TOWARDS A STRATEGY FOR SOCIAL MEDIA IMPLICATIONS ON HUMAN SECURITY IN NAMIBIA: CASE STUDY OF WINDHOEK

A MINI THESIS SUBMITTED IN PARTIAL FULFILMENT

OF THE REQUIRMENTS FOR THE DEGREE OF

MASTER OF ARTS IN SECURITY AND STRATEGIC STUDIES

OF

UNIVERITY OF NAMIBIA

BY

DORTEA SHIPENA

201602388

July 2020

SUPERVISOR	**Dr. T. Mude (Midland State University, Zimbabwe)**
Co-Supervisor	**Dr. F. Bhunu-Shava (Namibia University of Science And Technology)**

ABSTRACT

The study reports findings of a qualitative research study that propose a strategy for social media implications for human security in Namibia. The case study used the case study of Windhoek to determine social media implications on human security dimensions that include economic, personal, health, community, food, environmental and political threats. The study further assessed the social media crime situation, as well as types and prevalence of social media crime in Namibia., It also discussed the various challenges faced by the Namibian Police Force and the courts in dealing with cybercrimes and proposed strategies to be adopted to combat social media crimes. Studying the implications of social media is vital to ensure human security of all internet users. In phase 1, data was collected through open-ended questionnaires from 10 purposively sampled members of the public. In phase 2, data was gathered through face-to-face unstructured interviews held with 8 purposively selected respondents. The voice-recorded data was transcribed. Both phase 1 and 2 data were coded and organised in groups to create themes. Thematic Analysis was used to derive meaning out of data. Findings show that there are serious human security threats emanating from Facebook and WhatsApp usage, mostly threats to economic, personal, community and health security of individuals. The cybercrime situation is getting worse in Namibia with prevalent trends of distribution and circulation of obscene and pornographic materials, defamation of character, cyber bulling, internet fraud, hate speech and breach of privacy.

The least common is cyber terrorism. Namibia does not yet have a cyber legal framework though a draft bill has been crafted. The police currently only deals with cybercrime cases which were defined in common and statutory laws. Lack of awareness, capacity, resources, proper technology, and the transnational and anonymity nature of cybercrimes were identified as challenges faced by the Namibian Police and courts while dealing with cybercrime. Results confirmed findings by previous scholars: Wall (2011), UNODC (2013), UN (2013), Amedie (2015), Council of Europe (2015), Ajayi (2016), Adesina (2017), Dwivedi (2018), and Links (2018). A human security theory coined by UNDP (1994) was adopted to guide this study in a Namibian context. The study recommends a speedy passing and enactment of a cybercrime law, investment in both technology and capacity building of investigators and prosecutors, alongside public education to raise awareness among social media users to combat cybercrimes.

ACKNOWLEDGEMENTS

My sincere appreciation to the following people for their vast support and contribution to the success of this study: First and most important I am grateful to the Almighty God who gave me strength, courage and wisdom to complete this study. Secondly, I would like to recognise the hard work, support and commitment of my supervisors, Dr Torque Mude and Dr. Fungai Bhunu-Shava, I am forever indebted to you in many ways. You have dedicated your time and resources to the success of my study and provided me with all necessary guidance. I also commend my two role models, Grandmother, Mrs Teopolina Kafita and Godmother, Mrs Secilia Kaunongwa. They both have prayed for me throughout my study and have always told me to look up and climb the stairs toward success because nothing good comes easily. This study would not have been possible without the permission of the relevant authorities and the participation of their employees (Inspector General of the Namibian police, the Ministry of Justice and Communication Regulatory Authority of Namibia) as well as the members of the public, all participants' contribution is highly appreciated. Finally, I thank my family and friends who have understood my journey; they have given me enough time to study and some advised me well to accomplish my goal.

DEDICATION

I dedicate this thesis to my grandparents (Shaangeni Frans Mokaxwa, Teopolina Kafita, Wilhelm Valungameka Shipena and Helvi Iimene Neshuku).

DECLARATION

I, Dortea Shipena declare that “Towards a strategy for social media implications on human security in Namibia: Case study of Windhoek” is entirely my own work in content and accomplishment. All the resources I utilised in this study are acknowledged and referred to in the reference list as per the prescribed referencing system. I have not received any assistance apart from the mentoring and guidance from my supervisor, except as mentioned in the acknowledgements. I declare that the content of this thesis has never been used before for any academic qualification at any tertiary institution.

____

Signature

Date: January 2020

TABLE OF CONTENTS

Contents

LIST OF FIGURES AND TABLES

LIST OF ABBREVIATIONS AND ACRONYMS

CRAN: Communication Regulatory Authority of Namibia

HIV/AIDS: Human Immune Virus/ Acquired Immune Deficiency Syndrome

MICT: Ministry of Information Communication and Technology

MoJ: Ministry of Justice

MTC : Mobile Telecommunications Company

NAMPOL: Namibian Police Force

CHAPTER 1: INTRODUCTION

1.1. Background of the Study

Technological development proves to be one of the fastest innovations in the history of humankind. Over the past two decades, the development of modern societies has become intimately interconnected with new and increasingly sophisticated information technologies, all of which constitute a crime risk and threat in cyber-security terms. As a consequence, the re-organisation of criminal behaviour has been transformed by new technology (Minnaar, 2016). Minnaar (2014) again believes that the increasing sophistication of technologies, as well as the proliferation of internet connection devices such as notebooks, smart phones and tablets/i-pads, recourse to 'unsecured' social media sites, and the implementation of 'bring-your-own-devices' (BYOD) to work, has led to an increase in cyber security vulnerabilities. The potential of this innovation has not passed unnoticed by business, citizens and criminals. With more than 3 billion Internet users in the world and the speed with which technology brings new developments to the market, anyone connected can become a victim of cybercrime (European Cybercrime Centre, n. d).

Snell (2015) adds that since 1973, as computers became increasingly more accessible, affordable, diverse and pervasive, the nature and rate of offending via technology has evolved and grown to enormous proportions. Today technology is used to commit, not just fraud, but also theft, harassment, espionage, paedophilia, smuggling, piracy and trafficking. According to Wall (2015: 74-75), as cited in Minnaar (2016), “networked technologies have fundamentally changed and transformed online criminal behaviour. Network technologies allow one person to victimise many people simultaneously. As such cybercrime that began with Internet became a worldwide challenge mostly to law enforcement agencies. The 2010 Internet Crime Report from the Internet Crime Complaint Centre (IC3) reported that identity theft was the third highest complaint at 9.8% for 2010. Moreover, in 2010, statistics of cyber stalking victimization compiled by Who@ indicated that harassment most often originated through emails, comprising 34% of cases followed by Facebook with 16.5%. Of all cases reported, 79% escalated in some way. The top two ways in which incidents escalated were through email (28%) and Facebook (15%) (National White Collar Crime Centre, 2012).

The Namibian Crime Statistics Unit for the past five years showed an increase in certain types of crimes including murder, while new forms of cybercrimes are emerging (NAMPOL Annual Report 2012-2016). In light of this, the Namibian Police Public Relations Office report that the police received reports of videos and audios circulating on social media during the year 2012 to 2018. About 12 cases including pornography, sex extortion, cyber bullying and cyber stalking came to the attention of the police although not reported by victims. The police spokesperson stated that citizens did not want to open cases of such nature as they felt exposed and uncomfortable with legal proceedings and in most cases they did not know which case to open with the police (NAMPOL Press Release, January 2017).

Similarly, the Namibian Police Force spokesperson stated in a media briefing that the country's law-enforcement unit has noted with grave concern the recent spate of recordings, distribution and circulation of obscene, indecent and pornographic materials depicting women in graphic and explicit videos which were widely distributed on social media platforms in the country (nbc news, January 2017).

Moreover, the Ministry of Information and Communication Technology (MICT) also warned the public on creation, distribution and circulation of obscene incidents and pornographic materials, following the circulation of a video of the late Fred Savage, a 13 year old boy mauled to death by dogs in Windhoek. The MICT noted that videos of violent, sexual and hateful nature have been circulated in the past years in Namibia and as such the ministry cautioned citizens to stop circulation of such videos (MICT Press Statement, June 2015).

Such crimes were committed through social networks such as WhatsApp groups, Facebook, twitter, email, and other computer and internet devices. In light of this, Yar (2013) suggest that cybercrime should be viewed as signifying a range of illicit activities whose 'common denominator' is the central role played by networks of ICT in their commission. Therefore, the researcher focused on WhatsApp and Facebook as the most social media tools used commonly in Namibia.

The majority of countries with high usage of the Internet have now developed cyber legal frameworks to guide law enforcement agencies in dealing with cyber related crimes. ITU (2012) state that the Council of Europe Convention on cybercrime passed laws covering the erotic or pornographic materials, cybersex and child pornography in 2011. In addition, the Congress of the Philippines passed a Cybercrime Prevention Act of 2012 that provided cybercrime offenses and penalties. As such this has reduced the cybercrime and cyber security threats.

South Africa passed a Cybercrimes and Cyber security Bill in 2017 to create offences and impose penalties which have a bearing on cybercrime; to criminalise the distribution of data messages which is harmful and to provide for interim protection orders; to further regulate jurisdiction in respect of cybercrimes; to further regulate the powers to investigate cybercrimes; to further regulate aspects relating to mutual assistance in respect of the investigation of cybercrime (Republic of South African cybercrime and Cyber security Bill, 2017).

Despite the effort made by few countries such as Ghana, Senegal, Zambia and South Africa just to mention a few, the Council of Europe/Project Cybercrime Octopus 2015's overview report revealed that the current state of legislation on cybercrime and electronic evidence in Africa was not satisfactory. By April 2016, only 20% of countries seemed to have the minimum legislation in place. Thirty of the African States including Namibia did not have specific legal provisions on cybercrime and electronic evidence in force (Council of Europe, 2015).

The Namibian Constitution mandates the Namibian Police to uphold and prevent human rights violations, such as respect of human dignity and right to privacy (The Constitution of the Republic of Namibia, 1990). These are the rights most violated by cybercriminals on social media in relation to human security. Despite that mandate, internet was heavily used in Namibia and the country was among the African countries that do not have a legal framework to guide the Namibian Police and other law enforcement agencies in dealing with cybercrimes. Further, research on cybercrimes in Namibia was also at its infancy stage. Hence this study seeks to examine how the absence of a guiding cybercrime legal framework was impacting Namibian Police operations. The study was however limited to social media platforms, in particular WhatsApp and Facebook.

The study was warranted because some of the cyber social media crimes are a threat to human security. The cyber threat research done by Kaspersky Lab shows that the same channels of Internet such as communication, shopping, news, education, entertainment and work can be, and increasingly are also used by criminals, malicious attackers, terrorists and even (school) bullies and sex offender ‘stalkers’ (Kaspersky Lab (2015:1) as cited in Kader and Minnaar, 2015).

According to CHS (2003) as cited in United Nations (2009), human security means to protect the vital core of all human lives in ways that enhance human freedoms and human fulfilment. It means creating political, social, environmental, economic, military and cultural systems that together give people the building blocks of survival, livelihood and dignity” (CHS: 2003:

4). Therefore, it would be imperative for Namibia to have a legal framework and a strategy to deal with cybercrimes in order to comply with the United Nations Human Development Programme of 1994.

1.2. Statement of the Problem

The Namibian Police Crime Statistics Unit for the past five years show an increase in certain types of crimes including murder, while new forms of cybercrimes are emerging (NAMPOL Annual Report 2012-2016). The Namibian Police Force spokesperson stated in a media briefing that the country's law-enforcement unit noted with grave concern the recent spate of recordings, distribution and circulation of obscene, indecent and pornographic materials depicting women in graphic and explicit videos that were widely distributed on social media platforms in the country (nbc news, January 2017). Moreover, the Namibian Police Force is faced with challenges related to crime detection, investigation, evidence gathering and combating of online crimes. Despite that, Namibian residents heavily use the Internet for official and personal business, and the country does not have a legal cyber framework to guide the Namibian Police Force in dealing with cybercrimes. Therefore, the study will employ a human security theory to offer a strategy for the human security implications of social media crimes committed in Namibia and the challenges faced by the Namibian Police Force.

1.3. Research Questions

The main objective of the study was to propose a strategy for social media implications for human security in Namibia and this was to be achieved through answering the following questions:

1. What are the social media implications of cybercrime on human security in Namibia?

2. In the absence of a supportive legislation, what are the challenges faced by the Namibian Police Force in dealing with social media crimes that are threatening human security?

3. What strategy should NAMPOL develop to deal with cyber social media crimes?

1.4. Significance of the Study

The study would result in the development of a strategy to guide the Namibian police in dealing with cybercrimes. The study will inform the Namibian Legislative organ on the urgency to enact a cybercrimes legislation that will define cybercrime acts and regulate social media contacts. This study will serve as a reference point of cyber security and cybercrime in the academic field of security studies and it will be a source of information to all security sectors in Namibia and globally.

1.5. Limitation of the Study

This study would be a fulfilment of a mini-thesis, which limits the coverage of the study. Also, the researcher experienced the reluctance of the participants to provide information. MICT staff were busy during data collection hence the researcher could not interview them.

1.6. Delimitation of the Study

This study would be confined to cybercrimes committed in Namibia, specifically through WhatsApp and Facebook during the past five years.

CHAPTER 2: LITERATURE REVIEW

Cybercrime committed through social media presented human security threats in Namibia during the past five years. Worsening the situation was the absence of a cyber-legal framework to regulate law enforcement in dealing with social media crimes. Many studies reviewed focused on how social media could be used to disseminate security information by the police and only few studies focused on the social media implications on human security specifically on cyber bullying, hate speeches and hacking. The said studies were conducted by Law, Information Technology and Health Departments such as psychology. As such there was no record of cybercrime research conducted in Namibia from a human security perspective.

This current literature chapter presents the human security conceptual framework of the study and assesses the implications of social media crimes on human security. This study seeks to answer questions such as; what is the prevalence and types of social media crimes; and what are the challenges faced by the Namibian Police Force and courts in dealing with social media crimes? The chapter further examines the cybercrime legal framework in various states. The latter provides strategies offered by different authors to deal with cybercrimes. The main objective of this study was to offer a strategy for social media implications on human security and not national security; therefore, a human security paradigm will be adopted. The next section will outline the conceptual framework of the study.

2.1. Conceptual Framework

The main concern is how human security is impacted by social media crimes, also known as cybercrimes. It is therefore imperative for this section to present key concepts, their origin and features.

2.1.1. Human Security

Human Security is a people-centred concept. Its focus shifts from national security to protecting individuals, to respond to ordinary people's needs and dealing with sources of threats (UNDP, 1994). According to Singh (2014), the new definition of human security is the protection of the vital core of all human lives from critical and pervasive threats and situations, building on their strengths and aspirations. It also means creating systems that give people the building blocks of survival, dignity and livelihood. Adeyemi-Suenu (2014) maintains that the concept of human security underscores the desirability to preserve and protect man against activities and problems capable of exterminating him.

