestyle of the victim. According to Davis (2005) the theory attributes to the notion that people adhere to personal routines in living their lives. Therefore, lifestyle and victimisation rates are related to individual's demographic traits such as age and gender. Within the theory, younger and single people are therefore prone to victimisation due to the lifestyle they lead. Siegel (2004: 92) adds that the involvement of an individual with an on-going criminal career enable the individual room for victimisation. Reyns (2010: 37) highlights the lifestyle exposure theory by envisaging the degree of exposure to dangerous situations and opportunities that are available and dependent on the activities that comprise an individual's lifestyle.

The fundamental principles underlying the lifestyle exposure theory as argued by "Davis (2005) are:

- The uneven distribution of criminal victimization across space and time. This translates to the occurrence of high-risk places and high-risk times
- Offenders do not constitute a representative sample of the general population. This translates to the occurrence of high-risk persons
- Lifestyle determines the likelihood of personal victimization through the intervening variables of exposure and association
- People are not equally exposed to high-risk places and times, and they vary in the degree to which they associate with high-risk persons. This translates to a

person's lifestyle influencing the exposure and association with low-risk persons"

In general, the theory is premised on the demographic characteristics of the victims. It stipulates that demographic characteristics relate to the lifestyle of the individual and within this aspect, they are prone to cyber victimisation. In detailing on the lifestyle theory, Hindlelang et al (1978:242) argues that this is attributed to the relationship between demographic characteristics and structural constraints ascribed to groups whose members share those characteristics. In so far as people share the characteristics with potential offenders, they face increased risk of victimisation. From an offender's perspective, personal characteristics and lifestyles contribute to determine target suitability and desirability (Hindelang et al., 1978:242). The personal characteristics which are relevant in the current study comprise age, gender, marital status, family income and race

The theory is relevant in trying to determine cyberstalking and gender based offences committed online. This is because the theory is premised on the lifestyle of victims, the same lifestyle that invites cyberstalking. This is because one cannot become a perpetrator or victim of cyberstalking if there are not active within the cyber space (Reyns, 2010). However, when an individual is operating online and is active in technologies, can they become a victim or become prone to cyberstalking. Reyns (2010) in explaining the relevance of lifestyle theory in the discourse of cyber stalking argues that the lifestyle of engaging in the online realm requires some routine in daily activities as it could be needed for work purposes or be a part of one's social habits. Therefore, younger individuals and single people are more prone to cyber victimisation as they are more familiar with cyber space.

A victim is more likely to become a victim of cyberstalking as the perpetrator interacts with the victim anonymously or through an alias within the realms of cyberspace. Individuals post an array of information online and perpetrators may find personal information such as residential addresses, email addresses, contact information that can be obtained by online search directories or a simple web search (Chik, 2008). Cyberstalking is a distressing experience for victims; the repercussions

could place the victim in psychological trauma and possibly physical harm as the perpetrator has the advantage of exploiting their intended victim. The Lifestyle exposure theory contributes to the offender being able to cyberstalk their intended victim through information that is readily available online; or through the absence of a protective software programme (Chik, 2008).

3.5 Conclusion

This chapter discussed on the theoretical underpinnings in reference to this study. A theory is of vital importance for it produces an understanding on the research problem. This chapter therefore discussed on relevant theories such as the rational choice theory which stipulated on how individuals live their lives thus relevant in structuring how people conduct their day-to-day lives on the internet. This chapter also presented on the space transition theory which explains how the internet has evolved and is now impacting on the lives of people, the lifestyle exposure theory posits that certain information is accessible online that allows an individual to become a victim of cyberstalking which may be psychologically distressing for the victim. All these theories are relevant for they bring about their relevance in understanding the research problem.

CHAPTER FOUR

METHODOLOGY

4.1 Introduction

The research methodology plays a fundamental role in any research. This is because the methodology presents a blueprint of the research techniques within this chapter, the nature of the research design and the research approach utilized within the study will be explained in detail. This chapter also focuses on the data collection methods as well as data analysis methods. Important and integral within this chapter are the ethical considerations for they give base to the study.

Accordingly, Taylor, Bogdan and De Vault (2015) are of the view that the overall term methodology in research entails how researchers approach the research and seek answers in relation to the problem. The general underpinning of methodology in research is that it helps collect data within the research setting and helps authenticate the findings for generalizations on the entire population. As stipulated by Beng (2004: 32), research methodology entails systematic steps in order to form a collaborative approach to issues that affect the communities and/ or issues of study by applying a democratic, encouraging environment for individuals to share their problems. This chapter therefore details on the understanding of research methods utilized within the study.

4.2 Research Design

According to Van Wyk (2011: 1), research design entails *"the overall plan for connecting the conceptual research problems to the pertinent (and achievable) empirical research."* Generally, the whole concept of research design brings about the nature and type of information that needs to be collected, how that information will be collected: all in a bid to answer the research question. Babbie (2010: 29) argues that the research design is a main proposal of choosing the correct methods and procedures for collecting, analyzing the data collected from the study. The research design is rather a *"framework that stimulates the choosing of research approach in the research, how the sample was selected, data analyzed and the*

piloting" according to Flick (2014: 12). Accordingly, a research design is an intentionally organized proposition for the conditions of the data collection and data analysis in a way that ensures importance to the research objectives. Different design logics are used for different types of study. Following is a brief discussion on various research designs.

- **Explanatory Research Design**

Creswell (2014: 158) is of the view that *"explanatory research design seeks to explain the occurrence of certain phenomena and predict future happenings."* Within this perspective, explanatory research designs seek to understand and characterize the relationship between the dependent and independent variables within a research problem. For example, explanatory research designs seek to understand the impact of cyberstalking on victims of gender based violence committed online. Babbie (2010) argues that this design is normally ascertained under probability means to allow generalization of the results from where the sample or subset is selected.

- **Exploratory Research Design**

Flick (2014) is of the view that exploratory research designs are useful studies that seeks to confirm to a hypothesis through hypothesis testing. Generally, exploratory designs intend to formulate a research problem, elucidate concepts and create hypothesis. Derived from the name of this design, exploratory research designs are utilized in studies which are relatively new and where there is no studies that can be referred to. From this understanding, exploratory research designs are normally products of qualitative research approach.

- **Case Study Research Design**

Creswell (2014) argues that a case study research design is utilized in studies that seek to understand a particular case study, the objective being the need to understand present circumstances and realities. Babbie (2010: 29) defines a case study research design *as "an instrument that investigates a contemporary phenomenon in depth and within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident."* The advantage of this research design is that the researcher has the ability of understanding the research

problem within the context or setting, where information is raw. Creswell (2014) argues that case study research designs utilize a geographical area in which the sample has the actual understanding of the research problem. Therefore, purposive sampling is often used in case studies. Therefore, case studies, in their true essence, explore and investigate contemporary real-life phenomenon through detailed contextual analysis of a limited number of events or conditions, and their relationships.

The general notion underpinning a research design is that both data and methods, and the way in which these will be configured in the research project, need to be the most effective in producing the answers to the research question taking into account practical and other constraints of the study according to Van Wyk (2011). This research therefore utilizes the descriptive research design.

4.2.1 Descriptive Research Design

The nature of the research question is best suited to be understood through following the precepts of the descriptive research design. Van Wyk (2011) argues that the descriptive research design is where the researcher observes or goes through related information/research participants without intervening. Creswell (2014) argues that the simplest type of descriptive research design is that one which seeks to understand a single phenomenon, in this case cyberstalking based on gender. According to Van Wyk (2011: 12), a descriptive research aims to provide a valid and correct presentation that is relevant to the research question. The rationale of a descriptive design is that it is structured making it easier to comprehend than other research designs.

The rationale for utilising a descriptive research design is that it tells what is within a research problem, thus useful in both qualitative and quantitative studies. Furthermore, Babbie (2010) argues that descriptive research designs give an accurate detail pertaining to a certain individual or research setting. Descriptive studies therefore discover new meanings, describe what exists, describes the frequency of why something exists and categorises meanings. The research design that will be undertaken will be a descriptive design as it will describe and define the

phenomena as accurately as possible; documenting the different types of cyber criminology, the motivations of cyberstalking perpetrators, the prevalence of cybercrimes and the content analysis of media coverage on cybercrimes (Struwig & Stead, 2013: 7).

4.3 Research Approach

There are various research approaches utilised by researchers. The most common types include qualitative and quantitative research approaches. However, modern research scholars such as Flick (2014) and Neuman (2014) have identified mixed methods as one of the emerging approaches that researchers are now utilising. However, this study due to the nature of the research problem: Cyberstalking-a content analysis of gender based offenses committed online, will utilise the qualitative research approach.

4.3.1 Qualitative Research Approach

The study will follow a qualitative research method. This method allows the researcher to gather and provide explanations of the social phenomena and create an understanding of cyberstalking from a criminological perspective (Joyce, 2009: 101). Accordingly, Bouma and Atkinson (1995) suggests that qualitative research is that research that seeks to understand the lives of people, their stories, their perception about life and generally how they behave. The rationale behind this approach is that it allows for the detailed gathering of rich descriptive data from the owners of their own story therefore first-hand information is always reliable. Neuman (2014) asserts that qualitative approach leads to the broadest and most descriptive information that is useful within research. It is therefore essential for the study to utilise qualitative research for it will bring into light cyberstalking based on gender. In comparison with a quantitative study, the quantitative study is not capable of producing detailed information on the experiences and perceptions of research participants due to the methods of data collection it uses. This is however different with a qualitative study as it is rooted into views and perceptions of research participants (Neuman, 2014).

Babbie (2010) defines qualitative research as that approach that seeks to define the relationship amongst the research variables. In other words, qualitative research entails how a phenomenon under study is impacted or how a phenomenon under study is related to its social setting. Therefore Neuman (2014) stipulates that qualitative research is primarily exploratory research and is utilized to gain an understanding of underlying reasons, opinions, and motivations. Qualitative research is also used to uncover trends in thought and opinions. Creswell (2014) states that this research method is mainly designed to reveal a target population's range of behaviours displayed and the perceptions that drive this behavior with reference to specific topics or issues. It uses in-depth studies of small groups of people to guide and support the construction of hypotheses. The results of qualitative research are descriptive and inductive rather than predictive and deductive, thus useful in this research.

The study utilized the qualitative research approach for a number of reasons. Firstly, the qualitative approach seeks to understand the connotations and emotional value of things that people attach in their lives (Babbie, 2010). Generally, qualitative research seeks to understand a phenomenon from people's perspectives therefore the researcher should tap into the reality of the research participants if a detailed understanding of the phenomenon seeks to be understood. It is of paramount importance that the researcher understands the views, perceptions and experiences of victims of cyber stalking so that a detailed understanding of cyberstalking against women is understood and methods and means to counter this cybercrime framed.

The study utilizes qualitative research for it is inductive. Babbie (2010) asserts that inductive reasoning for it is a form of logical thinking that comes from making generalizations based on shared or specific incidents that have been observed or experienced. Strauss (1967) is of the view that researchers utilizing the qualitative approach create concepts, insights and understandings from patterns of data. Deductive reasoning therefore is premised on creating new ways of thinking through building up to a theory. This is in contrast with a quantitative research which utilizes deductive reasoning which starts with a theory and seeks to confirm to that theory.

This study therefore utilizes inductive reasoning where the research questions are the base of analysis.

This study also utilizes qualitative research for it is naturalistic in nature. According to Neuman (2014), qualitative research is concerned with how people react and act in their daily lives. To ascertain information in relation to the research approach, qualitative research uses methods that interact with individuals in their natural setting. Within this research for example, women who have been subject to gender based cyber bullying have a higher chance and probability of giving detailed information which helps understand the research question. The rationale of this method therefore is that information is gathered from knowledgeable individuals is beneficial to the study because the researcher gathers information of real-life experiences.