According to UNESCO (2008), human security has been called a 'paradigm in the making'. Certainly, ever since the concept of human security was first proposed in the UNDP (1994) Human Development Report, the concept has continued to be seen as complex, contested, and yet it has undeniably evolved to become a key term in discourse on international relations, development, security studies, in economics and the social sciences (UNESCO, 2008). Therefore, the researcher found it significant to utilise a human security approach as coined in the United Nations Human Development Report of 1994, to explore the dimensions of threat posed by social media crimes in Namibia.

The above definitions are coinciding on human-centricity, as they both express on protection of individual human beings and not the State. The researcher therefore adopted the United Nations Human Development Report of 1994’s definition to demonstrate how Namibian citizens should be protected from social media human security threats, and explain why a strategy to protect them from social media crimes was vital. As such enforcement of laws and protection of online human rights would ensure human security in Namibia and globally.

2.1.2. Social Media

The term 'social media' is a description of different ways people communicate through digital communication. This includes social networks, blogs, mobile applications and others (Navy Command Leadership Social Media Handbook, 2012:4 as cited in Turck, 2016). Kamp (2016) maintain that new media technologies have come to be generically referred to as ‘social media’ because of their ability to permit instantaneous human interactions and interconnectivity across space and time (Stein, 2006; Kaplan and Haenlein, 2010; Breuer, 2011).

Chander (2015) states that social media is a term used to describe a variety of web-based applications and mobile platforms through which users can generate and share digital contents. The digital contents could be in various forms such as text, picture, audio, video, location etc. Kaplan and Haenlein (2010: 62-64) as cited in Kamp (2016) and Nsude and Onwe (2017) classify social media into six different types, which are: collaborative projects (Wikipedia); blogs and microblogs (Twitter); content communities (YouTube); social networking sites (MySpace, Facebook, Flickr, LinkedIn, Tumblr); virtual game world (World of Warcraft); and virtual social worlds (Second Life). In the analysis of the above, Namibian residents heavily use social media tools such as Facebook, WhatsApp, Twitter, YouTube and Instagram among others. Consequently, the prevalence of cybercrime became high in recent years due to computer literacy advancement and affordability of networked devices, thereby posing threats to human security.

This study became important due to technological innovation which remains transnational in nature, allowing all states citizens including Namibian to participate on social networks. The researcher was aware that the majority of Namibian residents, Ministries, Agencies and Offices have Facebook and WhatsApp accounts where groups and pages were created to allow interaction. Nsude and Onwe (2017) and Chander (2015) concur with the researcher on the conception of Facebook as a major social media tool by stating that Facebook is the world's largest social network with over 1.4 billion members and annual revenues exceeding $12 billion. Nsude and Onwe (2017) again state that WhatsApp is another instant messaging-focused social network with over 700 million members globally. It was acquired by Facebook in February 2014 but operates as a separate entity.

It could be true that social networks offer numerous advantages to users, but equally social networks allow criminals to penetrate in cyberspace to advance personal interest. As a result, the increasing sophistication of information technology with its capacity to collect, analyse and disseminate information has posed significant cybercrime threats to social networks users. The below section presents a brief overview of cybercrime which was the core topic of this study.

2.1.3. Cybercrimes

The main question of the study was; what are the implications of social media crimes/cybercrime on human security in Namibia? Cybercrime could be summed up as crime that occurs in cyberspace. The field may also be referred to as "computer crime", "internet crime", "high tech crime", or a variety of other related names (Rosewarne, 2012). Das and Nayak (2013) adds that cybercrime was a term used to broadly describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial of service attacks.

McGuire and Dowling (2013) state that cybercrime was an umbrella term used to describe two distinct, but closely related criminal activities: cyber-dependent and cyber-enabled crimes. Smith (n. d) posits that the term cybercrime refers to a variety of crimes carried out online using the internet through computers, laptops, tablets, smart TVs, games consoles and smart phones. For the purpose of this study, the researcher adopted the definition offered by Smith since cybercrime could nowadays be committed on online social media using the internet through computers, laptops, smart TVs, and smart phones. Of course, the definitions offered by other authors were indeed valid; on the other hand they have focused more on criminal activities using computer or computer networks which may not necessarily be the case in Namibia as the majority of citizens use smart phone devices in commission of cybercrime.

The profit motive appears to be the first and major incentive that makes cybercriminals to pursue their nefarious activities of infiltration or unauthorized interference with computers and network systems (Ajayi, 2016). Choudhury, Basak and Guha (2013) postulate that the threat from cybercrime is multi-dimensional, targeting citizens, businesses, and governments at a rapidly growing rate. Cybercriminal tools pose a direct threat to security and play an increasingly important role in facilitating most forms of organized crime and terrorism. Mendoza (2017) add that three general parts that converge in the cybercrime are: *Cyber victims* (any user in cyberspace can be the victim of a criminal attack), *Cyber offenders* (individuals who, using ICT as an instrument, carry out an offense classified as a crime) and *The State* (government offices specialized in cybercrime, these entities with functions to protect Internet users in their crime prevention work, do reparation of the damage caused to the cyber victims, and pursuit of cybercriminals for prosecution). Cybercrime pose serious threats to human security, this might be the reason why the rights of Namibian residents (who are victims) need to be protected from cyber offenders by the Namibian Police Force through prevention of cybercrime and arresting offenders. Hence, it was vital to outline the human security as a paradigm and its dimensions.

2.2. Human security: The Theoretical Framework

This study is centred on human security theory. Human security could be traced to the publication of the United Nations Development Programme, Human Development Report of 1994, which identified a list of perceived new security threats, namely, economic, food, health, environment, personal, community, and political security (UNDP, 1994). Ossip (2017) concurred that the human security concept is often quoted from the 1994 United Nations Development Programme (UNDP) Human Development Report (HDR) that was the first mention of the concept. It consists of two main components: “freedom from fear” and “freedom from want”. This demonstrated the shift from national security towards human beings, where individuals either looked out for security threats concerning crime and war or concerns including hunger, poverty, disease, and natural disasters.

According to UNDP (1994), human security was relevant to people everywhere, in rich and in poor nations. The threats to their security may differ-hunger and disease in poor nations and drugs and crime in rich nations-but these threats are real and growing.

Ağır (2015, p.366) as cited in Adesina (2017) posits that human security was commonly understood as prioritising the security of people, especially their welfare and safety, rather than that of states. Adesina (2017), further states that human security concept identifies the security of human lives as the central objective of national and international security policy. UNESCO (2008) maintain that the UNDP Human Development Report considers that the emerging concerns of human security for most people all over the world today are job security, income security, health security, environmental security, security from crime, and that people's feelings of insecurity arise more from worries about daily life than from the dream of some cataclysmic world event. This current research demonstrated how social media crimes impact upon human security of people residing in Namibia. The seven dimensions of human security are discussed below.

Dimensions of Human Security

The United Nations Development Programme, Human Development Report of 1994 and some scholars defined the seven human security dimensions as follows:

Economic security: UNDP (1994) asserts that economic security requires an assured basic income, usually from productive and remunerative work, or in the last resort from some publicly financed safety net. But only about a quarter of the world's people may at present be economically secure in this sense. Singh (2014) adds that economic security refers to an individual’s enjoyment of a basic income, either through gainful employment or from a social safety net. The human security threats of economic nature could be violated through hacking of critical informational systems of individuals or stealing their identity electronically causing them economic lose.

Food security: Food security means that all people at all times have both physical and economic access to basic food. This requires not just enough food to go round. It requires that people have ready access to food, that they have an "entitlement" to food by growing it for themselves, by buying it or by taking advantage of a public food distribution system (UNTFHS, 1999). Singh (2014) adds that food security means end of hunger, malnutrition, ensuring healthy diet and life-styles, especially for vulnerable groups, ensuring availability of food entitlement with work and end of famine. Although this aspect might not be directly impacted by cybercrime, it could be linked to economic security in the sense of entitlement to food by buying it. Cybercrime could cause individuals to lose all monetary value and starve or become criminals, thus it was important to take note of the relationship between all dimensions.

Health security: This involves guaranteeing a minimum protection from disease and unhealthy lifestyle (Singh, 2014). Just the same as food security, the relationship between health and economic security was evident. People would have a better lifestyle when they have an income to sustain their daily needs such as food and medical services. Moreover, the researcher believed that personal security guarantees physical health of human beings, thus if personal security was threatened by cybercriminals, health security may as well be affected.

Environmental security: Singh (2014) maintains that environmental security means integrity of safe water, fresh air and arable land and also includes freedom from deforestation, desertification and natural disasters. In addition, UNTFHS (1999) posits that human beings rely on a healthy physical environment, curiously assuming that whatever damage they inflict on the earth, it will eventually recover.

Personal security: Singh (2014) and UNTFHS (1999) coincided that no other aspect of human security was so vital for people as their security from physical violence. The personal security threats take several forms: threats from the state (physical torture), threats from other states (war), threats from other groups of people (ethnic tension), threats from individuals or gangs against other individuals or gangs (crime, street violence), threats directed against women (rape, domestic violence) threats directed at children based on their vulnerability and dependence (child abuse) threats to self (suicide, drug use).

Community security: Singh (2014) states that community security covers the right to freedom of identity (of race, language, caste, class, ethnicity, gender, generation, religion, nationality and so forth). UNTFHS (1999) concurs with Singh that most people derive security from their membership in a group, a family, a community, an organization, a racial or ethnic group that can provide a cultural identity and a reassuring set of values. The researcher analysed the danger of social media in relation to human security, since social media could be used to advance racial, religious or ethnic interests which may result in violence and instability within communities, thereby threatening the security of residents. The Hutu and Tutsi Genocide by Hutu-led government in Rwanda in 1994 could be a good example to demonstrate the danger of ethnic unrest. Therefore, it was important to protect the security of community even in the digital world to prevent violence and ethnic war.

Political security: UNTFHS (1999) informs that one of the most important aspects of human security was that people should be able to live in a society that honours their basic human rights. Singh (2014) states that political security encompasses freedom of speech, conscience, and assembly. It also means freedom from government repression, systematic human right violation and militarization. Since this study was limited to WhatsApp and Facebook social media tools, it is obvious that individuals have somehow infringed on others' human rights by curtailing political freedoms as enshrined in article 21 of the Namibian Constitution. Therefore, it became the researcher's interest to find out what are the cybercrimes committed on social medial in Namibia in relation to political security dimension.

Ossip (2017) states that, based on the United Nations Development Programme (UNDP) Human Development Report (HDR), the seven categories in the human security paradigm discussed above involve the cyber sphere today or in the future warfare, especially personal, community, economic and political. However, this research focused more on the health, economic, community and personal human security threats as these are the major dimensions of cybercrime in Namibia. This study was aimed at designing a strategy to deal with human security threats of social media crimes in Namibia, hence the need to discuss the nexus between human rights and human security because the two are intertwined.

2.3. Human Rights and Human Security: The Nexus

Human Security complements state security, strengthens human development and enhances human rights (CHS: 2003: 2 as cited in UNTFHS, 1999). Singh

(2014) supports this observation by stating that another strategic approach to human security is respect. Respect for human security means that whatever their primary objective may be, all actors, whether institutional or corporate or individual, must ascertain that their action does not intentionally or unintentionally, threaten human security. This sense of respect has a close relationship to respect for individual human beings and their rights. This is what the study sought to address by providing a strategy for social media implications on human security, protecting the vital core of all internet users.

2.4. The Social Media Implications on Human Security

Social media crimes pose threats to human security in Namibia; therefore it would be significant to explain the implications of social media on human security. Singh (2014**)** believes that there is also a broad range of social problems. Progress in science and technology could in some aspects affect the safety of an individual. The development of a global information society could cause “future shock”, the stratification of communities with various accesses to new technologies or the creation of new categories of social exclusion and criminal acts like cybercrime.

Amedie (2015**)** demonstrates the negative impact of social media in three main categories. First, social media fosters a false sense of online “connections” and superficial friendships leading to emotional and psychological problems. The second harm of social media was that it could become easily addictive taking away family and personal time as well as diminishing interpersonal skills, leading to antisocial behaviour. Lastly, social media has become a tool for criminals, predators and terrorists enabling them to commit illegal acts. The researcher concurs with the above author, having observed that the amount of time people commit to social networking indicate a sense of addiction which impact upon their daily life activities, be it home, work or school.

Mengu and Mengu (2015) maintains that incidents of violence on social media was on increase these includes; child porn, visual material displaying, campaigns of abuse towards individuals and institutions or black propaganda, negative labelling, misdirecting people by establishing contact with fake identities (for instance, kidnapping or enslaving women and children on the pretext of employing them as well as the theft on social media (idea or money) were prevalent acts. These incidences have been reported in Namibia, although they have not been followed due to lack of legal framework.

UNODC (2013) postulates that consumer victims of cybercrime in 24 countries across the world report that they suffered average direct losses of between 50 and 850 US dollars as a result of a cybercrime incident(s) experienced in one year. Around 40 per cent of these costs were reported to consist of financial loss due to fraud, almost 20 per cent due to theft or loss, 25 per cent to repairs, and the remainder to resolving the cybercrime or other financial loss. Links (2018) adds that among a number of other speculative predictions of the costs of cybercrime, the IT security firm McAfee (a division of Intel), in collaboration with Centre for Strategic and International Studies, believe that cybercrime costs the global economy somewhere between $375 and $575 billion per year.

McGuire and Dowling (2013) state that similar proportions of men and women internet users experienced loss of money in the last year both three per cent according to the Crime Survey for England and Wales 2011/12 (ONS, 2012). McAfee Inc (2014) as cited in Adesina (2017) notes that the cost of cybercrime includes the effect of hundreds of millions of people having their personal information stolen. Morgan (2017) adds that cybercriminal activity was one of the biggest challenges that humanity would face in the next two decades. Cyber Security Ventures predicts cybercrime will cost the world in excess of $6 trillion annually by 2021. Cybercrime costs include damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, and post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm. Financial lose in Namibia was also incurred by the government, public and private institutions as well as individuals. However, there were no statistics so far due to underreporting of such acts. This research thus studied the economic implications of cybercrime.

Sinca and Mascas (2015) and Hughes (1997) as cited in Gitonga (2014) concur that social media was a new technique used by traffickers. Traffickers worked through networks and the profit generated by this business was enormous, this being a $32 billion-a year industry. Sinca and Mascas (2015) state that one of the new crimes facilitated by the digital environment and social media was grooming - a special form of harassment of minors online. By this it could meant that the pimp would take care of the minor with the purpose of prostitution. The target was girls, usually 11-12 years old, who are then sold for sex. Sinca and Mascas (2015) further express that Facebook plays an important role in the grooming of victims. Researching on human traffickers' use of social media to conduct criminal business was important considering that Namibians also heavily use social media. The study would therefore be significant in making Namibians aware of traffickers' scams. Therefore this study would educate Internet users on the dangers of social media.