Qualitative researchers emphasize the meaningfulness of their research as the approach gives the researcher the space to make sense of the empirical world. It ensures that there is a close connection between the data and what the people do and say in real life (Steven, et al., 2016). Furthermore, for the qualitative researcher, there is something to be learned in all settings and groups. Steven et al. (2016) propose the argument that no social life is too mundane or too trivial to be studied. The setting in which Respondent A and Respondent B were victims of cyberstalking is different so by understanding the setting on a participant, a more detailed and generalised understanding of the phenomenon can be established. This becomes the rationale of utilising a qualitative study.

Lastly, the study utilised the qualitative research due to its nature of utilising different methods, suitable within the research context (Creswell, 2014). In other words, qualitative research is a craft. Qualitative research is structured by guidelines not rules, meaning that the researcher is flexible, using methods that best suits the situation. In other words, qualitative research methods are subjective to the researcher. As stipulated by Steven et al. (2016), qualitative research does not entail rigid procedures but allows the researcher to utilise methods that helps better understand the researcher problem. This is the reason why the study utilise the qualitative research approach.

4.4 Data Collection - Secondary

Data collection instruments are essential in trying to create a framework that helps the researcher to gather data. There are basically two types of data collection in research. These are primary sources and secondary sources of data. According to Creswell (2014), primary sources include the information gathered directly from the research participants whereas secondary sources include that information gathered from published text. Due to the nature of the study, secondary sources of data collection will be utilized. This is because the behavior of victims of cyberstalking has been tabulated in published texts within South Africa.

This study utilises secondary sources of data collection. Secondary sources of data collection entails gathering informed and relevant data from published texts, journals books and other relevant sources. Within this regard, a search will be conducted on all online databases in relation to the data material required for the analysis. Online databases that will be searched include Ebscohost, Google Scholar, Psychinfo, Psycharticles and Departmental websites. Books published, peer-reviewed articles and dissertations will also be analysed. The media coverage will be assessed on the related topic on cybercrimes. Keywords that will be used to identify data material will consist of the following: cybercrimes, computer crimes, cyberstalking, online identity theft, stalker perceptions, cyber victimology, online harassment, stalker tendencies and characteristics.

4.5 Data Analysis

After data has been collected or gathered within any research, data analysis follows. Generally, data analysis entails making sense of the collected data. In line with the qualitative research approach, the collected data needs to be reviewed to generate initial codes for catching features of the entire data set (Maree, 2010). Van Wyk (2011: 23) argues that data analysis within a qualitative study entails explanation, understanding and interpretation of the intended subjects and documents that were investigated; which is from the qualitative data collected. The idea of data analysis therefore is to examine the meaningful and symbolic content of qualitative data.

There are various types of qualitative data analysis. However, this study utilizes content data analysis. Maree (2010) defines content analysis as the process of categorizing verbal or behavioural data to classify, summarize and tabulate the data. This research utilizes the descriptive content analysis which seeks to makes sense of the data that is there. Within this regard, content analysis will be conducted on existing literature, media coverage, Newspaper articles, Television shows; online media education from cyber security portals and specific YouTube channels will be researched (Bachman & Schutt, 2008: 16). The channels that will be analysed will be:

1. ABC news – American Broadcasting Company;
2. ABC Action News;
3. CBC News – Canadian Broadcasting Centre;
4. HLN – Headline News – United States,
5. KXLY - Washington,
6. WXII – United States,
7. The fifth Estate – Canadian News Network,
8. WPRI – Rhode Island, USA,
9. WXYZ - Detroit, USA,
10. WESH 2 News – Florida, USA.

Qualitative content analysis is categorised under the descriptive design that this study intends to follow. The analysis of contextual data will be conducted. According to Vaismoradi, Jones, Turunen & Snelgrove (2016), the ability of the researcher to generate ideas and themes depends on the immersion of data. This is obtained through careful reading, recurring items or ideas and key issues (Maree, 2010).

The characteristics of the cyber stalker and the type of study that was conducted will be analyzed. The researcher will seek out explicit and implicit ideas that are available in the literature through reflexivity. Due to qualitative research being complex in nature, the researcher needs to take cognizance of the researchers own reasons for conducting the study. A reflective journal will be kept in order to prevent a flawed biased study. The researcher needs to have a sense of openness and flexibility to data that is gathered is obtained (Watt, 2007).

The researcher will adopt these steps in the analysis of data as identified by Terre Blanche, Durheim & Painter (2006):

Step 1: Data collection and organisation.
Step 2: Study the collected data.
Step 3: Inducing categories and themes.
Step 4: Coding.
Step 5: Data is interpreted.
Step 6: Interpretation and checking.

4.6 Ethical Considerations

Ethical considerations or ethical issues play a significant part in any research. This is because these issues give credibility and dependability of the information gathered. Due to the study being a content analysis of existing data in the public domain, general ethical considerations of informed consent, confidentiality, non-maleficence and beneficence do not apply. This is because there are no participants that the researcher will interview. However, as this is a qualitative study, the researcher need to be aware of bringing the researchers own frame of reference into the study, and the interpretation of the data.

4.7 Limitations of the Study

Babbie (2010) argues that limitations of the study are those characteristics of the research design or methodology that have an impact on the interpretation of the findings within the research. The basic limitation of this study includes the use of secondary sources of data collection as the only collection method. Furthermore, another limitation of the study includes the tabulating and making sense of vast data collected through secondary sources. This process is time consuming and has the ability of leaving some information.

4.8 Conclusion

The research methodology is an important, a vital part of the research project. By abiding to the research ethics from the institute, this chapter presented on the research methods, approaches and determinants utilised within the study. The study utilises qualitative research methods for they help ensure a content analysis on cyberstalking is effectively conducted. Qualitative research methods were used within this study for they help present a perspective that qualitative forms can utilise to gather relevant and related information. The descriptive research design was also utilised within the study for it helps understand the nature of the research problem. Ideally, a research design presents the blueprint and design of the actual study. The study also utilised secondary sources of data collection thus no interviews or focus group discussions were conducted. The study therefore utilised content analysis as a data analysis method. The study also presented on the limitations of the study, and through accepting these limitations, only a study can be reliable.

CHAPTER FIVE

RESEARCH FINDINGS AND ANALYSIS

5.1 Introduction

The previous chapter detailed on the research methodology utilised within this study. The study due to the nature of the research utilises qualitative research in which secondary sources of data collection will be utilised as a data collection instrument. This chapter therefore presents the findings and further analyses and discusses on those findings. The findings are in turn related to the objectives of the study to empirically achieve the aim of the study. The study is premised on cyberstalking: A content analysis of gender based offenses committed online, therefore content analysis will be utilised as a data analysis tool. Content analysis is the process of categorizing verbal or behavioural data to classify, summarize and tabulate the data, thus this will be used in relation to the research objectives of the study. The study therefore collected, sorted and compared relevant information in order to come up with a summary relating to the study.

Since the study utilised content analysis, the following stages were utilised to understand the research problem:

- **Identifying data sources**

The study identified relevant and up-to-date data sources in relation to the research problem. The data sources were identified through a comprehensive and systematic way. According to Creswell (2014), data within a content analysis need to be transformed into written text before analysis can start. In doing a content analysis, the data reviewed was in reference to the research questions. The following channels were therefore identified as the data sources:

- ABC news – American Broadcasting Company;
- ABC Action News;
- CBC News – Canadian Broadcasting Centre;
- HLN – Headline News – United States,

- KXLY - Washington,
- WXII – United States,
- The fifth Estate – Canadian News Network, WPRI – Rhode Island, USA,
- WXYZ - Detroit, USA,
- WESH 2 News – Florida, USA.

By identifying data sources, the study therefore determined on the information to be used within the study

- **Categorising and coding the information**

After data sources were identified, the study therefore categorised and coded the information gathered. As stipulated by Babbie (2010), categories and a coding scheme can be derived from three sources: the data, previous related studies, and theories. Within this regard, the categories and codes were derived from the relevant literature visited as the secondary sources of data. Since the study utilised qualitative research methods, the coded themes were developed inductively. In ensuring the consistency of coding, the study developed a coding manual, which consists of category names, definitions and rules for assigning codes, and examples

- **Assess reliability**

Reliability is of paramount importance and the study ensured that where there was disagreement in information, reliability was put into effect. This was done after the coding of the entire data set. This was done because it is not safe within any research to assume thus there was need to ensure that the whole corpus of text was also consistent. Furthermore, the study assessed reliability for the researcher understood that the categories and coding rules may change subtly over the time, which may lead to greater inconsistency

- **Analyse results**

Based on the coding process, the study therefore analysed the results gathered and their relevance to the research study, determined. This process was enhanced through making sense of the collected themes and categories identified within the research. The study therefore presented inferences and presented reconstructions of meanings derived from the data. In analysing the results, the study ensured that there was the identification and discussion of the relationship between variables within the study as presented by the categories and the testing of categories against the full range of data.

5.2 Presentation and Analysis on the Research Findings

The following is a presentation of the content analysis on the findings of the research. This will be presented in relation to the research objectives for easy comprehension. The steps used in data analysis in this study included data reduction during which data were selected and focused, and clarified to develop coding categories. Coding categories were refined and defined as the researcher interacted with the data. As presented above, the study followed a critical content analysis path in which sources of data were identified, data was coded and categorised into themes, reliability was ensured and an analysis on the data was conducted.

5.2.1 Objective One: The prevalence of cybercrime

The turn of the new millennium has seen a lot of people increasingly using the internet and its related sources. However, the use of the internet has also come with the increased prevalence of cybercrime.

According Zaharia (2019), information from the Imperva Cyber threat Defence Report shows that Spain has the highest rate of cybercrimes reported at 93.7%. South Africa has been placed 7th on the list out of 17 countries coming in at 80.9% for general cybercrimes that were reported. South Africa was placed 5th on the list of ransomware crimes for having 66% reported however Spain was placed 4th and was in tie with South Africa. Ransomware was reported to have declined since 2017 however cryptojacking has begun taking over. The cybercriminals infect the user's

computer with malware and use their processing power to mine cyptocurrency. An example of cryptocurrency is Bitcoin. According to Internet Security Threat Report (Symantec 2019) almost 700 million people In 21 countries have experienced some type of cybercrime. Within the gathered information in relation to the research question, various definitions, historical development, impact and ways to combat cybercrime were gathered. A content analysis of these aspects follows in the next paragraphs.

5.2.1.1 Understanding of cybercrime

According to Verdegem, Teerlinck and Vermote (2015), cybercrime is an "umbrella term to describe different online threats such as mal-ware, scams and hacking. Within this regard, cybercrime is any criminal act dealing with computers, networks and smartphones. Additionally, cyber-crime also includes traditional crimes conducted through the internet "(Blackwell, 2018). Under the "Cybercrime Act 2001 in Australia, the term cybercrime is defined as crimes that target computer data and systems." Accordingly, the "UAE Federal Law No 2 of 2006 on The Preventive of Information Technology Crimes" define cybercrime as computer related crimes including aspects such as forgery, fraud, money laundering, bullying and others that are a threat to the religion and the society at large. The USA Department of Justice further defines cybercrime as computer crimes that include viruses, worms and other facets that infringe on the proper use for network systems. Of importance to note is that cybercrimes are interpreted differently according to a country. However, this study adopts the understanding of cybercrimes as including crimes involving the computer and internet.