According to Handley (2010) as cited in Milivojevic (2011), the issue of privacy was closely linked to a debate around vulnerability to victimisation. Facebook and other SNSs have been identified as potentially harmful spaces, particularly for young people, and in relation to sexual harassment and unwanted solicitation. Amedie (2015) maintains that many deaths, suicides, and emotional problems among youths have started several moral debates about the side effect of social media. Bullying victimization has currently been associated with an increased risk of suicidal behaviours, as well as an increased risk of mental health problems. Giving an example of one tragic case, 13- year-old Megan Meier hanged herself after being cyber-bullied on social media by Josh Evans, not a real boy, it turned out, but a false profile created by her adult neighbour (Amedie, 2015)

Pozza, Pietro, Morel and Psaila (2016) state that the increased availability of new technologies has resulted in a rise in cyber bullying cases in recent years. Victims can experience psychological maladjustment, social isolation and feelings of unsafety. In one case reported in the media across Europe, in extreme situations, cyber bullying has led to the victim's suicide or attempted suicide. According to recent data, in Europe more than 50% of children bullied online said that they became depressed as a result, and over a third of them stated that they harmed themselves or thought about suicide. Concurring on the effect of cyber bullying, Williams and Pearson (2016) maintains that cyber bullying can have significant negative effects on people's lives. Cyber bullying can result in depression, loss of confidence, fear, isolation and relationship problems, self- harming and suicide.

According to Amedie (2015), the study conducted by psychologist Dr. Mark Becker of Michigan State University found a 70% increase in self-reported depressive symptoms among the group using social media and a 42% increase in social anxiety. Clearly excessive social media usage leaves one prone to be at a higher risk of depression, anxiety, and ultimately stress. Clearly social media is inadvertently leaving youth susceptible to become overly self-conscious, anxious and ultimately depressed.

Dwivedi (2018) maintains that by posting personal information on social networking services, the user creates a hazard to personal security. For example, revealing that you would be away from home, especially if your address was posted in your profile, increases the risk that your home will be burglarized. Another study carried out in Nigeria by Asemah and Edegoh (2013) as cited in Nsude and Onwe (2017) revealed that the extent to which social media has caused insecurity in Nigeria was great, describing social media as a haven for uncensored free-wheeling discussions on everything from sexual fantasies to religious dogmas. Facebook causes insecurity more than any other Social network. Rose as cited in Punjabi (2014) warned that there are greater chances of private information becoming public, which opens users to serious security risk, as the information was easily transferred between social media sites. Barman (2015) adds that privacy was infringed when a hacker accesses a person's profile by hacking his account on a particular social networking website.

Dwivedi (2018) postulates that the technological advancements have abled non-state groups to affect powerful nations through cyber-attacks and also gathering millions of followers globally. The technology giants today remain "the order-and powerhouse networks preferred by terrorist". Social networking giants like Facebook, Twitter, Apple, Google, Microsoft, Yahoo and many other services like WhatsApp, YouTube, Instagram, Tumblr and Skype are accelerating the effects of global terrorism**.** Al-Qaida once and now the ISIS are being helped by these firms to raise funds, recruit, brainwash, train and spread their believers.

Nsude and Onwe (2017**)** added that many lives have been lost through Boko Haram insurgency. Boko Haram leaders, especially Abu Qaza, use the YouTube regularly to relay their messages. In Nigeria, Boko Haram leaders continue to use Facebook, YouTube, Twitter and other Jihadist networks to claim responsibility, celebrate success and issue threats for further attacks. Terrorist groups use chat rooms, dedicated servers and websites and social networking tools as propaganda machines, as a means of recruitment and organization, for training grounds and for significant fund raising through cybercrime.

According to Weimann Report as cited in Amedie (2015), terrorists started using the internet almost 16 years ago. After 9/11, many terrorist groups such as the Jihadist movements and al-Qaida moved to cyberspace. UN (2002) reports that the investigations that directly followed the 9/11 attacks also disclosed the use of the Internet to obtain information that could be used to plan attacks or obtain materials needed to make or improvise chemical, biological or radiological weapons.

Kamp (2016) maintains that the biggest change impacting the industry today was how consumers were getting their news. In addition to sharing news on social media, a small number of individuals were also covering the news themselves, by posting photos or videos of news events. Contributions on social media platforms are mostly not subject to journalistic standards and ethics. Due to the lack of regulations and standards, abuse in forms of spreading false information and rumors, defamation and hate speech can hardly be prevented.

Nsude and Onwe (2017) supports the above assertion, by stating that social media platforms were used to disseminate information very fast but has also become a platform for the dissemination of false reports and sometimes, these false reports spread so quickly. From the above literature, it was evident that social media crimes have impact on human security and needs to be addressed. Doing so requires an overview of the prevalence of social media crimes globally.

2.5. Prevalence of Social Media Crimes Globally

This study intends to answer the question; what is the prevalence of social media crimes in Namibia? Hence, this section presents an overview of cybercrime generally. Prevalence of criminal activity on social media sites could be difficult to determine and there were currently no comprehensive statistics on social media crimes, as such the literature lacks specific review. This could be due to a number of factors, especially considering the broad nature of social media, anonymity afforded to criminals, and relative unawareness of Internet users, which could create a ripe environment for victimization (National White Collar Crime Centre, 2011). However, the literature shows some statistical evidence of cybercrime prevalence globally.

According to Links (2018), the Norton Cyber-Crime Report reveals that, every second, 18 adults were victims of cybercrime, resulting in more than 1.5 million victims globally per day. South Africa (80 percent) has the third highest number of cybercrime victims in the world, after Russia (92 percent) and China (84 percent). Adesina (2017) adds that in Nigeria cybercrime, known as “Yahoo Yahoo” or “Yahoo Plus”, was a very popular cybercrime and a source of major concern to the country. Cybercriminals in Nigeria remain notorious for luring people across the planet into fraudulent scams via spam mails, cash-laundering e-mails, and cleverly designed but bogus company partnership offers.

Kobek (2017) posits that in 2013, Mexico held the number one position in the world for pornographic material involving minors and second place for its Internet usage. There were 1,330 websites, 116,000 web searches a day, and at least 80,000 children who were exploited. An estimated 800,000 adults and 20,000 children are trafficked for sexual exploitation, where some of the children become part of Mexico´s lucrative US$30 million a year pornography industry. According to UNODC (2013), during information gathering for cybercrime, acts involving child pornography were reported to constitute almost one third of the most commonly encountered cybercrimes for countries in Europe and the Americas.

Wong (2005) provides a statistical report of computer crimes, stating that in 1993, majority of computer crime cases (60.5%) were involved in illegal access to a computer with criminal or dishonest intent. The second most prevalent computer crime appears to be "obtaining property and service by deception" via the Internet, where 103 reported incidents of this crime constituted 17.5% of all reported computer crime cases. The third largest crime in 2003 was publication of obscene materials on the Internet at fifty-eight cases, representing 9.9% of reported crimes. Davis (2010) adds that in North Carolina the most frequently investigated computer crimes by an average reporting agency were fraud related (79.3%), criminal threatening (8.5%), and online enticement of minors/child pornography (4.9%).

Warner (2011) as cited in Barfi, Nyagorme and Yeboah (2018) identified three main forms of cybercrimes that prevailed in Ghana, namely: identity fraud, fake gold dealers and estate fraud. A research carried out in Ghana with 200 students in Sunyani Senior High School revealed that the most prevalent forms of cybercrime is hacking 20%, credit fraud 18%, identity theft 11%, pornography 10%, sweetheart swindle (social networking) 7.5%, defamation 5% and cyber stalking 3.5% among other forms.

Tushabe and Baryamureeba, (2007) informs that a study carried out in Uganda aimed at investigating whether internet users in Uganda have been victims or perpetrators of internet crimes revealed that 90% reported to have been victim of at least one cybercrime incident and twenty five percent confessed that they commit at least one wrongful act while in the cyberspace. Similarly, King and Sutton (2014) as cited in Williams and Pearson (2016) found an association between terrorist acts and a rise in hate crime incidents in the US. They show that following the 9/11 terrorist attack, law enforcement agencies recorded 481 hate crimes with a specific anti-Islamic motive, with 58 percent of these occurring within two weeks of the attack (4 percent of the at risk period of 12 months) (UN, 2013). In 2010, Ghana, long viewed as Africa’s flawless gem, had its sparkling reputation tarnished. In a report published that year, Ghana gained the unsavory distinction along with Anglophone African neighbours, Nigeria and Cameroon, as one of the top ten cybercrime generating states worldwide (Ghana and Nigeria 2010 as cited in Warner, 2011). Sources within the Ghanaian national security apparatus have delineated that three primary types of cyber-fraud are most commonly perpetrated in the country today. The most common of these is identity fraud and estate fraud.

European Union shows that a third of 18–24 year-olds and a quarter of 14–17 year-olds have been involved in sexting. This applies to almost half of young people who are sexually active (Livingstone et al. 2011 as cited in Hof & Koops, 2011).

OECD (2012) provides the cyber bullying prevalence rates across countries. High prevalence rates were noted for Australia, 6.6% from year 4 to 9 in 7 500 schools, 21% of 652 young persons aged 11-17; United States 11% of grade 6-8 ,50% of teens aged 13 to 18 were cyber bullied; Canada, 55% of student aged 12 to 15 China, 65% aged 11 to 14 United Kingdom, 22% aged 11 to 16, and Europe, Iceland with 15% of 9-16 year-olds, Estonia with 31% of 6-14 year-olds. UN (2002) informs that concerns were also expressed about the increase in identity theft, in which personal data are used to allow offenders to impersonate the individual whose data were stolen. Combined with the anonymity of online transactions and other activities, identity thefts were used in connection with a range of crimes ranging from fraud to terrorist activities.

In the analysis of the above, it was quite evident that there could be high prevalence of cybercrime worldwide. Majority of studies conducted by European, African and American States clearly demonstrate that cybercrime was indeed a burning issue. Despite that, other regions may also have trends of cybercrimes, only that few studies were conducted, therefore no much statistics to prove that cybercrime was prevalent there as in the three regions of the world cited above. Child pornography, cyber bullying, hate speech, sexting, trafficking and fraud seem to be the most prevalent crimes in general. In addition, the literature revealed that children were more vulnerable to cybercriminals than adults, more specifically to cyber bullying, sexting and trafficking for sex and pornography. This study would therefore seek to determine the prevalence and the types of social media crimes in Namibia which would be presented in the following section.

2.6. Types of Social Media Cybercrimes

This study seeks to address the types of cybercrimes committed in Namibia using social media. There are various types of cybercrimes and all cybercrime acts have varying forms, elements or features. Bhatia and Srivastava (2010) and Smith (n. d) concurs that cybercrimes fall into two categories: 1) the Computer as a target when a computer is used to attack other computers, for example hacking, virus/worm attacks and DOS attacks , and 2) the computer as a weapon when a computer is used to commit real world crimes, for example cyber terrorism, IPR violations, credit card frauds, EFT frauds, pornography et cetera. Wall (2011) also categorises cybercrimes in two, that is crimes using machines or computer-related ‘crimes which are committed using networked computers to engage with victims in order to dishonestly acquire cash, goods, or services. The other category was the crimes in the machine or computer content. These latter crimes relate to the content of computers or materials held on networked computer systems. They include the trade and distribution of pornographic materials, the dissemination of hate crime materials, and more recently, the publication of video nasties of the murders of kidnapped foreign nationals.

Prasanthi and Ishwarya (2015) indicate the different types of cybercrimes such as financial (using fake websites to market products so as to get the credit numbers), marketing strategies (selling narcotics or weapons online), Intellectual Property Software piracy (copyright infringement, trademark violations, theft of computer code), email spoofing (hacking email/password; sending unwanted messages to others ruining a person’s image) e-murder (manipulating medical records), transfer fraud (hackers intercept them and divert the funds), hate/commercial (building a website to promote hate or racial hate) and altering websites deleting web (pages, uploading new pages; controlling messages conveyed by the website).

According to Yar (2013:10) and Adesina (2017), Wall (2001a:pp.3-7) sub-divided cybercrime into four legal categories: a) *cyber-trespass* (crossing boundaries into other people's property and/or causing damage, e.g. hacking, defacement, viruses),

b) *cyber-deception and theft-* stealing (money, property), e.g. credit card fraud, intellectual property violations also referred to as piracy), c) *cyber-pornography (*breaching laws on obscenity and decency) and d) *cyber-violence (*doing) psychological harm to, or inciting physical harm against others, thereby breaching laws relating to the protection of the person, e.g. hate speech, stalking).

UN (2002) and Nfuka *et al.*, (n.d.) concur on the classification of cybercrime groups; a) *cybercrime against individuals:* harassment via e- mails, cyber-stalking, dissemination of obscene material, defamation, unauthorized control/access over computer system (hacking), indecent exposure, email spoofing, spamming, cheating and fraud. b) *cybercrime against individual property:* credit card fraud, computer vandalism, transmitting malicious code (virus/worm/trojans), unauthorized control/access over computer system (hacking), intellectual property crimes (software piracy: illegal copying of programs, distribution of copies of software, copyright infringement: trademarks violations, theft of computer source code), and internet time thefts. *c) cybercrime against organization:* denial of service, email bombing, salami attack, logic bomb, Trojan horse, data diddling, unauthorized control/access over computer system, possession of unauthorized information, distribution of pirated software and cyber terrorism against the government, organization etc., and *d)Cybercrime against society at large:* pornography (basically child pornography), polluting the youth through indecent exposure, trafficking, financial crimes, sale of illegal articles, online gambling, forgery and web jacking.

2.7. Cybercrime Legal Framework

Edappagath (2001) maintains that the term 'cyber law' in general refers to all the legal and regulatory aspects of internet. It means that anything concerned with, related to, or emanating from any legal aspects or issues concerning any activity of citizens and others in cyberspace comes within the ambit of cyber law. More specifically, cyber law can be defined as a law governing the use of computer and the internet. Namely, it focuses on a combination of state and federal statutory, decisional and administrative laws arising out of the use of Internet. Kalunde (n. d) assert that cyber-criminals around the world are constantly seeking loopholes through which to perform illegal or illicit businesses. Any country that has inadequate cyber-law could essentially be offering a safe-haven for cyber-criminals to act with impunity.

Tushabe and Baryamureeba, (2007) observes that some countries responded to the threat of cybercrimes by modifying and enacting cyber laws. Adding that Boda Mash examined the growth and development of the law related to cybercrime in the international community and divided them into nine categories: protection of privacy, protection of intellectual property, illegal and harmful contents, criminal procedural laws, computer related economic crime, unauthorized access, computer forgery, computer fraud and child pornography.

Finnan (2015) believes that while there are international efforts to help stop cybercriminals in their tracks, very little was being done in Africa to strengthen cybersecurity. Council of Europe (2015) report that 11 African States seemed to have basic substantive and procedural law provisions in place (Botswana, Cameroon, Côte d'Ivoire, Ghana, Mauritania, Mauritius, Nigeria, Senegal, Tanzania, Uganda and Zambia), although implementing regulations may still be missing in one or the other country. Meanwhile, 12 States seemed to have substantive and procedural law provisions partially in place. The sad truth could be that the majority of African States (30) did not have specific legal provisions on cybercrime and electronic evidence in force. Draft laws or amendments to existing legislation reportedly had been prepared in at least 15 States (Burkina Faso, Djibouti, Ethiopia, Guinea, Kenya, Lesotho, Mali, Morocco, Namibia, Niger, South Africa, Swaziland, Togo, Tunisia, and Zimbabwe). In some instances, bills had been presented to national parliaments; in others the fates of draft laws were uncertain.