Blackwell (2018) further understands that the common types of cybercrime within the South African perspective include: "

- Ransom ware
- Hacking
- Identity theft
- Phishing scams
- Electronic funds transfer fraud

- Online child sexual abuse (child pornography)
- Cyber-bullying
- Cyber-Impersonation
- Social Media profile cloning”

From the articles that were reviewed, it was gathered that the most common forms of cybercrime are hacking and identity theft. This is because identity theft for example ensures that one utilising all the stolen information from the victim and exploit it towards their advantage. Furthermore, on hacking, a vast number of accounts have been hacked and information stolen and all this have been exacerbated by the increase in the use of technology. Within this regard, cybercrime can be understood as including aspects such as web hacking and malicious software such as computer worms and viruses.

5.2.1.2 Historical development of Cybercrime

Ghosh and Turrini (2010) argue that the first known virus for a personal computer was traced back to 1980 but the idea of cybercrime became more relevant in 1999 when the Melissa virus began to infect millions of computers in the USA. However, the most documented genesis of cybercrime can be alluded to the disseminated denial-of-service attacks in early 2000 that brought down E-commerce sites in the United States and Europe, including Internet notables Yahoo!, Amazon.com, and eBay (Liptack, 2017). From then onwards, the prevalence of cybercrime has spun across borders and has affected all communities.

In the UK in 2016, the Office for National Statistics produced a report outlining that there were rampant increase in cybercrime within the country. It outlines that:

> *“The inclusion of 5.8 million fraud and other online offences in official statistics for the first time meant there were 12.1 million crimes in England and Wales up to the end of March 2016. The previous official annual total was 6.3 million.”*

This figure as reported by the Office for National Statistics (2016) meant that within the UK, every one in 10 people is becoming a victim of fraud or cyber offending.

According to Verdegem et al (2015), in 2010, the German Federal Police reported that there were 59,839 cybercrimes in Germany, up 20% from 50,254 in 2009.

Furthermore, in 2017, cybercrime reached new statures with the ransomware attack "WannaCry" for example infecting more than 200,000 computers in approximately 150 countries with more than 10,000 organizations being affected (Liptak, 2017). WannaCry was not the only major ransomware attack, Equifax, one of the largest credit agencies, suffered a cyber-security breach where cybercriminals accessed full names, addresses and highly sensitive information like social security numbers. It took Equifax more than five months to report the hack that compromised the personal information of more than 143 million people (Lynley, 2017). Cybercrime is not however affecting developed countries as this crime has also been reported in a number of cases within developing countries.

According to Blackwell (2018), the number of South Africans that have had access to the internet through internet devices such as laptops, PC, tablets and smartphones totalled to 36 million in 2017. Of this increased internet users, 19.6% reported cybercrime in 2017 alone and the law enforcement agencies gathered that 48.8% of the perpetrators were locals (Blackwell, 2018). This shows that cybercrime has not been perpetrated by outside criminals but has been utilised by locals as well. From the above statistics presented, the nature of cybercrime is that all societal classes and areas across the world are all prone to cybercrime.

5.2.1.3 The Impact of Cybercrime

Individuals, business organisations and even governmental institutes have all been affected by the increasing rise of cybercrime. Potential economic loss is the major impact of cybercrime. According to Coleman (2011), within the US for example, over 74 million people were victims of cybercrime in 2010 alone. These acts of cybercrime resulted in the direct losses of $32 billion (Coleman, 2011). This economic impact of cybercrime has further been exacerbated by the fact that contemporary businesses have increasingly become dependent on computer networks in storing and preserving information. Hancock (2012) argues that cybercrime impact on the economy of countries because the reliance on the internet exposes all systems to

threats posed by cyber-criminals. Aspects such as stock trade, bank transactions, purchases and other processes are done online and if these processes are tempered with, the economy can be adversely affected.

Cybercrime has also wide and diverse societal effects. Cyber-bullying is amongst the impact of cybercrime. As stipulated by Blackwell (2018), cyber-bullying entails the continuous harassing nature of personal bullying in cyberspace. However, not everyone bodily assaulted, but rather psychologically harassed and tormented. The aim of cyber-bullying therefore is to display the power and command of the perpetrator over the casualty or victim, as well as to disgrace and humiliate the victim. Another social impact of cybercrime is cyber-pornography where in recent years there has been an increase in progeny pornography on the internet, usually engaging those less than 18 years of age (Hancock, 2012). Generally, the increase of the internet has helped a new and expansive kind of bullying and has been directed to the expansion of progeny pornography. Therefore, various websites have become repositories of related to sex explicit images of young children, where the pictures are acquired and traded. This has damaged social phenomenon thus a societal impact of cybercrime.

Within this regard, economic and societal impacts are the major effects of cybercrime. On an economic level, cybercrime affect the monetary, banking and market value all of which have diverse effect on the economy of a state. Furthermore, cybercrime has become a threat to societal values as there has been a prevalence of social misconduct such as child pornography as well as cyber-bullying. This is indeed affecting human life as victims are living in fear and at times this is leading to distress and suicide.

5.2.1.4 Ways of Combating Cybercrime

Cybercrime has affected every society and every nation and it has taken both an individual and collective action by countries to combat this phenomenon. Since cybercrime came into effect with the dawn of the new millennium according to Ghosh and Turrini (2010), there have been different legislations, conventions and treaties

within countries across the globe in trying to combat cybercrime. According to Dobos (2016):

> *"Legislation determines what actions are deemed cybercrimes, how such actions should be investigated and what penal measures should be taken. International conventions and other intergovernmental agreements are an important way of coordinating the various sets of rules. They are also essential to facilitating cooperation between the police and prosecuting authorities in different countries."*

Within this regard, the most important international convention that has occurred in combating cybercrime is the "Council of Europe's Convention on Cybercrime adopted in 2001" which establishes a comprehensive set of rules for the formulation of national regulatory policies on cybercrime in relation to substantive and procedural law. In 2005, the United Nations (UN) conducted a workshop in trying to combat computer related crime in which the results of the workshop were that the UN should assist in fighting cybercrime in as much as there should be collaboration between local law enforcement authorities and the UN. The UN also initiated the International Telecommunications Union (ITU) where member countries were given the framework for a more established framework in fighting cybercrimes (Dobos, 2016). However, the ITU is facing challenges of the evolved nature of cybercrime thereby limiting on the success rate in combating cybercrime.

Various countries have also stipulated on legislation in a bid to combat computer related crime. In the USA for example, the Computer Fraud and Abuse Act of 1986 rests as the main legal instrument combating cybercrime. The Act was amended after the deadly 2001 terrorist attacks and it is relevantly amended to suit the prevailing cybercrime environment (Kshetri, 2006). Within the UK system, there has been legislation to combat cybercrime. The Data Protection Act was introduced in 1984 which stipulated on how computer data should be gathered, utilised and disposed (Sukhai, 2014). The Computer Misuse Act of 1990 was further enacted to define the law, procedures and penalties surrounding the unlawful use of computers. The UK is argued to be one of the first countries to enact laws to fight cybercrime.

The prevalence of cybercrime has also led to enactment of various laws and legislation within the South African perspective. Laws such as the Electronic Communications and Transactions Act, the Domestic Violence Act and the Protection from Harassment Act have all been legislated to detail with cybercrime. However, a detailed analysis on these laws will be discussed under the research objective number four. Of importance however is to note that both the international and domestic sphere has come up with laws to fight cybercrime.

5.2.2 Objective Two: To determine on gender based offenses committed online and document the strategies implemented in eradicating gender-based offenses in South Africa

Cyberstalking is one of the forms of cybercrime which has become prevalent within the 21st century. The effective use of internet by various people and the increasing use of social media networks have led to the increase of cyberstalking. Within this section, the main objective of the study which is to determine the gender-based offenses committed online and how these offenses have been combated will be discussed in detail as gathered from relevant secondary sources. This section will however present firstly on the nature and understanding of cyberstalking.

5.2.2.1 Nature and understanding of cyberstalking

According to Sissing (2016), cyberstalking is presently in its early stages but the occurrence and frequency of cyberstalking is expected to increase as the Internet continues enlist new users. There is no universal understanding of what cyberstalking entails for various scholars define the concept in accordance with their research context. According to Sheridan and Grant (2007), cyberstalking is:

> *"The inappropriate, unwanted social exchange behaviours initiated by a perpetrator via online or wireless communication technology and devices. Cyberstalking therefore includes the use of the Internet, e-mail, and other electronic communication devices to stalk another person."*

According to Merschman (2001), there are various forms of cyberstalking that differentiate the phenomenon from traditional stalking. Amongst these forms include sending threatening or obscene electronic emails, harassing in chat rooms, spamming, tracing another person's computer and internet activity, and posting threatening or harassing messages on blogs or through social media.

Cyberstalking is different from traditional stalking in a number of ways. Firstly Sheridan and Grant (2007) argue that cyberstalking is not limited by distance for the perpetrator can be from anywhere in the country or the world. Secondly, the internet can be utilised as the medium for stalking (Merschman, 2001). Furthermore, the use of the internet is a likely factor which limits the effort that the perpetrator must put to effect cyberstalking. For instance, the traditional stalker would have to follow the victim around but this is not the case within cyberstalking as the perpetrator can commit the crime without following the victim around (Sissing, 2016).

It is imperative to note the fact that cyberstalking entails the use of computer systems to cause distress on the victim. Cyberstalking is not limited to boundaries and as stipulated by Blackwell (2018), 48% of cybercrimes committed in South Africa in 2017 were caused by domestic perpetrators. This shows that 52%, which a considerable number was conducted by international perpetrators. Cyberstalking can be understood to be effected by persons close to the victims, particularly those they were in intimate relationships with. This is because the use and target of personal information refers to the idea that at one point, the perpetrator had access to their confidential files. Therefore, today, cyberstalking has gained relevant attention from both local and international spheres.

5.2.2.2 Gender based offenses committed online

As established in the previous section, perpetrators of cyber stalking once had an intimate relationship with the victim (Sissing, 2016). Sissing (2016) further argues that a study on gender-based cyber stalking found that “over half (54 %) of the cases cyber stalking involved a first encounter in a real world setting.” Generally, across all national boundaries and without exception, women and girls generally subjected to deliberate forms of violence based on their gender. These acts of violence are not

limited to dehumanising, aggressive and harmful acts that lead to either physical, psychological sexual, and exploitative abuse. According to Rima (2015), the turn of the new millennium came with the widespread use of the internet which has evidently led to the new breed of crime against women including gender based violence committed online.

According to a research by the Pew Research Centre (2015) in the United States, it was discovered that that women especially young women aged 18-24, had inexplicably experienced severe types of cyber harassment, namely cyberstalking and online sexual harassment. Data that was extracted from the "2014 FRA survey shows that 77% of women whom have experienced cyber harassment have also experienced at least one form of sexual or/and physical violence from an intimate partner; and 7 in 10 women (70 %) who have experienced cyber stalking have also experienced at least one form of physical or/and sexual violence from an intimate partner (Burney, 2009)." Rima (2015) therefore argues that there a number of types of gender based violence caused online. Amongst these offences include:

- **Hate speech**

Hate speech is the most common type of gender based violence committed online. Rima (2015) argues that within the context of gender-based offences committed online, hate speech entails demeaning language that vilifies, offenses, threatens or targets women based on their identity and sexual orientation. According to Burney (2009), hate speech online entails the wild extension of hostilities online and is a wide example of how technologies with a transformative and educational potential such as the Internet also enlists opportunities and challenges; and it implies multifaceted balancing between fundamental rights and principles of individual users, including freedom of expression and the defence of human dignity. Hate speech therefore rests as one of the forms of violence committed online.

A considerable number of women amounting to 77% of who have experienced gender based violence online have at one point in time, suffered from cyberstalking (Burney, 2009). Within this regard, cyberstalking, hate speech and cyber-harassment is also another form of gender based violence committed online.

- **Cyber Harassment**

Another form of gender-based offence faced by women online is cyber harassment. There is no one way to define and understand cyber harassment faced by women online but this study gathered that it includes aspects such as unwanted sexual or explicit contact online, inappropriate advances on social network platforms, threats for sexual violence committed online. As stipulated by UNESCO (2015), cyber harassment also known as "violent online behaviour ranges from online harassment and public shaming to the desire to inflict physical harm including sexual assaults, murders and induced suicides. " Cyber harassment therefore limits women rights to free and unrestricted participation of online activities, freedom of expression and the right to safety and to privacy. These are basic human rights which are being infringed upon.

5.2.2.3 Strategies implemented to eradicate gender-based offenses committed online in South Africa

There are a number of ways that can be identified to be curbing gender-based violence committed online. Following is a discussion on these factors.

- **Raising awareness**

Before there is an inclusion of policies and frameworks to counter gender based violence committed online, there is need to have an awareness that gender based offence is a real phenomenon. Recently there has been a spate of articles in magazines trying to create awareness in all types of cybercrimes. Articles have different sections and topics that are published. Articles are not limited to academia, but have been in wide array of magazines, for example, Pick and Pay – Fresh living, Sanlam life, Good Housekeeping and many others.

The South African government in relation with other national governments, civil society organisations and various stakeholders are therefore raising awareness on this phenomenon. There has been a consensus that just like global efforts to raise awareness against physical gender based violence, there is the need to raise awareness and protect women rights online too.

- **Setting up and supporting peer-support networks**

The most effective way of eradicating gender based offences committed online includes the setting up and supporting of peer-support networks. According to Rima (2015), in South Africa, there has the development of education programmes and education in technical solutions that need to be implemented that can control abusive behaviour is an appropriate role for online industry.

- **Industry regulations**

Industry regulations in combating cyber based offences against women have been implemented and human rights activists have largely applauded these measures. Of importance to note is that these industry regulations are not only South African related but covers a wide range of clauses.

Certain application have guidelines for users to follow,; YouTube advises users to 'use "YouTube without fear of being subjected to malicious harassment." However, in cases where an individual has been subjected to harassment into a malicious attack, it can be reported and removed. Blackwell (2018) stipulates that in April 2015, Twitter announced that a new filter would be introduced that would prevent users from seeing threatening messages. In an attempt to curb abusive messages, Instagram has a feature to report the message or picture, Twitter introduced temporary suspensions for accounts that fall foul of its policies. Facebook and Whatsapp, social media applications that people utilise to communicate with one another, however places the burden on the users to refrain from abusive and malicious use of these social platforms, but however, a majority of cases of gender based violence are prevalent within these platforms (Blackwell, 2018). Feminists and radical human rights activists therefore advocate for strict punishment and rules to limit the use of these social platforms in a bid to protect the rights and freedom of women.

5.2.3 Objective Three: To identify the motivations of cyberstalking perpetrators

The previous section documented and analysed on the nature of gender based violence committed online and how to combat those crimes. Of importance is to understand the reasons why cyber stalkers conduct these crimes. The motivations of

cyber stalkers therefore focus on illustrating why the stalking behaviour is performed. Based on the various stalking motivations listed in the relevant studies (Bocij, 2004; Bocij et al., 2002; Bocij & McFarlane, 2002; Bocij & McFarlane, 2003) and the many behaviours, this study summarize and reclassify the stalking motivations into four groups. These are

- To fulfil cyber stalkers' psychological needs, wishes, or cravings regarding another person
- To instil fear in or obtain control over a victim
- To seek revenge, vengeance or punishment of the victim
- To build any sort of relationship with the victim thereafter progressing to their desired outcome.

5.2.3.1 The need to fulfil cyber stalkers' psychological needs, wishes, or cravings regarding another person

The first category on the motivations of cyber stalkers includes the need to fulfil the psychological needs, wishes, or cravings regarding the victim on the part of the perpetrator. As stipulated by Bocij (2004), cyber stalkers possess in their capabilities an innate curiosity about another individual and they possess feelings of wanting to ridicule or vent out their bad mood gratuitously onto that individual. Bocij and McFarlane (2003) also identify the motivations of this group of stalkers as predatory in nature as cyber stalkers stalk for information gathering purposes or fantasy rehearsal in preparation for a sexual attack.

As stipulated by Blackwell (2018), this group of cyber stalkers can be split into two sub-groups. The first group is the one of ex-intimates who was predominantly ex-partners or ex-acquaintances of the cyber stalker, amongst this category are infatuates who individuals who were looking for intimate partner relationships. Ex-intimates present a combination of behaviours ranging from messages aimed at restoring their relationship to threats on their former significant other or friend, and the harassment often starts online (Blackwell, 2018). Impersonating their ex-partner or ex-acquaintance online is amongst the behaviours of this group of stalkers and in some instances, there are cases of the stalker buying goods via credit card

transactions. Of importance to note is that this group of cyber stalkers are only online related and studies have never reported cases of offline stalking within this nature.

The other sub-group within this classification of cyber stalkers is the infatuates. According to Mullen et al (1999), this group is motivated by the need to form a closer partnership with the victim. Mullen et al (1999) further highlights that the nature of their communication with the victim is much more intimate than the former sub-group, but when they were rebuffed their messages were more threatening. In a detailed analysis of this group of cyber stalkers, their motivations are the need to be relevant in the life of the victim and their harassment is limited online.

5.2.3.2 The need to instil fear in or gain control over a victim

Another group of cyber stalkers as identified by Bocij (2004) are those motivated with the need to instil fear and gain control over the victim. Bocij et al., (2002) also argue that this group of stalkers are also called resentful stalkers for they live on harassing their victims with the specific intention of causing fear and apprehension out of a desire for retribution for some actual or supposed injury or humiliation. In most cases, these cyber stalkers would have been in a relationship with the victim and that relationship ended in terms of which the perpetrator feels uncomfortable with.

Issuing of threats is a major component within this group of cyber stalkers. Bocij (2004) further highlight that their actions are aimed at causing constant annoyance and irritation to their victims. This group of cyber stalkers are motivated by the traditional definition of cyberstalking which is to instil fear on the victim and a continuous harassment of the victim through the use of online technology. This comes from the definition of cyber stalking according to Mullen et al (1999) which entails:

> *"The repeated use of the Internet, email, or related digital electronic communications devices to annoy, alarm, or threaten a specific individual or group of individuals."*

Within this regard, cyber stalkers are motivated by the use of technology in a bid to threaten and instil fear on the victim. The use of the internet is used since there is a high probability of anonymous and identity protection.

5.2.3.3 The need to seek revenge or punish the victim

Bocij et al. (2002) is of the view that there is a group of cyber stalkers motivated with the need to seek revenge or punish the victim. Ideally, this group of stalkers are usually a result from negative emotions toward the victim, such as anger and jealousy. Mullen et al (1999) argues that this group of cyber stalkers are mostly rejected lovers or family members and resort to stalking as a means of getting back to their victims. Bocij (2004) is of the view that on occasional basis, the victim may be a close friend or family member and views the termination of the relationship as unacceptable, incomprehensible and display signs of longing towards that individual. Their behaviour therefore is characterised by a mixture of revenge and desire for reconciliation.

Furthermore, Bocij and McFarlane (2003) argue that this group of cyber stalkers are also motivated with the desire of being vindictive. In some texts, this group is called vindictive stalkers and the name is constructed from their ferocity to which they victimise those whom they pursue. Blackwell (2018) argues that the behaviour of cyber stalkers who seek revenge often precede to offline stalking. Radebe (2010) highlights that this group of cyber stalkers have in their possession have a medium to high levels of computer literacy and therefore utilise the widest range of ICT methods to harass their target. Examples of revenge seeking cyberstalking include spamming, mail bombing, identity theft, revenge porn to mention just but a few.

5.2.3.4 The need to build a relationship with the victim

Some cyber stalkers are motivated with the need to build a relationship with the victim. Mullen et al (1999) refer to this group of stalkers as hopeless suitors for they tend to pursue and attempt to develop relationships but they fail to abide by social silent rules governing courtship. They are usually intellectually limited and/or socially incompetent on behaviours that should be displayed online and the acceptance of certain behaviours, and therefore resort to cyberstalking as a means to build a relationship with the victim. To Bocij et al (2002), this group is motivated by the need to 'win' the feelings and gain the attention of their victims. The method of cyberstalking utilised within this group of people is through the use of e-mail, Web

discussion groups, and electronic dating sites. Inherent within their behaviour is a demonstration of a detailed knowledge about victims (Bocij, 2004).

Of importance to note is that Pittaro (2007:188) sanctions that literature does often identify a link between cyberstalking behaviour and psychological mental health issues. This may late develop and lead into various psychopathological conditions, including paranoid, suspicious and delusional maladies. It is apparent that there are many motives as to the reason why cyberstalking may transpire. It is vital to acknowledge that these reasons are specific to individual cases, regardless of repeated patterns may be identified.

5.2.4 Objective Four: To identify any cyber law legislations that has been implemented within South Africa

In a bid to counter cyberstalking and gender based violence committed online, South Africa has enacted various legislation to combat this prevailing phenomenon. Amongst the laws enacted include:

5.2.4.1 The Electronic Communications and Transactions Act

The major cyber law that has been legislated within South Africa is the “Electronic Communications and Transactions Act 25 of 2002 (Guide to the ECT Act, 2005)” that was drafted into South African law on 30 August 2002. As stipulated by Sissing (2006), the principle enshrining the promulgation of this Act was the need by the government to establish a formal structure that would define, outline and regulate e-commerce within South Africa. “The Electronic Communications Act and the Transactions Act” therefore have a direct impact to any illegal unlawful actions that may be associated with electronic communications, data messages and transactions online. Furthermore, the Act has a jurisdiction in electronic communications such as text messages (sms), emails, and internet communications and even on phone and digital camera communications. As stipulated by Ballard (2015), the Communications Act serves as a legal instrument guiding the use of e-commerce.

Since this study seeks to understand cyber stalking against women, the Act is of paramount importance for it contains profound definitions of various words and

phrases relevant for the purposes of discussions within this study. Following, is a discussion on these phrases as propounded within the Act.

- **Automated transaction**

According to the Act, this means “an electronic transaction conducted or performed, in whole or in part, by means of data messages in which the conduct or data messages of one or both parties are not reviewed by a natural person in the ordinary course of such natural person’s business or employment”.

- **Data**

“The Act stipulates that data entails electronic representations of information in any form. Within this regard, data can be understood as an online process where application can get access to information in many forms or format. The concept and understanding of data also entails definitions on online data which refers to the practice of storing electronic data with a third party service accessed via the Internet. It is an alternative to traditional local storage (such as disk or tape drives) and portable storage (such as optical media or flash drives).”

- **Data message**

“Data message as stipulated within the Act refers to data generated sent, received or stored by electronic means and includes voice, where the voice is used in an automated transaction; and a stored record. Ideally, data message relates to information generated, sent, received or stored by electronic, magnetic, optical or similar means, including, but not limited to, electronic data interchange, electronic mail, telegram, telex or telecopy. “

- **E-mail**

“Within the Act, electronic mail, a data message used or intended to be used as a mail message between the originator and addressee in an electronic communication. In other words, an E-mail entails the exchange of computer-stored messages by telecommunication. E-mail messages are usually encoded in ASCII text. This text comes in the form of texts and numbers. However, you can also send non-text files, such as graphic images and sound files, as attachments sent in binary streams.”