According to Links (2018), the Namibian parliament intended to table the new Transactions and Cybercrime Bill in 2017, which was placed on the parliamentary agenda by Minister of Information and Communication Technology. However, the bill was removed from the agenda and it was unclear why it was pulled and when it would be placed back on the parliamentary agenda again. Cassim (2011) postulates that Namibia has also experienced misuse of information communication technologies (ICTs) such as identity theft and the use of pornographic images on cell phones, hence the need for such legislation. The bill, inter alia, addressed the regulation of electronic transactions, communications and information systems management, and promoted the use and development of electronic transactions and provided for incidental matters.

Although the incidence of cybercrime was low in Botswana, it was said to be increasing. Therefore, the Cyber Crime and Computer Related Crimes Act 22 of 2007 was passed in December 2007. The aim of the law was to 'combat cybercrime and computer related crime, to counteract criminal actions perpetrated through computer systems and to facilitate the collection of electronic evidence' (Cassim, 2011). Gambanga, (2016) as cited in Madondo (2017) states that in Zimbabwe the draft Computer Crime and Cybercrime Bill has attracted the most attention because it spills into how citizens use technology everyday through services like social media and sharing Wi-Fi connections. Some of the potential offences in the draft Computer Crime and Cybercrime bill are: computer-related terrorism activities, pornography, identity theft, racist/xenophobic/tribalism insults, spam, and online harassment. Elsewhere, Ndubeze (2014) states that in Nigeria the Cybercrime (Prohibition, Prevention), Act 2015 has been passed into law. The objectives of the Act were to provide an effective unified legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria.

Warner (2011) posits that in 2008 Ghana passed the Electronic Transactions Act (Act 772), which both criminalized computer hacking and gave police officers more latitude to pursue suspected cybercriminals. Kenya also enacted the Information Communications Amendment Act 2009 to combat cybercrime. These Acts deal with; inter alia, unauthorised access to computer data, access with intent to commit offence and electronic fraud among others. The enactment of the Kenyan Information Communication Amendment Act, 2009, facilitated the prosecution of cybercrime offenders (Cassim, 2011). Lastly in Africa, the South African Government passed a cybercrime and cyber security bill 2017, to define offences and impose penalties which have a bearing on cybercrime; to criminalise the distribution of data messages which is harmful (South Africa Cybercrime Bill, 2017).

Yong (n. d) states that cybercrime has caused serious damage to Chinese society and as a result China made relevant legislations on Cybercrime classified into two parts; the substantive law and procedure law. Article 287 of "Criminal Law of the People's Republic of China" and the "Decision of the Standing Committee of the National People's Congress on Ensuring the Internet Security" indicate that by using computer or internet, anyone whose conduct brings serious damage to the society and is convicted of a crime and shall be criminally responsible in accordance with the relevant criminal laws.

Brenner (2001) maintains that in the United States, there are a number of federal statutes which address varieties of cybercrimes. The framework utilized is based on the Model State Computer Crimes Code which was created by organizing state cybercrime statutes into eight categories: procedural issues; non-sexual crimes against persons; sexual crimes; crimes involving computer intrusions and damage; fraud and theft crimes; forgery crimes; gambling and other crimes against public morality; and crimes against government.

Human Security remains a global concern and cybercrime was a transnational crime requiring all states to have cyber laws to encounter the implications of such. Despite that, majority of countries, specifically in Africa, do not have cyber legal framework and that includes Namibia. However, the study was not geared to look much into legal aspects. This study shall therefore make recommendations for future research in legal aspects of cybercrime. A review of the legal status of countries with regards cybercrime is necessary because law enforcement and justice services need a legal framework to guide them in dealing with social media crimes. The following section outlines policing of cybercrimes.

2.8. Challenges for Law Enforcement Agencies

2.8.1. Technology challenge

There are several implications of socio-technological change for law enforcement organizations. The broad adoption of social media by the public and the increasing effect that this adaptation has in police work requires police organizations to define and implement strategies for social media adaptation (Denef et al., 2012 as cited in Chander, 2015). Bromby (2006) as cited in Brown (2015) states that many cybercrimes are sophisticated and well-conceived, requiring police to apply technological expertise and deductive reasoning to unravel complex 'modus operandi' and substantiate elements of an offence. However, Kubic (2001) as cited in Kader and Minnaar (2015) claims that in some cases, local police forces do not understand or cannot cope with technology. In other cases, nations simply do not have adequate laws regarding cybercrimes and are therefore limited in their ability to provide assistance. Wall (2011) also maintains that the relationship between the police and technology has been long-standing and complex. On one hand the police's responsive and localised nature always meant that they fell behind in their access to, and use of, technology. The challenge was that law enforcement agencies do not have the facilities to keep up with criminals, especially with regard to offences that require high policing.

2.8.2. Budget Constraints

Wall (2011) claims that over a century readers of the Police Review and other contemporary police journals were regularly told by police correspondents that they lacked the resources to obtain the latest technologies that would help them to respond to criminals. Keane (2016) adds that resources have not followed; nor have they been sufficient to enable proactive as well as reactive policing, or been devolved to local police forces to address low-value, high- volume cybercrime.

2.8.3. Jurisdictional / Transnational Challenge

According to Rosewarne (2012), cybercrime is borderless by nature; this also makes criminal investigations more complicated for law enforcement authorities. Choudhury, Basak and Guha (2013) believe that cybercrime is a global criminal phenomenon which blurs the traditional distinction between threats to internal and external security and does not respond to single jurisdiction approaches to policing. Snell (2015) adds that another challenge of investigating cybercrime could be that the internet has increased the reach of criminals so they can now strike from thousands of miles away. Cybercrime was often transnational with the offenders operating in a different country to that in which the victim lives and the police are working. The use of proxy servers, physical distance, international politics, and lack of legislation and national agreement to give up suspects for trial in another country, all make it difficult to investigate cybercrimes and often impossible to bring the offenders to justice.

2.8.4. Capacity Challenge

Kader and Minnaar (2015) hold that the internet presents new and significant investigatory challenges for law enforcement at all levels. These challenges include: the need to track down sophisticated users who commit unlawful acts on the internet while hiding their identities; the need for close co-ordination among law enforcement agencies; and the need for trained and well-equipped personnel to gather evidence, investigate, and prosecute these cases. UNODC (2013) believes that another challenge facing both law enforcement investigators and prosecutors mean that ‘brought to justice’ rates are low for cybercrime offenders. Majority of cases are handled by non-specialized judges, who, in many countries do not receive any form of cybercrime-related training. Kader and Minnaar (2015) add that cybercrime investigations require new rules to be followed concerning the collection and preservation of evidence. And in order to conduct these investigations successfully, investigators require significantly advanced skills. UNODC (2013); Pieterse (2015) Akuta et al (2008) as cited in Mushumba (2016) concur that in many countries, investigation of cybercrime and crimes involving electronic evidence was not well resourced and suffer from a capacity shortage. Some 70 per cent of specialized law enforcement officers in less-developed countries were reported to lack computer skills and equipment.

2.8.5. Cybercrime Reporting Challenge

According to UNODC (2013), one global private sector survey suggests that 80 per cent of individual victims of core cybercrime do not report the crime to the police. Underreporting derives from a lack of awareness of victimization and of reporting mechanisms, victim shame and embarrassment, and perceived reputation risks for corporations. Brown (2015) adds that the anonymous and faceless nature of cybercrime complicates issues associated with victimology and cybercrime reporting. There exists widespread misunderstanding among communities about the nature of cybercrime and capacity of law enforcement to apprehend offenders. Wall (2011), UNODC (2013), and Ajayi (2016) concur that the most revealing challenge is the under-reporting of cybercrimes to the police.

2.8.6. Lack of Awareness

According to Doshora (2011), one important reason that the Act of 2000 is not achieving complete success in Delhi is the lack of awareness among the citizens about their rights. Gharibi and Shaabi (2012) state that different types of cyber threats in social networks happens due to the fact that most of the users were not concerned with the importance of the personal information disclosure and thus they were under the risk of over disclosure and privacy invasions.

2.8.7. Evidence Challenge

UN (2013) maintains that evidence was the means by which facts relevant to the guilt or innocence of an individual at trial are established. Electronic evidence was all such material that exists in electronic, or digital, form. Mislan (2010) as cited in Brown (2015) believes that despite the pervasiveness of digital information, many police and prosecutors are hesitant to collect and present intangible sources of evidence. Lack of leading edge tools and shrinking budgets for procuring resources are ongoing problems. Ajayi (2016) adds that the nature of evidence, that is, forensic, needed in the prosecution of cybercrimes was expensive because of the high-tech equipment, materials and expertise involved to carry out such investigations, travelling and interpreting cost due to language barriers as opposed to gathering of evidence in terrestrial crimes.

2.8.8. International Cooperation

UNODC (2013) states that due to the volatile nature of electronic evidence, international cooperation in criminal matters in the area of cybercrime requires timely responses and the ability to request specialized investigative actions, such as preservation of computer data. Response times for formal mechanisms were reported to be of the order of months for extradition and mutual legal assistance requests, a timescale which presents challenges to the collection of volatile electronic evidence.

2.8.9. Anonymity Nature

Ajayi (2016) maintains that one of the greatest impediments against global efforts towards stemming the whirlwind of cybercrimes remains the anonymous nature of the identity of cybercriminals. In addition, Pieterse (2015) states that the challenge facing law enforcement in relation to the cybercrime phenomenon was in essence a faceless one, extremely complex to determine the true identity of a cybercrime perpetrator/identify the geographical location from where the cybercriminal operates/predict a pattern of behaviour.

2.8.10. Inadequate Legislation

The enforcement of cybercrime laws has largely been hampered due to inadequate legislations and the ineffectiveness of the same where there are extant laws in place for cybercrimes (Ajayi, 2015). Goodman and Brenner (n.d) also state that the laws of most countries do not clearly prohibit cybercrimes. Downing (2005), as cited in Brown (2015) adds that many cybercrime offenders have evaded prosecution due to weaknesses in substantive criminal laws that do not address technological means of offending.

2.8.11. Models and/or Strategies Challenge

Kader and Minnaar (2015) state that the current models pertaining to the investigation of crimes in cyberspace concentrate on only specific components of the investigation process and deal mostly with the technical aspects of the investigation of crimes that take place in cyberspace. Traditional law enforcement tools, methodologies and disciplines do not successfully address the detection, investigation and prosecution of cybercrime.

2.9. Strategies of combating cybercrimes

According to UNODC (2013), many countries of the UN study framed responses related to cybercrime prevention within the overall context of the need for a national cybercrime strategy. In return, many countries also highlighted the strong links between cybercrime and cyber security strategies. Therefore, different authors offered the following strategies:

2.9.1. Cybercrime Awareness

The UN cybercrime surveys report that all stakeholders highlight the continued importance of public awareness-raising campaigns, including those covering emerging threats, and those targeted at specific audiences, such as children (UN, 2013). Cassim (2011) adds that it is imperative to educate the public about the threat of cybercrime as ignorance has been mooted as one of the main reasons that Africans fall victim to cybercrime. Livingstone et al. (2011) as cited in Hof and Koops (2011) suggest that stimulating digital literacy and safety skills should therefore be a primary policy objective. Similarly, one clear policy priority should be to increase levels of parental awareness in the case of those children who do encounter risks through their online activities.

2.9.2. The involvement of academia in cybercrime prevention

Academic institutions and intergovernmental organizations may prevent cybercrime, in particular through knowledge development and sharing; legislation and policy development; the development of technology and technical standards; the delivery of technical assistance; and cooperation with law enforcement authorities. Universities should house and facilitate cybercrime experts, some computer emergency response teams (CERTs), and specialized research centres (UN, 2013).

2.9.3. Legislations and policies

Seger (2012) maintains that states should adopt legislation which were harmonised with international standards in order to criminalise conduct and provide law enforcement with procedural law tools for efficient investigations. Goodman and Brenner (n. d) suggest that nations must modernize their procedural law as well as their substantive law, their law of crimes. Nations must also evaluate their procedural law governing evidence collection and analysis, and amend existing legislation as necessary.

2.9.4. Reporting cybercrime

India has established cybercrime reporting mechanism, a system that involves registering complaints with the local police stations or cybercrime cells (Ernst & Young, 2015). Mashiloane (2014) as cited in Kader and Minnaar (2015) informs that the proposed South African Police Service (SAPS) Cyber Centre will implement a cybercrime reporting mechanism for the enhancement of the public and organisational understanding of the scope, threat, trends and collation of data in order to detect pattern of organised criminality.

2.9.5. Capacity building

Cassim (2011) posits that states should introduce specialised law enforcement and training skills. There should also be continuous research and training of personnel in the security, finance, judicial and police enforcement sectors to keep abreast with evolving technology. Snell (2015) adds that the Mainstream Cybercrime training in South Africa was designed to enable all police officers and staff to be able to respond to digital crime. Training will succeed in introducing participants to online crime and increasing their confidence in using technology to investigate it.

2.9.6. Arrest and Prosecution

In the United States, a strict application of existing anti-child pornography laws has led to the criminalization of these activities. Teenagers have been arrested for taking nude pictures of themselves and texting them to classmates or putting them online (Associated Press 2008; 2009 as cited in Hof & Koops, 2011).

2.9.7. Technological development

Chander (2015) states that in India, some intelligence agencies and Mumbai Police have set up social media monitoring labs. Delhi Police is also contemplating such a cell and has floated ·expression of interest for implementation of “Open Source Intelligence (OSINT)” solution. Canadian Global Information (2014) states that police can use predictive analytics to identify suspicious activity to warn citizens not to use certain sites or close sites down before too many people fall victim. Implementing regular and frequent automated analysis of big data can help police identify unusual behaviour patterns and close down fraudulent sites more quickly.

2.9.8. Using territorial jurisdiction and international cooperation

All international or regional cybercrime instruments that contain a jurisdiction clause recognize the territorial principle, requiring state parties to exercise jurisdiction over any offence that is ‘committed’ within the state’s geographical territory, established in accordance with the instrument (UN, 2013). Choudhury *et al.*, (2013) hold that more centralized coordination at regional and interregional levels was needed to streamline the fight against cybercrime. UNODC (2013) wrote that due to the volatile nature of electronic evidence, international cooperation in cybercrime matters requires timely response and the ability to request specialized investigative actions. Formal cooperation among countries requires using bilateral instruments as the legal basis.

2.9.9. Cybercrime detection

Honey pot lures can be employed to entrap and keep an electronic criminal occupied long enough to allow for identification and even apprehension of the preparatory. These lures can be bogus system administration accounts, fictitious product or client information, or a myriad of created files that appear to contain sensitive information. In addition to facilitating perpetrator identification, honey pots also store the evidence of the electronic crime itself (Prasanthi & Ishiwary, 2015).

The application of these strategies depends on the will, resources and support of the state. All the above discussed strategies support one another. However, the citizens need to be aware of cybercrime and report it to relevant authorities and other stakeholders should be willing to fight cybercrimes. Moreover, the government should invest in technological development and capacity building to ensure that right people are dealing with the digital crime using advanced technology. The researcher agrees that each country should adopt social media policies and have adequate laws to govern internet and social media usage. Cybercrime requires jurisdictional and international cooperation at all cost and by all means because failing to do so will escalate human security threats. More importantly, internet users in Namibia need to protect themselves against cybercrime by learning online safety.

2.10. Summary of chapter 2

This chapter presented the literature review. The first section established the conceptual framework of the study, defining Human Security as a people centred concept whose focus shifts to protecting individuals, to respond to ordinary people’s needs and dealing with sources of threats. Social media was also defined as a term used to describe a variety of web-based applications and mobile platforms through which users can generate and share digital contents. Cybercrime refers to a variety of crimes carried out online using the internet through computers, laptops, tablets, smart TVs, games consoles and smart phones. This definition was adopted for this study as it clearly demonstrates the Namibian case in terms of smart phones utilisation on social media. The researcher explains the theoretical framework using human security theory which could be traced to the publication of the United Nations Development Programme, Human Development Report of 1994 (UNDP, 1994). The nexus between human security and human rights was described as very strong and the two remain inseparable. Furthermore, social media crimes have implications on human security such as economic, health, safety and privacy. The literature reveals high prevalence of cybercrime in Africa, Europe and North America. However, few studies indicate that cybercrime exist in other parts of the World such as Asia and only very few authors wrote about social media crimes and the impacts thereof. Despite lack of publications in Namibia, it remained evident through new media reports that cybercrime became a thorny issue especially that it remained unregulated.

Generally, various types of cybercrimes committed on social media were discussed, ranging from cyber terrorism, cyber bullying, hacking, child pornography, grooming, sexting, fraud, cyber stalking, identity theft and defamation and so on. Each of the type has its forms and implication on human beings. This chapter outlined the legal framework across continents and countries as well as international organisations. Based on the review, African states lacked adequate cyber legal framework and states such as Namibia do not have cyber law. Moreover, the study reviewed how law enforcement agencies police cybercrime across the globe. Cybercrime presents law enforcement and judicial services with challenges such as lack of reporting crimes. The transnational nature of cybercrime and jurisdiction made it even more difficult to combat social media crimes.

Equally, technology remained the major challenge, followed by lack of capacity and resources needed to fight cybercrime. Finally, the literature presented different strategies that could be employed to mitigate or fight cybercrime. For instance, citizen education, implementing reporting mechanisms, involving academic institutions, international cooperation and having cybercrime investigation and prevention model.

CHAPTER 3: RESEARCH METHODS

3.1. Introduction

This chapter described the research design used in this study to design a strategy for the social media implications on human security in Namibia using a case study of Windhoek. The chapter outlines the methodology of this study, including the population of the study, sampling procedure, data collection instruments, research procedures and data analysis. The chapter also discussed the ethical issues in research such as voluntary participation, anonymity and confidentiality in data collection as well as reporting.

Table 1: Table Mapping

Research Questions	Methods/Strategies /Tools
What are the social media implications on human Security in Namibia	**Method**: Qualitative **Strategy:** Case Studies **Tools**: Interview Guide and Questionnaires
In the absence of a supportive legislation what are the challenges faced by the Namibian Police Force in dealing with social media	**Method**: Qualitative **Strategy**: Case Studies **Tools**: Interview Guide and Questionnaires

crimes that are threatening human security	
What strategy should NAMPOL develop to deal with cyber social media crimes	**Method**: Qualitative **Strategy**: Case Studies **Tools:** Interview Guide and Questionnaires

3.2. Research Design

The study employs a qualitative approach. As such the researcher used an exploratory case study design. Case study is an empirical inquiry that investigates a contemporary phenomenon within its real life context, especially when the boundaries between phenomenon and context are not clearly evident (Yin, 2003). Plooy-Cilliers, Davis and Bezuidenhout (2014) state that a case study is a thick and detailed description of social phenomenon that exists within a real- world context. The case study method allows a deep exploration within natural contexts, while providing a full and thorough understanding of a particular and lived experience of a participant. An exploratory case study involves a rigorous description of the case within its broader context in an attempt to understand the nature of the case. Leedy and Ormrod (2010) maintain that qualitative research allows the researcher to describe the nature of the situation, settings and relationships, system or people. Harding (2013) states that the key aim of the qualitative researcher was to understand the perspectives of respondents.

3.3. Target Population

Population refers to the entire group of people, events, or things of interest that the researcher wishes to investigate (Sekaran, 2003). The researcher is based in Windhoek and is not a fulltime researcher. Therefore the population target of study was drawn from Windhoek due to resources and time constraints addressed in the limitations of the study. According to World Population Review (2018), Windhoek has a population of about 268 132. The participants of the study comprise of the public members, and experienced personnel from the top management of the Namibian Police Force (NAMPOL), Ministry of Justice (MoJ), Ministry of Information, Communication and Technology (MICT), Namibian Legislature and the Communication Regulatory Authority of Namibia (CRAN). The members of the public will complete the questionnaires and the rest of the participants will be interviewed.

3.4. Sampling Procedure

The researcher used a purposive sampling method. Kumar (2011) states that the primary consideration in purposive sampling is the judgement as to who can provide the best information to achieve the objective of the study. Etikan, Musa and Alkassim (2016) also agree with Kumar by stating that the purposive sampling technique is judgmental, is the deliberate choice of a participant due to the qualities the participant possesses. Furthermore, purposive sampling allows for the selection of specific instances so as to have those that will yield the most relevant and plentiful data pertinent to your topic (Yin, 2016). Therefore, no statistical formula was required to determine the sample size. The researcher used this method to select 20 participants (ten public members, three management members of NAMPOL, two officials each from MoJ, MICT, CRAN and one official from the Legislature) , because this involved identification and selection of individuals or groups of individuals that were proficient and well- informed with a phenomenon of interest (Etikan, Musa & Alkassim, 2016).

Sekaran (2003) states that in qualitative studies, only small samples of individuals, groups, or events are invariably chosen, in view of the in-depth nature of the study. It was not possible to use lager samples because it entailed huge costs and energy expenditure. For this reason, qualitative studies use small samples which allow restriction of generalizability of findings. Moreover, the researcher used saturation to justify the sample size. Bowen (2008) states that data saturation entails bringing new participants continually into the study until the data set is complete, as indicated by data replication or redundancy. In other words, saturation is reached when the researcher gathers data to the point of diminishing returns, when nothing new is being added. Therefore the researcher purposively used a samples size of 20 participants as representatives of the target population.

3.5. Data collection instruments

The researcher intended to conduct research using open-ended questionnaires and unstructured face-to-face interviews. Therefore questionnaires and unstructured interview guides/protocols and phone voice recorder was used to collect data. Kumar (2011) believes that the strength of unstructured interviews is the complete freedom in terms of the content, questions and structure. Kvale and Brinkmann (2009) as cited in Creswell (2013) maintain that one should design and use an interview protocol or guide, a form about four to five pages in length with space to write in answers, with approximately five to seven open ended questions and enough space between questions to write response to the interviewee's comments. Kumar (2011) also states that the use of a developed loose list of issues that is to be discussed with respondents is an interview guide. It allows coverage of the areas of enquiry and comparability of information across respondents.

- *Interview guide:* the unstructured interviews guide with open-ended questions was used to collect data from 10 purposively sampled key informants. The research used face-to-face, in-person interviews. Ritchie, Lewis, Nicholls and Ormston (2014), maintain that face-to-face interview provides a stronger basis for the establishment of a good rapport between the research and the participants, helping to create an environment where the interviewee can respond in a free ranging and full way and the researcher can take note of non- verbal communication.

- *Questionnaire:* Self-administered questionnaires were completed by the 10 purposively sampled members of the public while the researcher was waiting. Neuman (2000) states that the advantage of self-administered questionnaires is that the researcher can give the questionnaires directly to respondents. This allowed for a high response rate from the target population to address the question.

- *Phone voice recorder:* with the consent of the respondent, the interview was recorded with an Oppo phone voice recorder to capture responses verbatim.

3.6. Data collection procedures

Data was collected through questionnaires and unstructured face-to-face, one-on-one, in-person interviews to understand social media crimes/cybercrime in Namibia in great depth. Kumar (2011) states that the strength of unstructured interviews is the complete freedom in terms of the content, questions and structure. The study used the open-ended questions in the interview and questionnaires due to its flexibility of answering questions. Ritchie et al. (2014) posit that open-ended questions put the onus on the respondents to supply content of the answer in contrast to dichotomous questions. Kumar (2011) further adds that despite the difficulty of analysing the open-ended questions, they provide in-depth information if used in interview and in questionnaires they provide a wealth of information provided respondent feels comfortable about expressing their opinions and are fluent in the language used. The researcher audio- taped the interview using a smartphone voice recorder and transcribed the interview. Questionnaires were hand-delivered to respondents for completion while the researcher is waiting.

3.7. Data Analysis

The collected data was coded and analysed using thematic analysis and presented using graphs, charts and tables. According to Creswell (2013), data analysis in qualitative research consists of preparing and organising the data, (test data as in transcripts, or image data as in photographs) for analysis, then reducing the data into themes through a process of coding and condensing the codes and finally representing the data in figures, tables or a discussion. Creswell (2014, p.195) adds that the intent of qualitative data analysis is to make sense out of text and image data, it involves segmentation and taking apart the data as well as putting it back together. Shank (2006) states that coding is an act of selective intention and it uses three aspects, inductive approach, feedback and comparison as well as saturation. When we code, we mark those things in our data that we need to revisit. As these codes take more determinate shape and form, we often call them themes. Shank (2006) further describes thematic analysis as searching for patterns in data, when these patterns become organisational and when they characterise different segments of data, then they are called themes.

Welman, Kauger and Mitchell (2005) claims that the purpose of coding is to analyse and make sense of the data that have been collected. Codes are tags or labels that attach meaning to the raw data or notes collected during field work and these tags or labels are used to retrieve and organise chunks of text in order to categorise it according to themes. Codes can be created by using the conceptual framework of research questions, divide the field notes into different segments afterwards and by conditions in field notes. The researcher used free text tags to describe the contents from each interview question, divide them into written notes and categorise them in different themes.

3.8. Ethical consideration

Plooy-Cilliers *et al.* (2014) maintain that ethics are a matter of integrity on a personal level, but their implications reach much further than the individual. A researcher who acts with integrity adheres to ethical principles and professional standards that are essential for practicing research in a responsible way. Shank (2006) believes that a good researcher is an ethical researcher. Creswell (2013) adds that regardless of approach to qualitative research, a qualitative researcher faces many ethical issues that surface during data collection in the field and in analysis and dissemination of qualitative reports. Therefore the researcher sought approval from relevant authorities, the University of Namibia and participants gave informed consent. Ritchie *et al.* (2014) maintain that informed consent should be obtained from participants, meaning that people should be given adequate information to enable them to make a decision about their participation.

According to Plooy-cilliers *et al.* (2014), in collecting data from participants researchers need to prioritise their physical and psychological comfort. Therefore the researcher informed participants how their identities or sensitive information will be protected. The researcher tried to manage time by proper scheduling of interviews time slots. Further, the researcher remained objective while interacting with participants.

Importantly, the introductory paragraphs of certain standard self-administered questionnaires and the interview guide contained an ethical statement that informed respondents about their voluntary participation in the study and the purpose of the study. The rights and privacies of participants was fully honoured and they were clearly explained thereof. The principle of confidentiality and anonymity was fully maintained by assigning numbers or aliases to individuals.

The researcher reported the findings of this study to the institutions and the document could be published for academic purpose. As explained above by Nueman (2000), Ritchie et al., (2014) ethical codes are clear that researchers should do everything possible to maintain confidentiality and anonymity of participants in research. This then allowed reporting and publication of findings. Lastly, there are a number of legal and regulatory standards that have implications for the collection, storage and transfer of research data (Ritchie, 2014). Therefore, the researcher familiarised and complied with the countryand institutional legal standards.

In summary, this chapter described the research design of the study towards a strategy for the social media implications on human security in Namibia using a case study of Windhoek. The chapter outlined the methodology of this study, including the population of the study, sampling procedure, data collection instruments, research procedures and data analysis. The later discussed the ethical issues in research.

CHAPTER 4: DATA PRESENTATION AND DISCUSSION OF THE FINDINGS

4.1. Introduction

This chapter presents the findings of the study from primary research. It also analyses data collected. Further, the chapter discusses the findings in relation to the reviewed literature with the intent to design a strategy for the social media implications on social media. Each research question was analysed thematically by grouping and categorising themes that emerged from the interviews and questionnaire responses. The themes would be linked to the literature where applicable for discussion.

4.2. Presentation of findings

Section A: Demographic data

Interviews: The interview respondents were 8 from CRAN, NAMPOL, Ministry of Justice, and the Law Society and Legislature Organ respectively. The Ministry of Information and Communication Technology were also sampled for interview, but however, they did not respond to the letter of participation. Male participants were majority (75%), and female (25%) [see Figure 1]. Furthermore, the age representation of the respondents was as follows:

Table 2: Participant age groups

20-29yrs	12.5%
30-39yrs	25%
40-49yrs	25%
50-59yrs	25%
60yrs+	12.5%

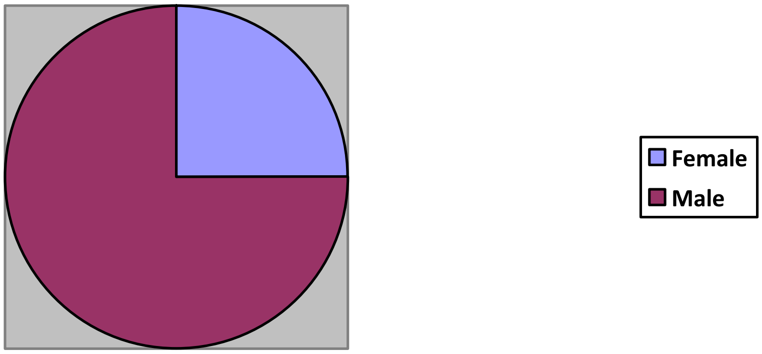


Figure 1: Interview gender representation

Questionnaires: Open-ended questionnaires were handed to 10 public members, and all were completed and returned. Female participants were the majority (60%) and male were minority (40%). Participants of the study were between the age group of 20-59 years. All participants were purposively selected based on the area of expertise in usage of social media, laws, and security.