- **Electronic communication**

This refers to a communication by means of data messages. Electronic communication is a broad term that encircles all kinds of computer-mediated communication in which individuals exchange messages with others, either individually or in groups. Electronic communication therefore relates to communication by advanced technologies

- **Information system**

"The Act stipulates that information system means a system for generating, sending, receiving, storing, displaying or otherwise processing data messages and includes the Internet. An information system therefore is the information and communication technology (ICT) that an organization uses, and also the way in which people interact with this technology in support of business processes."

- **Internet**

Internet ideally refers to the interconnected system of networks that connects computers around the world using TCP/IP (a suite of communication protocols used to interconnect network devices on the internet) and includes future versions thereof;

The notion of cybercrime within the South African perspective is introduced within "Chapter XIII of the Act. Sections 85 to 89 of the Act introduce statutory criminal offences relating to information systems and it includes:

- unauthorised access to data;
- interception of or interference with data;
- computer-related extortion;
- fraud; and
- forgery."

For example, "Section 86 (Government Gazette No. 29474, 14 December 2006) regulates unauthorised access to, interception of or interference with data as follows:

Unauthorised access to, interception of or interference with data

(1) Subject to the Interception and Monitoring Prohibition Act, 1992 (Act No. 127 of 1992), a person who intentionally accesses or intercepts any data without authority or permission to do so, is guilty of an offence.

(2) A person who intentionally and without authority to do so, interferes with data in a way which causes such data to be modified, destroyed or otherwise rendered ineffective, is guilty of an offence.

(3) A person who unlawfully produces, sells, offers to sell, procures for use, designs, adapts for use, distributes or possesses any device, including a computer program or a component, which is designed primarily to overcome security measures for the protection of data, or performs any of those acts with regard to a password, access code or any other similar kind of data with the intent to unlawfully utilise such item to contravene this section, is guilty of an offence.

(4) A person who utilises any device or computer program mentioned in subsection (3) in order to unlawfully overcome security measures designed to protect such data or access thereto, is guilty of an offence.

(5) A person who commits any act described in this section with the intent to interfere with access to an information system so as to constitute a denial, including a partial denial, of service to legitimate users is guilty of an offence."

In Chapter XII and XIII of the ECT Act, (Guide to the ECT Act, 2005) provisions are made for cyber inspectors and cybercrime respectively. This shows that the government is serious in combating cybercrime. Inspectors therefore are equipped with the right to search and seize property if there is reasonable conviction that cybercrime has been committed. Activists have also applauded for the role of inspectors as in recent times; they have assisted the police in combating cybercrime.

The Act is the major step within the South African perspective to fight against cybercrime in all its forms. Firstly, the Act is relevant for it makes it an offence to those people who hack or have unauthorised access to someone's data. Furthermore, the Act challenges computer-related extortion. Fraud, unlawful financial gain, forgery all fall under this Act. In addition, the Act states that "any person assisting another in the performance of any of the above crimes will be guilty as an

accessory." The penalties involved in these kinds of transgressions indicative of the type of crime may be from a fine to imprisonment for a period not exceeding six months (Electronics Communication and Transactions Act 25 of 2002).

5.2.4.2 The Domestic Violence Act

Relevant within this study and integral in combating gender based offences committed online is the "Domestic Violence Act 116 of 1998." The rationale for this Act is to combat domestic violence in all its forms. Sissing (2016) argues that the Domestic Violence Act was propounded after there was a rise in gender based violence in all forms and that this phenomenon was discovered to be an evil against the society. Victims of domestic violence are seen as vulnerable members of society under this act. "The Act is strictly based on the South African Constitution, 1996 which offers the right to equality, freedom and security (Domestic Violence Act (Republic of South Africa, Domestic Violence Act 116 of 1998)."

As stipulated within the Act, domestic relationship entails a situation where two people share a relationship in various ways. Amongst the ways of the relationship includes marriage, living together, Co-parenting in joint custody, family members, dating, engaged or any intimate or sexual relationship. Relevant within gender based offences committed online is the fact that the Act postulates that domestic violence encompasses various abuses such as "physical, sexual, economic, emotional, psychological, or intimidation, harassment and stalking." The Act is all-encompassing in protecting the rights of victims of domestic violence. This act goes as far and beyond in including cyber harassment and stalking as a serious offence against society. However, the downfall of this act is that, the Act is only suitable for individuals who are or were in a domestic relationship with the accused. The disadvantage is that it makes no allowances for victims of cyberstalking committed by a stranger.

5.2.4.3 Protection from Harassment Act

Relevant within the study is the Protection from Harassment Act 17 of 2011 which was promulgated in a bid to address harassment and stalking occurrences where the

cyber stalker and victim do not any relationship whatsoever. As stipulated by Blackwell (2018), the Act is more of a restructuring of the Domestic Violence Act, addressing the weaknesses of such an Act. The ideal that the Protection from Harassment Act includes harassment from persons not in a relationship with, it protects women against all forms of stalking, whether traditional or online.

“In terms of Section 1 of Act 17 of 2011, "harassment" means directly or indirectly engaging in conduct that the respondent knows or ought to know. In terms of the same section, "harm" is defined as any mental, psychological, physical or economic harm. "Sexual harassment" in turn is defined as any:

> *(a) Unwelcome sexual attention from a person who knows or ought reasonably to know that such attention is unwelcome;*
>
> *(b) Unwelcome explicit or implicit behaviour, suggestions, messages or remarks of a sexual nature that have the effect of offending, intimidating or humiliating the complainant or a related person in circumstances, which a reasonable person having regard to all the circumstances would have anticipated that the complainant or related person would be offended, humiliated or intimidated;*
>
> *(c) Implied or expressed promise of reward for complying with a sexually oriented request; or*
>
> *(d) Implied or expressed threat of reprisal or actual reprisal for refusal to comply with a sexually oriented request.”*

As conveyed by Radebe (2010), the Act intends on dealing with stalking by means of an immediate, quick and inexpensive civil remedy in the form of a protection order. Section 1(2) of the Protection from Harassment Act states that:

> *This Act does not prevent a person who may apply for relief against harassment or stalking in terms of the Domestic Violence Act, 1998 (Act No. 116 of 1998), from applying for relief in terms of this Act*

This clause stipulates that cyberstalking has become to be understood as a crime and there are avenues to seek relief against this crime. Of importance to note is the

fact that this Act identifies the gap left by other forms of legislation in detailing with cyber stalking. In bridging that gap, the Act therefore makes provisions for cyberstalking: making it a criminal offence. This is a development in fighting against gender based offences committed online as a victim of cyberstalking can now apply for a court order against the perpetrator even if the latter is a stranger. The South African Police Service (SAPS) are also ordered by the court to help track the cyber stalker and bring them to book. Perpetrators of cyberstalking can be persecuted if found guilty of the act. Within this regard, this Act is a step forward in combating cyberstalking within South Africa.

5.3 Conclusion

This chapter presented and discussed the findings of the study gathered from relevant secondary sources of information. The study is premised on cyberstalking: A content analysis of gender based offenses committed online; therefore a content analysis on relevant sources of information was conducted to detail on the research problem. The chapter detailed on the prevalence of cybercrime in the contemporary times and the study gathered that the increased use of the internet and the evolving nature of the internet is nurturing cybercrime into higher levels. Cyber bullying, identity theft, revenge pornography and cyberstalking are amongst the forms of cybercrime within the 21st century.

The chapter also detailed on the nature of gender based offences committed online in which harassment, hate speech and cyberstalking are the major forms that women are exposed to on the internet. There is therefore the need to raise awareness in combating gender based offences committed online. Cyber stalkers are motivated by a number of reasons and amongst these include instilling fear, threatening the victims and gaining control over the victim. The South African perspective has therefore seen the documentation of legislation such as the Communication Act and the Domestic Violence Act in a bid to counter cybercrime, cyberstalking and gender based violence committed online. Chapter six therefore follows and present a summary of the findings, a final conclusion, and recommendations.

CHAPTER SIX

FINDINGS, CONCLUSION AND RECOMMENDATIONS

6.1 Introduction

The previous chapter presented on the findings and made a comprehensive analysis and discussion on the findings of the research. This chapter builds from that chapter and presents a summary on the findings and relates these findings to the research objectives. Furthermore, this chapter presents on the recommendations and conclusions pertaining to the study: Cyberstalking: A content analysis of gender based offenses committed online. The aim of the study was to critically understand the nature of cyberstalking and gender based offences committed online within South Africa. The study was therefore motivated by the increased number of gender based offences committed online thus the need for relevant authorities and various stakeholders to come up with laws and legislation to counter this phenomenon.

The study was guided by the following objectives:

- To briefly document the prevalence of cybercrime.
- To determine on gender based offenses committed online and document the strategies implemented in eradicating gender-based offenses in South Africa.
- To identify the motivations of cyber stalking perpetrators
- To identify any cyber law legislations that has been implemented.

6.2 Summary of the Findings

Following is a presentation on the summary of the findings gathered within the research. The summary of findings is presented from the related information gathered from the findings within the study which was arrived at through a content analysis on articles that detail on cyberstalking, gender based offences committed online.

6.2.1 The prevalence of cybercrime

The study gathered that the 21st century has come up with the increased use of technology and this has been welcomed by cyber stalkers for it has exacerbated cyberstalking. Cybercrime can be understood as an overall universal term to describe different online threats such as mal-ware, scams and hacking. Within this regard, cybercrime is any criminal act dealing with computers, networks and smartphones. In its form, cybercrime has wide and diverse impact on an individual, community and a country as a whole. From a broad perspective, the study gathered that cybercrime impact on the economy. This is because a number of world systems are now reliant on the internet for purchasing, stocking and trading and an attack on these systems has wide and diverse effects on the economy. On an individual and society level, the study gathered that cybercrime impacts on the way of life. Effects such as child pornography, sexual harassment all are evils within a society which impacts on the way of life.

The study also gathered that both the domestic and international community has reacted to cybercrime and there has been a promulgation of various laws, legislations and norms in a bid to counter cybercrime. For example, the UN, the EU and other international and regional bodies have all come up with legislation such as Council of Europe's Convention on Cybercrime adopted in 2001 and the 2005 International Telecommunications Union (ITU) by the UN, laws which establishes a comprehensive set of rules for the formulation of national regulatory policies on cybercrime in relation to substantive and procedural law. Various countries have also stipulated on legislation in a bid to combat computer related crime, South Africa included.

6.2.2 Gender based offenses committed online and the strategies implemented in eradicating gender-based offenses in South Africa

The study gathered that cyberstalking has grown considerably within the contemporary environment. Cyberstalking entails the inappropriate, unwanted social exchange behaviours initiated by a perpetrator via online or wireless communication technology and devices. Forms of cyberstalking includes sending threatening or

obscene electronic emails, harassing in chat rooms, spamming, tracing another person's computer and internet activity, and posting threatening or harassing messages on blogs or through social media.

Gender based offences have considerably increased online. The study gathered that women (particularly young women aged 18-24) disproportionately experience severe types of cyber harassment, namely cyberstalking and online sexual harassment. Women and girls generally subjected to deliberate forms of violence based on their gender. These acts of violence are not limited to dehumanising, aggressive and harmful acts that lead to either physical, psychological sexual, and exploitative abuse. Forms of gender based offences come in the form of hate speech, sexual harassment online and cyberstalking. The study also gathered that of the women who have suffered from gender based offences committed online, over half (54 %) of the cases of cyberstalking involved a first encounter in a real world setting.