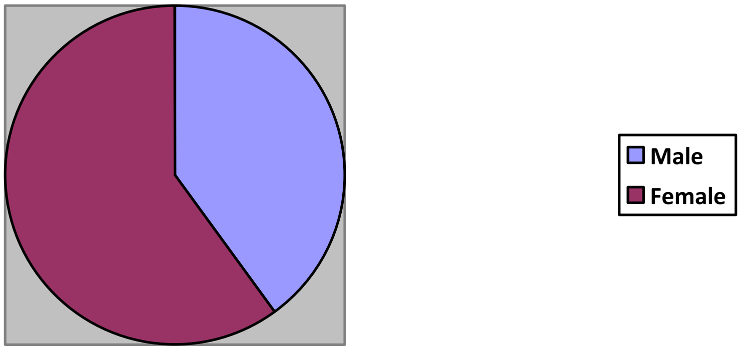


Figure 2: Questionnaire gender representation

4.2.1. Phase 1. Questionnaires Findings

The researcher purposively selected 10 members of the public. The participants completed the self-administered questionnaire consisting of seven open-ended questions. The respondents were to provide their answers on the provided line space in the questionnaires. All ten questionnaires were received back and completed. The questionnaires were numbered respondent 1 to 10 to allow analysis and discussion of the participants' response and make conclusions of the findings.

4.2.1.1. Perception on social media implications on human security of persons in Namibia.

Economic security: Respondent 1 stated that some customers lost their money and properties on social media through scams. Respondents 7 and 9 also concurred that many Facebook and WhatsApp users might fall victims of identity theft and online scam, whereby criminals would steal their banking details to defraud them and in most cases Namibians incurred economic loses through theft under false pretence. Respondents 2, 3, and 8 coincided that it was very expensive to stay online; therefore many people spend money on buying data causing them to be in debt. Respondent 4 stated that social media spread false economic information that may influence individuals’ expectations on the future economy of the country, thereby affecting their perception on commodity prices. Respondent 6 had no idea of any economic implications while respondents 10 and 5 stated that posts on social media might affect the economy negatively because they might reduce or prevent investors in the country and this affects individuals’ economic status.

Personal Security: Respondent 1 stated that posts on Facebook and WhatsApp lead to robbery of personal belongings, and in some cases allowed human trafficking specifically of women and children. In addition, respondents 1, 2, and 7 agreed that Facebook and WhatsApp are commonly used to spread hate speech and commit defamation of characters. Respondent 3 opined that majority of Facebook and WhatsApp users have a habit of revealing their physical locations which leads to physical attack by those who want to harm them. Respondents 3, 4, 5, and 10 claimed that there was violation of human rights, specifically the right to privacy and dignity. Meanwhile respondents 6, 9 and 10 agreed that Facebook and WhatsApp were a threat to human dignity and reputation, stating that many people’s private conversations, sexual acts and pictures were being taken or recorded without their consent and exposed on

Facebook and WhatsApp. Respondent 4 further claimed that Facebook promoted cyber bullying. Respondents 7 and 8 also noted that Facebook and WhatsApp were time consuming Apps which limited physical connection with families and friends, thereby causing individual isolation.

Community Security: Respondents 1 and 2 stated that communities became victims of wrong information sharing such as employment opportunities and education, and fake news about death of residents. In addition to respondent 2, 3 and 10 also concurred that Facebook and WhatsApp destroy community ethics, morals and traditions and cause divisions among citizens. Respondent 3 stated that citizens adopted foreign cultures and replaced their own by connecting with everyone across the globe. Respondents 4 and 7 stated that Facebook and WhatsApp increase cybercrime activities such as child pornography and cyber bullying. Respondents 5 and 6 had no idea on community security, while respondent 8 stated that Facebook and WhatsApp allowed thieves to exploit the resources of the community through theft. Respondent 9 added that Facebook and WhatsApp opened up the world of adults to children under age and some acts were prohibited in Namibia such as drug and pornographic materials.

Environmental security: Respondents 1, 2 and 5 stated that social media, mostly Facebook, promote unregistered business that exploits and degrades the environment. Business such as sand mining and brick-making damages the environment and this in turn threatens human lives. Respondent 10 stated that Facebook could be used as a platform where individuals discuss matters that harm the environment such as illegal hunting, illegal fishing, and cutting down of trees for timber. Respondents 3, 4, 6, 7, 8, and 9 stated that social media has no implications on environmental security.

Food security: Respondent 1 stated that some citizens sell and advertise expired food products on Facebook and WhatsApp status. Respondent 3 stated that Food Bank Namibia took responsibility to feed thousands of citizens who were going hungry. However, jealous citizens go on Facebook to criticize the initiatives which were aimed to alleviate hunger in the country. Respondents 2 and 5 stated that some individuals promote laziness on Facebook by posting that poor people should not cultivate their fields but should wait for the government drought food. Respondents 7 and 10 coincided that social media has implications when individuals spread misinformation about certain food brands, thereby influencing consumption patterns of such foods. Respondents 4, 6, 8 and 9 stated that there was no implication on food security.

Health Security: Respondent 1 noted the spread of unofficial health-related warnings on social media platforms such as Facebook and WhatsApp. Many users advertise uncertified medical products or services such as spiritual healing. Pastors and witch-doctors spread claims about curing HIV and AIDS and other sicknesses on social media platforms. Respondent 2 stated that social media challenges the provision of humanitarian intervention by hindering responses because of false information spread on Facebook or WhatsApp. Respondent 4 stated that Facebook and WhatsApp were used to violate privacy of patients by exposing their sickness. Respondent 5 claimed that Facebook and WhatsApp added to the spread of infectious diseases when minors are groomed for sex and some end up having unprotected sex. Respondents 6 and 10 agreed that staying online leads to anxiety, addiction and depression, and that some posts traumatise social media users. Respondent 7 claimed that certain individuals are given false data to purchase drugs or other products which could be harmful to them.

Political Security: Respondent 1 stated that some terrorist agencies recruit their members from Facebook. Meanwhile respondent 2 stated that many attacks were centred on political activists, while some individuals opened fake accounts to befriend political leaders to create trust over time so as to advance their ill-intentions. Respondent 3 stated that social media is used to incite mass movements and cause political unrest. Respondents 4, 6 and 9 stated that politicians are insulted by citizens on Facebook and WhatsApp and this sometimes results in civil cases. Respondent 5 claimed that Facebook can promote xenophobic attacks. Respondent 6 further stated that individuals could post and discuss political matters on Facebook or WhatsApp groups which could lead to social mobilisation which may pose danger if information shared is seditious, treasonous or about organised crimes. Respondent 7 stated that political parties post hate statements and false accusation anonymously to politically victimise others. Respondent 8 stated that sometimes political leaders threaten citizens not to use social media when there was no law to back up their action.

Respondent 10 stated that Facebook and WhatsApp create a disrespectful environment between the government and the citizen.

4.2.1.2. Experience of cybercrime situation in Namibia

Respondent 1 stated that cybercrime was a serious threat and that it was unfortunate that most Namibians had no clear knowledge of what constituted cybercrime. Respondent 2 also stated that the growth of social media has resulted in online crimes such as blackmailing, embezzlement, defamation and hacking of accounts.

Respondents 3, 6, 8, 9 and 10 agreed that the common trend in Namibia was exposing of individual sexual acts, mostly nude videos and pictures of couples on Facebook and WhatsApp without the knowledge of the victims. The respondents further stated that this situation was persistent and information shared on social media is permanent; one cannot undo the damage caused. Further, cyber-bullying was also on the increase among young children and this affected their academic performance. Respondent 10 added that hacking and internet fraud on other people’s Facebook accounts was also common.

Respondent 5 stated that criminals explore the use of social media and approach unsuspecting victims under false pretence and rob them of their properties or groom them. Respondent 7 proffered that the cybercrime situation in Namibia was normal compared to other countries such as South Africa.

4.2.1.3. Perception on the prevalence of social media crime in Namibia

Table 3: Prevalence of social media crimes in Namibia

	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10
Distribution or circulation of materials	1	1	1	1	1	1	1	1	1	1
Child pornography	2	2	2	1	2	3	3	1	2	1
Grooming	4	2	2	4	3	4	3	4	3	3
Cyber stalking	2	1	5	5	1	2	1	5	1	1
Cyber bullying	1	1	5	1	1	1	1	5	1	1
Defamation of character	1	1	5	1	1	1	1	5	2	5
Hacking of personal computers/accounts	3	4	2	1	3	4	2	1	2	5
Sexting	1	2	2	1	1	2	3	1	5	1
Identity theft	3	1	1	4	3	2	1	1	5	1

Hate Speech	1	1	5	1	4	1	2	3	1	1
Drug/Human trafficking	5	1	1	5	3	4	4	2	2	5
Internet Fraud	1	1	5	5	3	4	1	5	3	1
Phishing	4	1	4	4	4	4	4	3	2	3
Cyber terrorism	5	5	5	5	5	5	5	5	5	1
Breach of privacy	1	2	5	1	2	1	2	4	2	5
Pornography	1	1	3	2	1	1	2	5	1	5

Table 3 displays a list of some of the social media crimes committed in Namibia through WhatsApp and Facebook and their occurrence ratings on a scale of 1-5 (1 being the most prevalent and 5 the most least). Respondents were requested to rate the crimes according to their occurrence. The most prevalent social media crimes rated 1 are; Distribution and circulation of obscene materials 100%, followed by cyber bullying 80%, hate speech 60%, then sexting, identity theft, cyber stalking and pornography 50%. The prevalent ones rated 2 are child pornography 50% and breach of privacy 40%. The moderate crime rated 3 was hacking of personal computers and accounts 30%, while phishing 60% and grooming 40 % were rated 4 being the least prevalent crimes. Cyber terrorism was rated 5 with 90%, as the little prevalent crimes while drug and human trafficking, cyber stalking and internet fraud 30% each.

4.2.1.4. Perception on how social media crimes are committed in Namibia

Respondent 1 noted that criminals advertise services or products for sale such as flats, houses and vehicles which they did not have and they w ask interested clients to pay a certain deposit. Respondent 2 observed that some people hack Facebook users' accounts and unfriend them after they have tampered with their private settings. Respondent 3 claimed that WhatsApp messenger allows people to send instant messages, video, photos, and short audio messages to either one person or within a group chat, while Facebook allowed anyone to search for anybody they might be interested in even if they were not their friends. As a result it becomes possible to post unauthorized pictures and videos on anybody's profile.

Respondent 4 also claimed that individuals invade personal information of Facebook users. Respondent 5 argued that criminals create fake Facebook accounts and approach unsuspecting victims under false pretence to defraud them. Respondent 6 added that some individuals have a habit of sharing pornographic materials to many Facebook and WhatsApp users.

Respondent 7 posited that in many occasions Facebook accounts were being hacked and as a result the owners of the accounts were not able to access or log into their accounts. Affected users have to open other accounts and are forced to use different usernames. Respondent 8 added that Namibians developed a habit of sharing confidential information about others such as health records and extort such victims for money. Respondents 9 and 10 also concurred that there was a habit of exposing others on Facebook and WhatsApp by uploading sex and nude pictures and videos. Some users pretend to sell products online and when they receive money from clients they block their numbers and de-activate their Facebook account.

4.2.1.5. Knowledge of Namibia’s legal position with regard to cybercrime.

All 10 respondents agreed that Namibia does not have any legal framework that regulates cybercrimes. Respondents 4, 5 and 10 add that the Ministry of Information Communication and Technology was busy finalising the Electronic Transaction and Cybercrime Bill.

4.2.1.6. Perception on the challenges faced by the Namibian Police Force and the courts

Respondents 2, 3, 4, 5, 8, 9, and 10 concurred that the absence of cyber legal framework appeared to be the main challenge for both the courts and the police. They stated that the police cannot arrest suspect without a law. Respondents 1, 2 and 10 agreed that there was lack of expertise to deal with cybercrime cases; as such capacity building was a big challenge. Respondents 1, 6 and 10 further observed that the police and courts might experience difficulties in gathering and presenting evidence to prosecute perpetrators.

Respondents 3 and 10 stated that some social media crimes were committed by foreign nationals and it was difficult to trace and arrest such offenders because of the transnational nature. Respondents 3 and 4 further noted that the police and courts lacked technological tools and models to investigate and prosecute social media crimes. They further added that the police struggled to handle confidential information. Respondent 4, 7 and 10 commented that anonymity of Facebook users allowed individuals to create fake accounts to commit crimes and this made it difficult to arrest them. Respondent 6 also added that social media usage accelerated organised crimes such as human trafficking and terrorism acts.

4.2.1.7. Proposed strategies that should be adopted by the Namibian Police, MICT and CRAN to deal with social media crimes

Respondents 1 and 3 maintained that the police, MICT and CRAN should come up with a memorandum of understanding to deal with social media crimes. Respondent 2 stated that the police should use common and statutory laws to deal with cybercrimes. Respondent 4 proposed to establish public and private intelligence to prevent organised crimes and ensure protection of information. Respondents 1, 5, 7 and 10 suggested that it was important to have public meetings to create awareness on the danger and and implications associated with usage of social media. Furthermore, awareness campaigns aimed at providing safety tips on internet should be announced on radio and broadcasted in all local languages to ensure that everybody was aware. Respondent 1 added that churches should play a role in dissemination of safety information to create awareness. Further to that, respondent 1 suggested that the Ministry of Education, Art and Culture should use Life Skill teachers to educate school learners on the dangers of social media.

Respondents 5, 6, 7, 8 9 and 10 proposed that the government should speed up the formulation of a cybercrime bill and it should be passed and be known to all citizens. The law would define certain acts as crimes and provide guidelines to the police and courts on how to handle reported cases. Respondents 6, 7 and 10 suggested that the police should invest in capacity building as this would ensure that there was expertise to investigate, gather evidence and detect cybercrime. Respondent 7 added that there should be a department that focuses on monitoring social media crimes and work together with service providers such as MTC, Telecom, Facebook and WhatsApp to acquire evidence that would ensure prosecution of offenders. Respondent 10 proposed international cooperation, urging the Namibia Police Force to collaborate with law enforcement agencies in other countries so that they could share ideas on how to combat cybercrime.

4.2.2. Phase 2. Interview responses

Interviewees were given numerical order such as Respondent 1, Respondent 2, up to Respondent 8 in the chronological order in which the interviews were held to present the interview phase findings. This was done to adhere to the ethical considerations of anonymity and confidentiality. The researcher purposively selected all 8 respondents to allow in-depth explanation of the questionnaire findings in phase 1. The researcher further used the same research questions in the interview and the questionnaires to test the reliability of data.

Interviewee responses provided clarity to the results provided by the questionnaire respondents in phase 1, especially on the social media implications on the seven human security dimensions and the cybercrime trends. Some questionnaire results such as the cybercrime situation and prevalence on WhatsApp and Facebook needed explanations. To gain in depth understanding of the social media crimes implications, it was necessary to sample experts from the Namibian Police Force (NAMPOL), (Legal Division, Public Relations Division and Criminal Investigation Directorates), the Communication Regulatory Authority of Namibia (CRAN), Ministry of Information and Communication Technology (MICT), Ministry of Justice (MoJ), Law Society of Namibia and the Legislature. Their input was necessary to address each of the research questions in particular because the respondents specialised either in security, law, communication and media.