There are a number of ways which have been documented to deal with cybercrime. The first one is through raising awareness on gender based violence, both online and offline. The study gathered that before there is an inclusion of policies and frameworks to counter gender based violence committed online, there is need to have an awareness that gender based offence is a real phenomenon. There is also the need of setting up and supporting peer-support networks for the eradicating gender based offences committed online. Furthermore, there have been industry regulations such as punishment from using Twitter, Instagram and YouTube if found to be offensive. However, there is still need for social media platforms to enhance the continued fight against gender based violence committed online.

6.2.3 Motivations for Cyberstalking

The study also detailed on the motivations for cyberstalking. The motivations of cyber stalkers therefore focus on illustrating why the stalking behaviour is performed. The study therefore identified four distinct categories of what motivates cyberstalking. The first category on the motivations of cyber stalkers includes the need to fulfil the psychological needs, wishes, or cravings regarding the victim on the part of the perpetrator. The motivations of this group of stalkers as predatory in

nature as cyber stalkers stalk for information gathering purposes or fantasy rehearsal in preparation for a sexual attack. The second group includes those who are motivated by the need to instil fear and gain control over the victim. This group of cyber stalkers group of stalkers are also called resentful stalkers for they live on harassing their victims with the specific intention of causing fear and apprehension out of a desire for retribution for some actual or supposed injury or humiliation.

The third group of cyber stalkers are those motivated with the need to seek revenge or punish the victim. Ideally, this group of stalkers are usually a result from negative emotions toward the victim, such as anger and jealousy and this group of cyber stalkers are mostly rejected lovers or family members and resort to stalking as a means of getting back to their victims. The last group of cyber stalkers are those motivated by the need to build a relationship with the victim. These cyber stalkers are usually intellectually limited and/or socially incompetent and resort to cyberstalking as a means to build a relationship with the victim.

6.2.4 Cyber law legislations that have been implemented within South Africa

The study gathered that South Africa has passed on laws and regulations in combating cybercrime and cyber stalking. The most celebrated legislation is “the Electronic Communications and Transactions Act 25 of 2002 (ECT Act) “(Smit, 2015) that was drafted into South African law on 30 August 2002. The Act is the major step within the South African perspective to fight against cybercrime in all its forms. Firstly, the Act is relevant for it makes it an offence to those people who hack or have unauthorised access to someone’s data, it challenges computer-related extortion such as fraud and forgery and the Act states that any person assisting another in the performance of any of the above crimes will be guilty as an accessory. The Act also aids assists cyber inspectors the powers of seizure and investigation over electronic devices (Smit, 2015).

The study also gathered that the “Domestic Violence Act” is a relevant piece of legislation that documents on gender based violence and offences. “The Act is based on the South African Constitution, 1996 which offers the right to equality, freedom and security. The Act goes as far as including cyber harassment and

stalking as a serious misdemeanour against society. However, the Act is only suitable for people who are or were in a domestic relationship with the accused. It makes no allowances for victims of cyber stalking perpetrated by a stranger. To bridge the shortcomings of the Domestic Violence Act, the Protection from Harassment Act 17 of 2011 which was promulgated in a bid to address harassment and stalking incidences whereby the assailant and victim do not have a domestic relationship is of vital importance. The Act therefore makes provisions for cyber stalking: making it a criminal offence. “

6.3 Recommendations

The study gathered the following recommendations:

6.3.1 Need to raise awareness on gender based offences committed online

The study recommends that there is need to raise continued awareness on the impact and effects of gender based offences committed online. The conventional wisdom is that gender based violence is an evil in a society and is only relating to physical, psychological and other forms of harm against women in relationships. What of cyberstalking and other forms of gender based offences committed online? The study therefore recommends that the community at large need to be taught on the ills and evils of hate speech, cyberstalking and cyber bullying as well as harassment against women online. There is need for the community to instil a sense of respect and dignity as well as acceptance on the choice of life lived by women and respect that choice. There is also need to make sure that the punishment for gender based violence is more the same with the convictions on gender based offences committed online.

6.3.2 Increased role of international institutions in combating gender based violence committed online

There is the need for increased roles of international organisations in combating gender based offences committed online. The United Nations for example should maximise its influential role as an organisations maintaining international peace and security by also leading the fight against cyberstalking in all its forms. In 2016, for

example, the “United Nations Human Rights Council passed a resolution on the protection and promotion of online freedom as a human right; a watershed moment in the on-going struggle for universal access to the internet.” There is therefore the need for countries to adopt such laws and procedures so as to influence the fight against such a phenomenon and the UN can play an increasing part within this initiative. The UN has helped craft policies such as the Convention on the Elimination on all forms of Discrimination against Women (CEDAW) which have gone a further step in combating gender based offences; therefore there is the need to create a more influential policy combating gender based offences committed online.

6.3.3 Role of the government and various stakeholders in South Africa

The study also recommends that the government in South Africa in partnership with civil society and various stakeholders have a role in public awareness and education on informing women of their legal rights and how to implementation of them, while making ensuring that general society understands the serious consequences of online abuse. These stakeholders should therefore make it imperative that abuse policies are clear, transparent and easy to find, with clear and consistent measures for redress.

6.3.4 Accountability

The study recommends that there is need for enforced accountability on the part of service providers and the government in combating gender based offences committed online. Telecommunications companies and technology firms are always competitive and should position themselves as consumers’ main points of access to the internet, new forms of alliance and teamwork across sectors need to emerge. Within this regard, a multi-sectorial approach to address online offences that are carried out against females of all ages is essential for the mitigation of this ever increasing phenomenon. The amount of females entering the online world is ever increasing, it is imperative to create a safe that is more conducive productive for their self-actualisation needs. Network providers and the government therefore need to work hand in hand in ensuring that perpetrators of this crime are apprehended and in some cases brought to book. In business, profitability is the key but there is also the

need for enhancing the safety and satisfaction of consumers, and the safety and satisfaction of women online is essential.

6.4 Conclusion

Cyberstalking has increasingly expanded within the 21st Century. Even though studies have been conducted, documenting on the phenomenon, the discourse has not received the widespread attention it should have. There is dearth of information on the forms, types and also ways to combat this increasing phenomenon. Individuals, the community, the governments and the international community at large have a role to play in determining the impact and effects of cyberstalking as well as in combating this crime. The collective action is all but necessary to ensure online safety of persons across all political and social divide.

Cyberstalking entails the inappropriate, unwanted social exchange behaviours initiated by a perpetrator via online or wireless communication technology and devices. Forms of cyberstalking includes sending threatening or obscene electronic emails, harassing in chat rooms, spamming, tracing another person's computer and internet activity, and posting threatening or harassing messages on blogs or through social media.

Gender based offences have considerably increased online. Young women aged 18-24 disproportionately experience severe types of cyber harassment, namely cyberstalking and online sexual harassment. One in three women who frequents the internet is prone to gender based offences committed online and this is an alarming rate of such a crime. Of importance to note is that of all the women who have suffered from gender based offences committed online, over half (54 %) of the cases of cyberstalking involved a first encounter in a real world setting. There is therefore the need to counter gender based violence both online and offline. There is need to come up with effective legislation both nationally and internationally to counter this ever increasing challenge to societal security.

REFERENCES

Acheson, J. 2002. Rational choice, Culture Change, and Fisheries Management in the Gulf of Maine. *Research in Economic Anthropology,* 21: 133–159.

A Current Affair, 2019. *Surfboard company owners turn amateur sleuth after $17k scam,* Nine Digital Pty Ltd. Available from: http://www.9news.au/article/67e99603-fc23-4fa4-be49-dad244f89769 (Accessed on 23 June 2019).

Agosto, D. E., Forte, A., & Magee, R. 2012. *Cyberbullying and Teens, What YA Librarians Can Do to Help,* Young Adult Library Services. 39-43.

Anderson, W. L. 2010. Cyber Stalking (Cyber Bullying - Proof and Punishment). Insights into a changing world. Journal, 12. ISSN 1550-1574.

Anon. 2016. Cyber bullying and Stalking guide. [Online] Available from: http://cyberbullyingandstalkingguide.com/the-difference-between-cyber-bullying-and-cyber-stalking/ (Accessed 16 March 2016).

Anon, n.d. *Cyber Crime: A conceptual and Theoretical Framework.* [Online] Available from: shodhganga.inflibnet.ac.in>bitstream. (Accessed 16 May 2016).

Babbie, L. 2010. *Qualitative and Quantitative Research Methods*. Chicago: Chicago University Press.

Bachman, R. & Schutt, R. K. 2008. *Fundamentals of Research in Criminology and Criminal Justice.* S.I : Sage Publications.

Baum, K., Catalano, S., Rand, M., & Rose, K. 2009. *Stalking victimization in the United States.* Washington, D.C: U.S. Department of Justice.

Beng, T. 2004. *Introduction to Research*, Chicago: Chicago Press.

Blackwell, T. 2018. *Social Impact of Cybercrime.* Available Online from: https://www.ukessays.com/essays/media/looking-at-the-social-impacts-of_-cyber-crime-media-essay.php (Accessed on 11 March 2019).

Bocij, P. 2004. *Cyber stalking: Harassment in the Internet Age and how to Protect your Family*, Wesport : Praeger.

Bocij, P. 2005. Reactive Stalking: A New Perspective on Victimization. *The British Journal of Forensic Practice*, 7(1): 23-45.

Bocij, P. & McFarlane, L. 2003. Seven Fallacies about Cyber Stalking. *Prison Service Journal,* 149(1): 37-42.

Bocij, P. & McFarlane, L. 2002. Cyber Stalking: Genuine Problem or Public Hysteria? *Prison Services Journal*, 140(1): 32-35.

Boon, J. & Sheridan, L. 2002. *Stalking and Psychosexual Obsession. Psychological Perspectives for Prevention, Policing and Treatment.* UK: John Wiley & Sons.

Bouma, G.D. & Atkinson, G.B.J. 1995. *A Handbook of Social Science Research: A Comprehensive and Practical Guide for Students.* Oxford: Oxford University Press.

Bransen, J. 2001. Rational Choice Organisational Theory, *International Encyclopaedia of the Social & Behavioral Sciences*, Vol. 12(19).

Brookman, F., Maguire, M., Pierpoint, H. & Bennett, T. 2010. *Handbook on Crime*, London: Willan.

Burney, E. 2009. *Making People Behave: Anti-Social Behaviour. Politics and Policy*, Chicago: Routledge.

Cambridge Dictionary. (n.d). Available from: https://dictionary.cambridge.org/dictionary/english (Accessed on 15 May 2019).

Campbell, M. A. 2005. Cyber bullying: An old Problem in a New Guise? *Australian Journal of Guidance and Counselling,* 15: 68-76.

Chik, W. 2008. Harassment through the Digital Medium A Cross-Jurisdictional Comparative Analysis on the Law on Cyberstalking. *Journal of International Commercial Law and Technology,* 3(1). 13-44.

Cohen, L. E., & Felson, M. 1976. Social Change and crime rate trends. *American Sociological Review,* 44, 588-605.

Coleman, K, G. 2011. *Cyber Intelligence: The Huge Economic Impact of Cyber Crime.* Available from: http://gov.aol.com/2011/09/19/cyber-intelligence-the-huge-economic-impact-of-cyber-crime/ (Accessed on 23 February 2019).

Collin, P., Rahilly, K., Richardson, I. & Third, A. 2011. *The benefits of Social networking services: A literature review,* Melbourne: Cooperative Research for Young People, Technology and Wellbeing.