Three (3) respondents (respondents 2, 4, and 6) were from NAMPOL Public Relations Division, Legal Division and Criminal Investigation Directorates respectively. Two (2) participants were from Ministry of Justice, where Respondent 1 was a prosecutor and Respondent 3 was a lawyer. Respondent 5 was from Law Society of Namibia, while Respondent 7 was from Namibia Legislature and Respondent 8 was from CRAN. All the sampled interview respondents were considered to be experienced with regards to laws, security matters and media communication matters respectively.

4.2.2.1. Question 1. Perception on the social media implications or threats on human security

Economic security: All eight respondents agreed that social media usage has implications on an individual's economic security. Respondent 1 pointed out that some individuals could be put on spotlight on suspicion of breach of law, thereby being forced to declare their assets. As a result of declarations on assets, such individuals might be victims as this information would be made available on Facebook and WhatsApp, giving criminals' knowledge of their wealth and possessions. This might expose individuals to theft, robbery, and even physical attacks. Respondents 1, 3 and 6 voiced on the same when it came to financial scams, stating that individuals with criminal intentions ask email and cell phone numbers of Facebook and WhatsApp users with the intention to defraud them. Respondent 6 gave an example of a Namibian lady whose information was taken from Facebook after receiving an email and text message that she won a scholarship to pursue her studies in Ghana or Nigeria and that if she did not want to go study; she could claim her scholarship money by sending her banking details. The lady responded by sending her banking details and what happened next she found her bank account with a zero balance where she had had about

N$30 000.00 savings. In addition to financial scams, Respondents 1, 2, 4, 5 and 7 shared that many Namibians fell victim to hacking of bank accounts and identity theft through Facebook.

Respondents 3, 5 and 6 concurred that,

> "…There is an online shopping trend mostly on clothing, handbags and Brazilian hair from China. Usually, a Namibian meets a friend on Facebook and exchange mobile numbers and start communicating through WhatsApp. Later on they get into business. The dealer starts asking for 50% deposit of the order price. Individuals get enticed because for the first time they receive their products and items, and when they put in a big order with huge deposit, the dealer disappears, and making sure that that individual will not communicate further".

Respondents 3, 6 and 7 again concurred that,

> "WhatsApp is commonly used to defraud people, for instance there was a WhatsApp group called My Life Change, where individuals were lured to join the financial pyramid by investing their money for a period of some months on promise of high interest on such investment." Respondent 3 added that "I was on that group, I lost about N$4000.00 and there were about 40-50 individuals complaining of having lost their money.

On economic implications, Respondent 5 stated that “when individuals post their locations, they expose the safety of their properties as criminals will know that you are not at home, they will come break into your house and steal valuable properties. As a result, you have to buy and replace the broken and stolen items. Respondents 2, 3, and 8 stated that social media is addictive, one has to purchase units or data bundles for you to be online. Many people now buy units every day and such units or data is expensive leading them into debt even.”

Respondents 3, 5, and 6 concurred that,

“…there is a Facebook Page called **‘**buy and sell’**.** Some individuals advertise that they are selling items such as cars, computers, fridges, car parts and other expensive machines and interested buyers call them for sales. Some people agree to buy items, where in most cases, the seller asks the buyer to deposit 50% of the purchase price to reserve the item for them. After depositing the requested amount, the seller deactivates their Facebook account and create another one with a fake name”.

Respondents 5, 6, 7 and 8 agreed that,

“…some people lost their properties such as houses, livestock and vehicles through false advice from pastors and witch doctors. Some pastors who were met on Facebook and WhatsApp groups tell individuals that their houses or vehicles were afflicted with demons and they should sell or donate to the church. Some families end up homeless as a result of advice from pastors and witch doctors". Respondent 3 added that theft by false pretence was also committed by fake estate agents who advertise houses on Facebook and WhatsApp status and ask interested buyers to deposit top up amount, although the house the client would have viewed would not be for sale. In another case, a wedding planner was paid full amount for decoration and catering in 2017 in the northern region on the country, but the catering lady did not turn up to fulfil the job she was paid for and she switched her mobile phone off.

Respondent 8 noted that what individuals post on their Facebook and WhatsApp status affected their employment opportunities because employers check the candidates' profiles to assess their moral behaviour before they hire them. Respondents 2 and 4 agreed that most Identity Theft cases are committed on Facebook. They also added that information obtained or hacked from social media such as confidential or banking details were used by individuals to steal money from bank accounts and this resulted in financial losses. According to Respondent 4, there was a recent case in October 2018 of somebody who stole the identity of another person, went to the bank and stole around N$400 000.00 from the bank account and this was discovered when the victim went to inquire at the bank.

Respondents 3, 5, and 6 stated that theft under false pretence became too prevalent in Namibia, with people losing their fortunes due to this false pretence known as ‘okatoo’. Respondent 6 added that there was a case of a seller who advertised a vehicle on Facebook. an interested buyer in Opuwo responded and the seller was in Okahandja. The seller asked the buyer to deposit N$100 000 so that the seller could keep the car for him. After depositing the money, the buyer decided to travel to Okahandja to get the car, but on arrival, the seller’s number went off air forever.

Respondents 2, 4 and 7 observed that embezzlement had become quite common in Namibia. Some Facebook users create accounts with the names of prominent people, family and friends of people they want to defraud. They send friend request to those users and inbox or request their mobile numbers. They befriend them and pretend to be in trouble and in need of urgent financial help and ask such individuals to send money to them on e-wallet and blue wallet. When they receive the money, they throw away the mobile sim card and deactivate their Facebook accounts and create another account with a different name.

Personal Security: All 8 respondents agreed that Facebook and WhatsApp pose physical threats. All interviewees stated that Namibian residents have a habit of posting their locations on Facebook, like ‘current situation’, which could put their lives in danger. Respondent 5 added that users may post materials that are offensive to others, that while they are expressing themselves, some friends might get provoked by such posts, resulting in fights or violence. Respondents 3,4, and 7 stated that when parents post on Facebook that they are travelling for vacation, they pose threats to their home security as criminals might know that they would not be available at their homes and they might break into their houses and hurt the children. Respondent 1 said that Facebook and WhatsApp reveal names of individuals who commit certain acts such as domestic violence, robbery and murder and as a result these individuals get attacked by the community members.

Respondents 1, 2, 4, and 7 agreed that social media increased organised crime against humanity, such as kidnapping and human trafficking which was a personal security threat. They gave reference to a recent incidence of missing school children including the girl named Avihe who was murdered and her body found in a river bed in Windhoek in 2018. Respondent 7 further added that his/her friend's grandchild committed suicide because of Facebook stories.

Respondents 3, 5, and 6 observed that,

> "…Nowadays people do not have privacy anymore, everything a person does is on Facebook. While you are busy making sex, someone is taking a video with the intention to defame the other person. .". Further, respondents 3, 4, 5, 6, 7, and 8 observed that Namibians developed a habit of recording videos and taking photos of other people's private

> lives. Respondent 6 reported that somebody recorded a video of a Namibian soldier in uniform who was relieving himself behind the bush and posted it on Facebook and shared it on other social media platforms. The respondent stressed that these acts were bad as it felt like everyone was watching you wherever you were and this infringed upon the privacy of individuals.
>
> Respondent 3 said that in 2017 there was a WhatsApp group administrator who was beaten up by group members because he did not add another participant when he was asked to. Respondents 3, 5, and 8 agreed that the majority of Namibians had their life on Facebook and WhatsApp, updating current situations revealing where they were, what they might be doing, where they studied, their work, and their marriage status and their problems, exposing themselves to danger of being attacked, robbed, assaulted and stalked.

Respondents 3 and 5 further stated that there was an add on ‘Facebook Check In’ revealing live locations of individuals to all Facebook friends by giving them a notification that you are near them, giving the distance and time when you were near them. This notification might expose individuals to physical attack by those who befriend them with bad intentions. Respondent 6 added that,

“…cyber bullying lowers one’s self-esteem and confidence, especially in teenage. Bullying people results in fighting and in some children to be expelled from school. This affects their education progress. Many people’s reputations and dignity was ruined through social media when their sexual life, health status and other confidential information are revealed. One married woman was exposed for having sex with a young man and the man tried to blackmail her for money. When the woman refused, the man circulated the video on WhatsApp, resulting in the woman attempting to commit suicide”.

Community Security: Respondent 1 commented that,

“…Facebook and WhatsApp give headlines on criminals and accused persons providing the identity, pictures and descriptions and this results in mob attack. Mob attack poses danger to identical individuals mistaken with criminals because in some cases the society might take law into their own hands to seek justice. As a result, crimes and violence would keep increasing and minors might become victims of the angered gangs as the cases of missing young children were also reported in Windhoek in 2017-2018. This was worrisome and parents feared for their children after the death of Avihe, a young girl who was murdered while she was coming from school.”

Respondents 3, 4 and 8 concurred that many youths were addicted to Facebook and as a result they did not perform their tasks and duties at home or in the community, slowing down the development of such. Respondent 7 added that

Facebook and WhatsApp users get addicted and they isolate themselves from their friends, family and community members.

Respondents 3 and 6 agreed that Facebook and WhatsApp platforms were commonly used to spread fake news, either about health information, crime, weather, and employment opportunity. Respondent 6 gave a reference of a case whereby someone posted a video clip of Dineo cyclones on Facebook in 2017 and stated that the cyclone would be passing Gobabis toward Windhoek and people should remain indoors. This put the community in fear and their right to liberty was violated until the news was verified as not true. Respondent 3 stated that through social media rumour spread in the community like wildfire causing misunderstanding. Some people post accident scene pictures, causing shock to victims' next of kin who would not have been informed of such mishaps. Seeing such circulation of videos and pictures of their loved one on WhatsApp or Facebook could traumatise community members and families**.**

Respondents 1 and 4 posited that Facebook was used to cause tribalism and racism among community members. As result there would be division among the community members as some may lose their sense of belonging due to racial discrimination.

Respondent 3 said that, on the other hand, immoral practices such as pornography being done on Facebook and WhatsApp shock the community as their culture and traditions would not countenance such practices. Respondent 4 added that Facebook and WhatsApp are an affront on community ethics. An example was cases of lifeless bodies of persons who committed suicide or died in accidents circulating on social media. This would shock and traumatise most of the community members. Respondents 6 and 7 also added that some citizens circulate indecent materials and defame others on social media and when victims report to the police, justice take long to prevail, leaving some community members to take the law into their own hands. Pornographic and obscene materials destroy moral ethics of communities and traumatise individuals.

Respondents 1, 3 and 6 reported that the easy access to information on WhatsApp and Facebook enable recruitment of criminals and increases organised crimes in drug and human trafficking, terrorism, grooming of young girls into prostitution and mob attacking. These crimes make the community members insecure because criminal activities keep increasing. Respondents 3 and 5 stated that social media breaks marriages because many married couples who cheat on their spouses get exposed of their adultery through circulation of sex videos, voice clips and messages on social media platforms. Exposing of sexual partners results in divorce, murder or gender-based violence.

Respondents 4, 5 and 6 commented that Facebook promotes transgender activities. Some countries promote gay and lesbian relationships and marriages while Namibia prohibits it. Consequently, some individuals in communities demand that transgender relationships be allowed in Namibia, and this causes division among community members. Other individuals were now living in isolation because of their gender and being discriminated, mistreated, or attacked because they were gay and lesbians. Respondent 7 stated that, social media increased criminal activities because criminals can easily communicate and access vulnerable community members. Children were being groomed and abducted for sex and prostitution because of information provided on social media.

Environmental Security: All 8 respondents agreed that information posted on Facebook and WhatsApp might threaten the environment. They all pointed out the poaching of rhinos and elephants as a serious matter. They also stated that individuals may post pictures of the endangered species and their locations and poachers would get a hint as to where to find them. Respondent 5 also added that Namibians pose protected resources to danger either by individual citizens or by citizens in collaboration with foreigners. The case in point was that of a Chinese national who poached rhinos and elephants for trading, threatening the endangered species with extinction.

Respondents 3, 4, 5, and 6 agreed that Facebook and WhatsApp facilitate commission of crimes such as illicit trading of natural resources such as timber, wildlife, minerals (gold and diamond) and marine resources (fish). Respondent 4 gave an example of a recent case of an American citizen who came to Namibian and killed a family of six baboons in November 2018 and this damaged the Namibian ecosystem. Some people advertise that they sell dry game meat without revealing whether they have a hunting permit; Other people may see this as a business opportunity and engage in illegal hunting.

Respondents 4, 5 and 6 concur that posts of sand mining for business on WhatsApp and Facebook became an environmental threat, stating that many citizens mine sand without authorisation from local authority and this results in environmental degradation. They gave reference to the recent sand mining case of two businessmen in Oshikoto region who were mining sand illegally in November 2018. Respondent 8 stated that, the MICT warned the citizens not to post photos of protected species (rhino and elephants) on Facebook and WhatsApp because they will expose them to danger of poaching. Some people post videos of them driving on dunes, and this may encourage others to do the same and this damages the environment.

Food Security: Respondents 1, 3, 4, 5, 6, and 8 coincided that,

> Social media can spread rumours of food poisoning, causing majority to refrain from consuming and purchasing food at certain places. For instance, the outbreak of the listeriosis bacteria in South Africa in 2017 allegedly contaminated processed meats produced by Enterprises Foods Company that resulted in 200 reported deaths in South Africa and one in Namibia caused fear to majority of canned meat consumers. The information was circulating on Facebook and WhatsApp in Namibia, and some individuals added names of some unaffected canned meat products to the list. Many individual refrained from eating all sorts of canned meat, thereby causing food security threat.

Respondent 4 stated that if Facebook or WhatsApp users provide information that there was no security for marine resources, such information could increase illegal fishing in rivers and the sea. Illegal fishing can result in food insecurity because there is no one to control fishing activities, and fish will get depleted quickly.

Respondent 5 remarked that,

> "…Some individuals post video clips showing how certain foods are processed, giving a picture that these foods were not well processed. There was footage of rice made by Chinese showing that that rice contains plastic particles; this could mean that majority of people would not eat rice made from China. Some circulate a picture of opened canned fish, whereby among the fish pieces there was a human finger, this was disgusting, people would think that all canned fish have human fingers and some might stop consuming".

Respondent 6 remarked that,

"…A recent case of breaking news on social media and television was of a Moroccan woman who killed her boyfriend and cooked his meat and gives it to people to eat. The photos of a plate of rice served with human flesh which looked like chicken circulating on both Facebook and WhatsApp could discourage many people from eating meat. Some spread rumours that Chinese restaurants cook dog and cat meat".

Health Security: According to 6 respondents, Facebook and WhatsApp make users get addicted, and addiction could be a mental health hazard. Mostly, young people do not sleep enough; they spend all night on Facebook and chatting with friends on WhatsApp. Respondent 4 stated that "individuals may spread habits that might be adopted by those who are not health conscious, causing them to put their health at risk. Also, it becomes fashionable for the youth to smoke 'humbly bubbly', a container of water with a pipe, and that water vapour damages the lungs. Some individuals post video clips of car racing which may promote speeding and this causes motor vehicle accidents, causing some people to die in the process and some to become disabled".