Cornish, J. 2010. *The Rational Choice Perspective.* Chicago: Chicago Press.

Cramer, T. 2014. *Would you quit social media if you could?.* Available from: http://www.econtentmag.com. (Accessed on 29 April 2016).

Creswell, J. W. 2014. *Research Design, Qualitative, Quantitative, and Mixed Methods Approaches.* Los Angeles: Sage Publications.

Davis, L. 2005. In L. Davis and R. Snyman. (2005). *Victimology in South Africa*. Pretoria: Van Schaik.

Dobos, E. 2016. How can we combat Cybercrime? *Journal on Science Nordic*, Vol. 5 (21).

DreBing, H., Bailer, J., Anders, A., Wagner, H., & Gallas, C. 2012. *Cyberstalking in a large sample of social network users: Prevalence, Characteristics, and Impact upon Victims.* Cyberpsychology, Behavior and Social Networking, V14 (2).

Duggan, M. 2014. *Pew Research Centre*. [Online] Available from: http://www.pewinternet.org/2014/10/22/online-harassment/ (Accessed on 22 March 2016).

Early, J. R. 2010. *Cyber-bullying on Increase*. Available from: http://www.tmcnet.com/usubmit/ (Accessed on 13 February 2019).

Eterovic-Soric, B., Choo, R., Ashman, A & Mubarak, S. 2017. Stalking the stalkers – detecting and deterring stalking behaviors using technology: A review, *Journal on Security and Technology*, 70: 278-289.

Fattah, A. 1991. Victimology: Past, Present and Future. *Criminologie,* 33 (1), 17-46.

Finkelhor, D. 2014. Commentary: Cause for Alarm? Youth and internet risk research – a commentary on Livingstone and Smith. *Journal of Child Psychology and Psychiatry,* 55 (6), 655-658.

Flick, U. 2014. *Introducing Research Methodology, A Beginner's Guide to Doing Research Project*. London: Sage Publications 85-93.

Ghasem, Z., Frommholz, I., & Maple, C. 2015. *A machine learning framework to detect and document text-based cyberstalking.* CEUR Workshop Proceedings. 1458. 348-355.

Ghosh, S. & Turrini, E. 2010. *A Multidisciplinary Analysis*. Berlin Heidelberg: Springer-Verlag.

Goldsworthy, T., Crowley, J., & Raj, M. 2015. *The conversation. Available from:* http://theconversation.com/revenge-porn-is-just-one-part-of-a-changing-picture-of-harassment-43703 (Accessed 16 02 2016).

Gulf News 2012. *Full text of UAE deccress on combating cybercrimes.* Available from:https://gulfnews.com/uae/government/full-text-of-uae-decree-on-combating-cyber-crimes-1.1104040.

Hancock, B. 2002. Security Crisis Management: The Basics, *Computers and Security*. 21(5): 397-401.

Hill, S. 2010. *Social networking websites encourage stalking.* Available from: http:cyberpaths.blogspot.com (Accessed 04 March 2018).

Hindelang, M, J., Gottfredson, M. & Garofalo, J. 1978. *Victims of Personal Crime:An Empirical Foundation for a Theory of Personal Victimization,* Cambridge: Ballinger Publishing Co.

History.com Editors, 2019. *Man charged in California cyberstalking case.* A&E Television Networks. Available from: http://www.history.com/this-day-in-history/man-charged-in-california-cyberstalking-case (Accessed 24 June 2019).

Home Office, Research, Development and Statistics Directorate, BMRB, Social Research, 2008, *British Crime Survey, 2005-2006,* [data collection], UK Data Service, 9th Edition, Accessed 24 August 2019. SN: 5543.

Hutton, S. & Haantz, M. 2003. Cyber Stalking. Available Online at National White Collar Crime Center Web site: http://www.nw3c.org.195 (Accessed on 13 February 2019).

Jahankhani, H. 2011. In: Jahankhani, et al. (Eds.), *Handbook of Electronic Security and Digital Forensics*. London: World Scientific.

Jahankhani, H, Al-Nemrat, A., & Hosseinian-Far, A. 2014. Chapter 12: Cybercrime classification and characteristics. *Cyber Crime and Cyber Terrorism Investigator's Handbook.* 149-164.

Jaishankar, K. 2011. Cyber Criminology: Exploring Internet Crimes and Criminal Behaviour. *CRC Press, Taylor and Francis Group*. LLC

Jaishankar, K. 2008. Space Transition Theory of Cybercrimes, In F. Schmallager & M. Pittaro, (Eds.), *Crimes of the Internet* (pp. 283-301). Upper Saddle River, NJ: Prentice Hall.

Jenkin, C. 2015. Stalkers Go High Tech to Intimidate Victims. *Journal on Criminology*. 5 (12): 112-267.

Jensen, B. 2013. Cyber stalking: Crime, Enforcement and Personal Responsibility in the On-line World, Available from: http://www.law.ucla.edu/Classes/Archive/S96/340/cyberlaw.htm (Accessed on 04 June 2019).

Joyce, P. 2009. *Criminology and Criminal Justice: a Study Guide*. Devon: Willan Publishers.

Kaspersky, L. 2012. *Spam in April 2012: Junk Mail Gathers Pace in the US*, Available from: http://www.kaspersky.co.uk/about/news/spam/2012/Spam_in_April_2012_Junk_Mail_Gathers_Pace:in_the_US (Accessed on 13 February 2019).

King-Ries, A. 2011. *Teens, Technology, and Cyberstalking: The Domestic Violence Wave of the Future?.* Texas Journal of Women and Law. Vol. 20:2.

Kshetri, N. 2010. *The Simple Economics of Cybercrimes*, IEEE Security and Privacy. Vol. 4(1):33-39.

Lenhart, A. 2007. Cyberbullying and online teens. *Pew Internet & American Life Project.* Available from: www.pewinternet.org. (Accessed 20 July 2016).

Lenhart, A. 2009. Adults and social networking websites. *Pew Internet & American Life Project.* Available: http://www.pewinternet.org/Reports/2009/Adults-and-Social-Network-Websites.aspx. (Accessed 20 July 2016).

Liptak, A. 2017. *The WannaCry ransomware attack has spread to 150 countries*. Available from: https://www.theverge.com/2017/5/14/15637888/authorities-wannacry-ransomware-attack-spread-150-countries (Accessed on 10 March 2019).

Lipton, J. D. 2011. Combating Cyber-Victimisation. *Berkeley Technology Law Journal,* 26(1103), pp. 1104-1155.

Longman dictionary of contemporary English. 2003. 4th edition. Harlow: Longman.

Lucks, B. D. 2004. Cyberstalking: Identifying and examining electronic crime in cyberspace, *Alliant International University,* 2 (23).

Lunker, M. (manishl@india.com). 2012. *Re: Cyber Laws: A Global Perspective.*

Lynley, M. 2017. *Equifax was reportedly hacked almost five months before its first disclosed date.* Available from: https://techcrunch.com/2017/09/18/equifax-was-reportedly-hacked-almost-five-months-before-its-first-disclosed-date/ (Accessed on 10 March 2019).

Maat, S. M. 2009. Cybercrime chapter 3. *Unisa Institutional Repository.* Available from: http://www.uir.unisa.ac.za. (Accessed 06 May 2016).

Manyame, L. 2018. Are your Hands Tied when it comes to Cyber Harassment? *De Rebus*, DR 22.

Maree, J. 2010. Research on Life Design in (South) Africa: a Qualitative Analysis, *South African Journal on Psychology*. Vol. 1 (12).

Maple, C., Shart, E. & Brown, A. 2011. *Cyber stalking in the United Kingdom: An Analysis of the ECHO Pilot Survey.* Available from: https://www.beds.ac.uk/__data/assets/pdf_file/0003/83109/ECHO_Pilot_Final.pdf (Accessed on 11 March 2019).

McFarlane, L., & Bocij, P. 2003. Cyber Stalking: Defining the Invasion of Cyberspace, *Forensic Update*, 1(72), 18-22.

McVeigh, K. 2011. *The Guardian online.* [Online] Available from: http://www.theguardian.com/uk/2011/apr/08/cyberstalking-study-victims-men (Accessed 22 March 2016).

Merschman, J. 2001. The Dark Side of the Web: Cyber stalking and the Need for Contemporary Legislation, *Harvard Women's Law Journal*, 255-276.

Mohandie, K., Meloy, R., McGowan, M & Williams, M. 2006. The RECON Typology of Stalking: Reliability and Validity Based Upon a Large Sample of North American Stalkers. *Journal of Forensic Sciences,* 51 (1): 147.

Moore, R. 2012. *Cybercrime: Investigating High-Technology Computer Crime*. Abingdon, Oxon: Routledge.

Mshangi, M., Sanga, C., & Nfuka, E. N. 2014. The Rapid Growth of Cybercrimes affecting Information Systems in the Global: Is this a Myth or Reality in Tanzia?. *International Journal of Information Security Science.* Vol.3 (2). 182-199.

Mullen, P.E. 2018. Impact of stalking on victims, *Journal on Stalking Profile*, 2 (12).

Mullen, P, E and Pathé, M, Purcell, R & Stuart, G.W. 1999. A study of stalkers, *American Journal of Psychiatry*, 156, pp. 1244-1249.

Mullen, P.E., Pathé, M. & Purcell, R. 2009. *Stalkers and their Victims*, London: Cambridge University Press.

Muncie, J., Talbot, D. & Walters, R. 2010. *Crime: Local and Global.* UK: Willan Publishing.

Mustaine, E. E. & Tewksbury, R. 1999. A Routine Activity Theory Explanation for Women's Stalking Victimizations, *Violence against Women*, 5(1): 43-62.

Neuman, W. 2014. *Social Research Methods: Qualitative and Quantitative Approaches*. Essex: Pearson.

Nyast, C. 2015. *Technology-related Violence against Women: Recent Legislative Trends, Association for Progressive Communications*. Available from: https://www.genderit.org/sites/default/upload/flowresearch_cnayst_legtrend_ln.pdf (Accessed on 15 February 2019).

Office for National Statistics. 2016. Cybercrime in the UK. Available online from: https://ons.gov.uk/aboutsus/transparencyandgovernance/freedomofinformationfoi/cybercrimeintheuk (Accessed on 12 May 2019).

Parker, L. 1976. New Challenges for International Rules Against Cybercrime, *European Journal on Criminal Policy and Research*, Volume 1(10): 27-37.

Parliamentary Joint Committee of the Australian Crime Commission (PJC). 2004. *Cybercrime.* Canberra: Parliament of the Commonwealth of Australia.

Pathé, M. 2002. *Surviving Stalking*, London: Cambridge University Press.

Independent Online. 2018. *South Africans losing R2.2 billion a year to cyber attacks'*. Available from: https://www.iol.co.za/capeargus/news/south-africans-losing-r22-billion-a-year-to-cyber-attacks-15601682 (Accessed on 15 May 2019).

Petherick, W. 2007. *Cyberstalking.* Available from: http://www.crimelibrary.com/criminology/cyberstalking/ (Accessed on 12 May 2019).

Petrocelli, J. 2005. Cyber Stalking, *Law & Order,* 53(12):56-58.

Pittaro, M. L. 2007. Cyber stalking: An analysis of online harassment and intimidation. *International Journal of Cyber Criminology,* 1(2): 180-197.

Pittaro, M. L. 2011. *Cyber Stalking: Typology, Etiology and Victims*, In K. Jaishankar. 2011. Cyber Criminology: Exploring Internet Crimes and Criminal Behaviour, London: CRC Press, Taylor & Francis.

Popovac, M. & Leoschut, L. 2012. Cyber Bullying in South Africa: Impact and Responses. *Centre for Justice and Crime Prevention*: Issue No.: 13, June, pp. 1-16.

Pretoria News. 2015. *Warding Off Stalkers*. Available from: https://www.iol.co.za/pretoria-news/lifestyle/warding-off-cyber-stalkers-1823007 (Accessed on 14 February 2019).

Purcell, R., Pathe, M., & Mullen P. E. 2001. A Study of Women who Stalk, *The American Journal of Psychiatry*, 158(12): 2056-2061.

Quarmby, K. 2014. *The Guardian.* [Online] Available from: http://www.theguardian.com/books/2014/sep/26/hate-crimes-in-cyberspace-danielle-keats-citron-review. (Accessed 22 March 2016).

Radebe, J.T. 2010. *Opening remarks on the second reading debate of the Protection from Harassment Bill.* Available from: http://www.info.gov.za. (Accessed on 08 March 2019).

Reidenberg, J, R. 2006. Governing Networks and Cyberspace Rule-Making, *Emory Law Journa*l, 9 (11).

Reno, J. 1999. *1999 Report on Cyber Stalking: A New Challenge for Law Enforcement and Industry.* Available Online from United States Department of Justice Web site: http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm (Accessed on 14 February 2014).

Republic of South Africa. Department of Justice. Electronics Communication and Transactions Act 25 of 2002. Published in the *Government Gazette,* (23708) Pretoria: Government Printer.

Republic Of South Africa. Department of Justice. Protection from Harassment Act 17 of 2011. Published in the *Government Gazette,* (34818). Cape Town: Government Printer.

Reyns, B. W. 2010. *Being pursued online: Extent and nature of cyber stalking victimisation from a lifestyle/routine activities perspective,* Cincinnati: University of Cincinnati.

Reyns, B. W. 2010. *A situational crime prevention approach to cyberstalking victimization: Preventive tactics for Internet users and online place managers.* Crime Prevention and Community Safety, Vol. 12(2), 99-118.

Rima, A. 2015. *End violence: Women's rights and safety online. From impunity to justice: Improving corporate policies to end technology-related violence against women.* Available from: http://www.genderit.org/sites/default/upload/flow_corporate_policies_formatted_final.pdf (Accessed on 12 March 2019).

Roberts, L. 2008. *Cyber-Victimisation in Australia: Extent, Impact on Individuals and Responses.* Briefing Paper No.6. Conducted by the Tasmanian Institute of Law Enforcement Studies.

Rosenwald, M. 2004. Every Step You Take…Every Move You Make…My GPS Unit will be Watching You. *Popular Science,* 1-8. Available: http://www.markwynn.com/stalking/every-step-you-take-my gps-will-be-watching-you-2004.pdf (Accessed 23 August 2019).

Savait, J. 2014. *Case Study Number 1, DRC*. Unpublished; case study summary. Available from: https://www.genderit.org/node/4253 (Accessed on 15 February 2019).

Shackson, T. 2016. *Cyber Stalking*. Available Online at Australian Institute of Criminology Web site: http://www.aic.gov.au/publications/tandi/tandi66.html (Accessed on 14 February 2019).

Sheridan, L & Grant, T. 2007. Is cyber stalking different? *Psychology, Crime & Law*, 13 (6): 627-640.

Shimizu, A. 2013. Domestic Violence in the Digital Age. *Berkeley Journal of Gender, Law & Justice.* Vol. 28 (1).

Siegel, L. J. 2004. *Criminology: Theories, Patterns and Typologies*. California: Thomson Learning.

Siegel, L, J. 2010. *Criminology: Theories, Patterns, and Typologies*, Belmont, CA: Wadsworth/Cengage Learning.

Siegel, L. J. 2011. *Criminology: The Core.* 4th ed. Belmont: Wadsworth:Cengage Learning.

Singh, S. 2008. Anti-Social networking: Learning the art of making enemies in web 2.0. *Journal of Internet Law, 3-11.*

Sissing, S. 2016. *A Criminological Exploration of Cyber Stalking in South Africa*, a Dissertation Submitted in Accordance with the Requirements for the Degree of Masters of Arts, Unpublished.

Smit, D. M. 2015. Cyberbullying in South African and American schools: A legal comparative study. *South African Journal of Education,* Vol 35(2). 1-11.

Smoker, M. & March, E. 2017. Predicting perpetration of intimate partner cyberstalking: Gender and the Dark Tetrad. *Computers in Human Behaviour, 72. 390-396.*

South African Police Services. 2015. *South African Police Service.* [Online] Available:http://www.saps.gov.za/resource_centre/publications/statistics/crimestats/2015/crime_stats.ph (Accessed 26 May 2016).

Stalking Resource Centre. The National Center for Victims of Crime. 2009. *Social Networking sites: A bonanza for stalkers? Available from: http://www.ncvc.org (Accessed on 26 05 2017).*

State of the Phish Report. 2019. Proofpoint, Security Awareness Training. [online] Available from:http://www.wombatsecurity.com/research (Accessed 10 June 2019).

Statistics Canada. 2014. *General Social survey on Canadians' safety.* Victimization. Available from: www150.statgan.gc.ca. (Accessed 18 June 2019).

Statistica Research Department. 2013. *Distribution of cyberstalking victims in South Africa,* Figure 2.2. Available at: http://www.statistica.com. (Accessed 1 July 2018).

Spitzberg, B. H., Marshall, L., & Cupach, W. R. 2001. Obsessive Relational Intrusion, Coping, and Sexual Coercion Victimization*, Communication Reports*, 14: 19-30.

Spitzberg, B. H., & Cupach, W. R. 2007. The state of art of stalking: Taking stock of the emerging literature. *Aggression and Violent Behavior, 12, 64-86.*

Steven, J.T., Bogdan, R. & Devault, M. 2016. *Introduction to Qualitative Research Methods,* New Jersey: John Wiley & Sons.

Strauss, A. 1967. *The Discovery of Grounded Theory: Strategies for Qualitative Research,* Mill Valley, CA: Sociology Press.

Struwig, F. W. & Stead, G. B. 2013. *Research: Planning, Design and Reporting.* 2nd ed Cape Town: Pearson Education.

Suarez, K. 2014. Teenage Dating Violence: The Need for Expanded Awareness and Legislation, *82 CAL. L. REV*. 423, 430 (2014).

Sukhai, N, B. 2014. *Hacking and Cybercrimes, in Proceedings of the 1st Annual Conference on Information Security Curriculum Development,* Georgia, Kennesaw

Suler, J. 2005. *The Psychology of Cyberspace.* Available from: http://users.rider.edu/~suler/psycyber/psychspace.html (Accessed on 14 February 2019).

Symantec. 2012. *Intelligence Report:* October 2012. Available from: http://www.symantec.com/connect/blogs/symantec-intelligence-report-october-2012 (Accessed on 13 February 2019).

Symantec. 2019. *Internet Security Threat Report.* V24. Available from: https://www.symantec.com/security-center/threat-report (Accessed 20 June 2019).

Taylor, S.J., Bogdan, R. & DeVault, M. 2015. *Introduction to Qualitative Research Methods: A Guidebook and Resource*. New Jersey: John Wiley & Sons.

Telecommunication Development Sector. 2012. *Understanding Cybercrime: Phenomena, Challenges and Legal Response.* ITU Telecommunication Bureau. Available: http://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html. (Accessed 18 June 2019).

Terre Blanche, M., Durrheim, K. & Painter, D. 2006. *Research in Practice: Applied methods for the Social Sciences.* 2nd ed. Cape Town: UCT Press.

Thomas, A. 2019. *Back off: Surviving and Combating Stalking and Cyberstalking,* The Epoch Times. Available from: http://www.theepochtimes.com/back-off-surviving-and-combating-stalking-and-cyberstalking_2932790.html/amp (Accessed on 23 June 2019).

Thompson, C. 2014. *Stalkers Turn to Cell Phones to 'Textually Harass'*. Available from: http://www.msnbc.msn.com/id/29493158/ (Accessed on 14 February 2019).

Thyer, B.A. 2009. *The Handbook of Social Work Research Methods.* 2nd ed.. SAGE Publications.

Turvey, B.E. 2012. *Criminal Profiling: An Introduction to Behavioral Evidence Analysis*, London: Elsevier.

UN Broadband Comission for Digital Development. 2015. *Cyber Violence against Woman and Girls,* s.l.: UNESCO.

United Nations. 2013. *Comprehensive Study on Cybercrime Draft,* Vienna: United Nations Office on Drugs and Crime.

United States Department of Justice. 1999. *Cyberstalking: A new challenge for law enforcement and industry - A report to the attorney general to the Vice President.* Washington, D.C.: U.S. Department of Justice.

Vaismoradi, M., Jones, J., Turunen, H. & Snelgrove, S. 2016. Theme Development in Qualitative Content Analysis and Thematic Analysis. *Journal of Nursing Education and Practice,* 6(5):pp. 100-110.

Valentino-DeVries, J. 2018. Hundreds of Apps Can Empower Stalkers to track Their Victims, New York Times. Available from: http://www.nytimes.com/2018/05/19/technology/phone-apps-stalking.html (Accessed on 21 May 2019).

Van Wyk, B. 2011. Research Design and Methods Part I, Western Cape: University of the Western Cape.

Verdegem, P., Teerlinck, E. & Vermote, E. 2015. Measuring cost and impact of cybercrime in Belgium (BCC): D.3.1.1. *Risk perception monitor report (1st wave, 2015)* Ghent.

Vitelli, W. 2018. *What Is the Psychological Toll of Stalking?* (Online) Available from: https://www.psychologytoday.com/intl/blog/media-spotlight/201805/what-is-the-psychological-toll-stalking (Accessed on 13 May 2019).

Wall, D. S. 2005. *The Internet as a Conduit for Criminal Activity. In: Pattavina, A. (Ed.), Information Technology and the Criminal Justice System*. Chicago: Sage Publications.

Watt, D. 2007. *On Becoming a Qualitative Researcher: The Value of Reflexivity.* [Online] Available from: http://www.nova.edu/ssss/QR/QR12-1/watt.pdf (Accessed 21 May 2016).

Watt, N and McLean B. 2012. Celebrities and Cyberstalkers: T*he Dark Side of Fame in the Internet Age* (Online) Available from: https://abcnews.go.com/Technology/celebrities-cyberstalkers-dark-side-fame-internet-age/story?id=16741230 (Accessed on 13 May 2019).

Welsh, A. & Lavoie, J.A.A. 2012. Risky eBusiness: An Examination of Risk-taking, Online Disclosiveness, and Cyberstalking Victimization. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace,* 6(1), Article 4, doi:10.5817/CP2012-1-4.

Whitty, M.T & Johnson, A.N. 2009. *Truth, Lies and trust on the internet.* New York: Routledge.

Willard, N.E. 2006. *Educators guide to cyberbullying: Addressing the harm caused by online social cruelty. Available: www.asdk12.org/MiddleLink/AVB/bully_topics/EducatorsGuide_Cyberbullying.pdf* (Accessed 23 August 2019).

Wright, P. 2009. *Rational Choice Theories*, Boston: Harvard Press.

Wyndham, H. 2010. Protection from Harassment Bill criticised in Parliament. Available from: http://www.info.gov.za. (Accessed on 12 March 2019).

Yar, M. 2006. *Cybercrime and Society,* London: Sage Publication Ltd.

Zaharia, A. 2019. *300+ Terrifying Cybercrime and Cybersecurity Statistics and Trends [2019 Edition].* Comparitech. Available from: https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/. (Accessed on 23 June 2019).