Respondents 3, 4, 6 and 8 coincided on how individuals' behaviour can get influenced by Facebook and WhatsApp posts. There was a case of a pastor feeding people with snakes in South Africa in 2017 apparently for them to get healed, targeting those without children and those diagnosed with cancer.

Furthermore, respondents 3, 4, 5, 6, and 8 agreed that,

"…some church pastors and traditional healers post on Facebook claiming to cure some illnesses, many people get their contacts and run to them for cure. In most cases the HIV/AIDS and cancer patients get brainwashed by the traditional healers by giving them herbs to drink and smoke for them to get cured, and as a result they keep smoking and drinking herbs instead of taking their medicine from the hospital. In the end their health condition become bad and they die. Some individuals get anointed water or oil from pastors apparently to apply and to protect them from getting diseases. Consequently, patients stop taking the prescribed medication".

Respondent 4 gave an example of a recent case of a Zimbabwean prophet, W. Magaya, who was on news and his video clip was circulating on WhatsApp being interviewed and claiming that he found the cure for HIV/AIDS and cancer. It was found out that he was just misinforming people that he had found cure for cancer and HIV/AIDS. Majority of people would drop their treatment or medication and start taking herbs from witch doctors and this makes their health deteriorate and some die sooner than expected.

Respondent 6 explained the implication of Facebook and WhatsApp on health in detail,

"…that many social media users engage in businesses that sell health products, such as tablets that allegedly help to relieve and some cure diseases such as high blood pressure, cough, flu, back pain, headache and many more. These tablets, herbs and other products are advertised on Facebook and WhatsApp status and interested buyers contact those selling to purchase. The seller does not give prescription as to how the products must be used. Some people apply certain

> ointments and it changes their skin colour, while others develop swollen feet. Some tablets have side effects and many people with health conditions are already on treatment from hospital and they are not supposed to use other drugs at the same time they are taking their treatments as this makes their treatment not to work, complicating their health. Some pastors and witch doctors end up sleeping with women in order to treat their womb so that they can have children in their marriages, because some women struggle to conceive and their husbands get angry toward them. Women resort to sleeping with the pastors in the hope of getting help; as a result some get infected with STIs while others end up pregnant with their children".

> Respondents 3, 4, 5, 6, and 8 commented on the influence of Facebook and WhatsApp on losing weight,

> "…some individuals see people posting how they lost weight on Facebook and get information on how to lose weight by drinking and eating certain foods and products, and others drink tablets. Some people skip meals because they want to lose weight. Consequently, they end up having miscarriages and their health condition deteriorates as a result of taking tablets or products that are meant to make them lose weight".

Respondents 2, 3, 4, 5, and 6 postulated that young people upload drug clips that show what drugs can make a person happy or act higher. Such practices can lead to drug abuse which causes cancer and other complications. Respondents 2, 3, 4, 5, and 6 expressed that sharing of accident photos and videos was way too muchand that Namibians have lost feeling for others. The videos send on social media might be received by relatives of the victims and deceased in the car accidents. This might cause heart attack and other health related complications to the bereaved family in case of death.

Political security: Respondents 1, 3, 4, 5 and 6 stated that Facebook and WhatsApp can cause political instability because individuals express views and post hate speeches aimed at their political opponents. Individuals are threatened in homes, schools, churches, families and workplaces because of their political affiliations. Hate speeches are directed from one political party to the other on Facebook and WhatsApp groups. This fuels up discrimination among citizens and some end up resigning or refraining from political participation.

Respondent 3 remarked that when people gather on a WhatsApp group for political activity such as overthrowing a government, this could lead to political instability. In most cases private political conversations, videos and pictures leaked to Facebook and WhatsApp can cause political threats on individuals. Respondent 4 added that some individuals would be watching the terrorist acts on Facebook, while others may join foreign terrorist groups and this poses serious threats to human security of Namibians if that person is used to attack his or her own country.

Respondents 5 and 8 coincided that the statutory law provided that for any political gathering or meeting, the political party should inform the police about such gathering prior to the meeting. However, the police cannot monitor online gatherings. Facebook and WhatsApp provide platforms that allow political demonstration and gatherings that result in uprising. Respondent 5 stressed that;

"…it is possible nowadays to find about 200 individuals gathering on Facebook page or WhatsApp group discussing very sensitive political matters and the police cannot police or monitor such gatherings. Such group discussions might result in motives that result in public violence, sedition and high treason. Some individuals may incite others to overthrow the government, and civil war or conflict can as well result if the situation is not handled well".

4.2.2.2 Experience of cyber social media crime situation in Namibia.

According to the 6th respondent, anonymity of cybercrime makes the cybercriminals hide their faces and identity while committing criminal activity such as sending threats to individual Facebook and WhatsApp users. The situation was worse when it came to sexual relationships of boyfriend and girlfriend, and married persons with unmarried ones. A third party who gets involved with one of the partners may threaten the one he or she was involved with to cause the break up or expose him or her by sending pictures or conversations they had privately to the real girlfriend or boyfriend, husband or wife of the concerned person or send such to Facebook or WhatsApp using an anonymous number. Respondent 2 added that exposure of others in compromising situations became rampant in Namibia. This could be caused by lack of expertise and desire to follow up and prosecute those involved in these activities, because the more people get away with these activities, the more they become prevalent.

Respondent 1 stressed that in most cases, people blackmail others by threatening to send nude pictures to social media or shame them by informing their partners and families, leading to confrontation and fighting. Respondent 3 and 5 referred to an incidence in 2017 of a guy who got involved in a sexual relationship with a married woman in Windhoek. While they were having sex, the man recorded a video of their act and afterward extorted the married woman to give him money and materials if she did not want the video to be sent to the husband. In the end the said video was circulating on social media, WhatsApp and Facebook. There were many cases of circulation of obscene materials, defamation and exposing individuals which resulted in sour relationships, suicide, murder and divorce. Most married couples divorced when their adultery acts were exposed on Facebook or WhatsApp.

According to respondent 7, Namibians accept any friend request even if they do not know the person requesting them on Facebook. Some even give their mobile numbers to Facebook friends whom they do not know in person. Namibian citizens lacked understanding of the danger of social media.

Respondent 8 concluded that “the situation is getting worse because people know that there was no law that compeled them to remove posts that offend others, or prevented them from acting in a way that hurt others. More prevalent was cyber bullying among young children on Facebook, defamation of character and hate speeches. Uploading of accident scene pictures, obscene and indecent materials were also on the increase.

4.2.2.3. Types of cybercrimes in Namibia

Table 4: Prevalence of social media crimes in Namibia

	R1	R2	R3	R4	R5	R6	R7	R8
Distribution or circulation of obscene materials	1	1	1	1	1	2	1	1
Child pornography	4	2	3	4	5	1	1	3
Grooming	3	2	2	3	3	5	3	3
Cyber stalking	2	1	1	1	1	5	1	2
Cyber	2	1	1	1	2	2	1	1

bullying								
Defamation of character	2	1	1	1	2	1	1	1
Hacking of personal computers/accounts	4	4	3	3	4	1	2	4
Sexting	4	2	1	1	1	4	3	1
Identity theft	5	1	2	3	3	1	1	3
Hate Speech	3	1	1	1	1	2	2	1
Drug/Human trafficking	1	1	2	4	2	4	4	3
Internet Fraud	2	1	1	1	3	3	1	3
Phishing	5	1	1	3	3	4	4	3
Cyber terrorism	5	5	4	5	3	5	5	4
Breach of privacy	2	2	1	1	2	4	2	1

Pornography	1	1	1	2	1	3	2	1

Table 4 shows a list of some of the social media crimes committed in Windhoek through WhatsApp and Facebook and the respondents were requested to rate the crimes according to their occurrence from 1 to 5 (1 being the most prevalent and 5 the least). The most prevalent social media crime rated 1 was Distribution and circulation of obscene materials 87.5%, followed by defamation of character 75%, then pornography, hate speech, cyber stalking and cyber bullying 62.5% and the least prevalent was sexting 50%, internet fraud 50%, hacking of personal computers and accounts, 50%, and breach of privacy 50%. . Moderate rated 3 crimes were grooming 62.5%and cyber terrorism also with 62.5%.

4.2.2.4. Perception of how social media crimes were committed in Namibia

According to respondent 1, “criminals use Facebook and WhatsApp to network in committing crimes. There was an incidence of a vehicle rental company that collaborated with criminals on WhatsApp. When tourists visited Namibia, they hired cars from that rental company, giving information of their destinations. Meanwhile, someone in the same company gave away that information to criminals and shared locations of such tourists on WhatsApp. The criminals would hire a vehicle from the same company and track the tourists. Consequently, before the tourists reached their destinations, they would be attacked and robbed of their items.

Respondents 1, 3, and 4 coincided that some people stole pictures of others from Facebook and edited such pictures into something else, for instance a male turned into a female, and posted them back on Facebook with a misleading caption of the person's details.

Respondent 1 stated that "cyber stalking was prevalent in Namibia. This particular respondent cited the existence of a Stalking software that can reveal what a partner is doing, which cost about 40 to 50 thousand Namibian dollars and it only required a cell phone number of the person to be stalked and this can only be done on WhatsApp. This software was used when there was infidelity suspicion in a marriage. In that case the spouse does not have privacy any longer as every chat and contents shared between the husband and wife and the other contacts would be viewed simultaneously. Stalking of this nature poses serious threats by putting the lives those concerned at risk of physical harm when wrong or bad contents erupt.

Respondents 2, 3, 4, 5 and 6 shared the same view that people lost humanity. In cases of accidents, instead of rescuing a fellow human being burning in a vehicle people are interested in covering the incident and be the first to share such news on social media. Respondents 2, 3, 4, and 5 gave an example of an incident of a boy who was maulled by bull dogs in Windhoek in 2015, stating that instead of helping, people were in their vehicles taking videos and sharing it on WhatsApp.

Respondent 2 stated that criminals use social media for embezzlement, asking individuals to send them money pretending to be in trouble. Respondents 2, 3, 4, 6, and 7 agreed that some people advertise products on Facebook or WhatsApp asking interested buyers to make payment to e-wallet, blue wallet and easy wallet, but once the payment was done, the criminal disappeared when items are not delivered to the buyer.

Respondent 3 claimed that “there was a WhatsApp group called My Life Change where individuals were added, brainwashed that their lives will change for good and they would get cars and other things if they invested their money in My Life Change scheme. However, individuals have not received anything in return. More than 40 people that I know lost about N$4000.00 in that scheme.

Respondents 4, 5, 6 and 7 stated that many people receive messages that they have won certain amounts of money and they should send banking details, and some transport money to send the award. The perpetrators keep asking for more money and the victims lose out. Perpetrators sometimes defraud bank accounts using false identity based on information obtained from Facebook.

According to Respondent 3, many Windhoek women were exposed in sexual acts on WhatsApp and Facebook during 2014-2018. About 30 incidences of such acts, including pornography, became viral during the said period. All 8 interviewees agreed that the most common and disturbing trend on social media was exposing of individuals by circulating sex videos, pictures and private conversations on WhatsApp and Facebook to defame others. Respondent 3 and 5 gave an example of a married woman who got involved in a sexual relationship with a young man. The man had an intention to defraud the married woman; therefore he started blackmailing the woman for money. The woman refused, and the man posted their sex video on Facebook and WhatsApp. The woman attempted to commit suicide.

Respondent 5 remarked that,

"…Mostly committed in recent years is defamation of character; people posting matters and statements that derogate or defile and diminishe the reputation and dignity of other individuals. A Facebook user, known Chris Paul, posted on his wall mentioning names of individuals who were involved in sexual relationships with their employers and got benefits related to employment and promotions. About 3 individuals who were offended by that post opened cases of defamation of character and Chris Paul was arrested. Some citizens incited others to commit crimes. Between 2014 and 2015 an individual posted on Facebook that he wanted anybody to bring him a human head of someone whose name was also mentioned in the post. Whoever saw such a post and knew the wanted person might actually murder them because he or she would get a lot of money".

Respondents 4 5, 6, 7 and 8 shared that the majority of Windhoek residents advertised goods and products such as Brazilian hair, clothes and cell phones on

Facebook and WhatsApp status asking interested buyers to deposit certain amounts when placing their orders. When buyers enquire about their items, the sellers' Facebook accounts are deactivated and the cell phone numbers become unreachable.

Respondent 5 again stated that criminals took advantage of electronic transactions and cell phone banking such as e-wallet. They send fake messages that show that they have send you some money by mistake and they would request you to send that money back and keep some of it. The receiver would send that money back to the criminal when in actual fact the criminal had not send any money in the first place. Respondent 6 added that criminal-minded persons could easily hack into another individual's Facebook account and send inbox messages to their Facebook that they are stuck somewhere and needed them to send money that they would refund later. The targeted individual Facebook user would think it could be a friend that they knew and send them money. They would then discover that they had been defrauded by somebody who hacked their account.

Respondent 8 claimed that there was too much hate speech towards government leaders such as ministers. One girl wrote on Facebook page of Landless Peoples' Movement saying 'vootsek' to the president. In 2018 an individual was bullied for being gay on Facebook.

4.2.2.5. Perception on Namibia's cybercrime legal position

Respondent 1 had no idea on the cyber legal position of Namibia. Respondent 2, 3, 4, 5, 6, 7, and 8 agreed that Namibia does not have cybercrime legal framework. The Electronic Transaction and Cybercrime Bill was still to be passed. Respondent 5 stated that there were only provisions on Communication Act as the cybercrime bill were being drafted. Respondent 7 added that the Bill is still to be tabled in the Namibian parliament. Hopefully it will be promulgated in year 2019.

4.2.2.6. How do courts and the Namibian Police handle reported cybercrime cases?

All 8 respondents coincided that the police cannot do anything unless the crime committed was defined under common law or statutory laws. Both respondents emphasised that there could be no crime if there was no law. The cybercrime law was supposed to define crimes and their elements. Respondent 1 added that when an individual came to the police to report that their account was hacked, the police officer has to ensure that he or she registers the case according to the legality principle. Therefore it was possible to use alternative charges of common law such as fraud in case of hacking and identity theft cases when there was proof that money was taken from the account and suspect can be traced and linked to the commission of the crime.

Respondent 2 argued that, “In terms of the definition of cybercrime, we might have shortcoming, I don’t think all of it at this point in time is covered, and since it is not covered, the aspect of prosecuting it, detecting, investigating and apprehending culprits is lacking, therefore it will be difficult to take cybercriminals to court”. Respondent 3 claimed that there were a number of cybercrime cases reported, but however, one would not know if that was cybercrime because there was no law that defined such crimes and its elements. For example, if someone insulted the other person on Facebook or publish materials that contained pictures of the other, that person would be charged under statutory law for defamation of character.

Respondent 4 added that there was a cybercrime unit established within the Namibian Police Force. However, the absence of the law made everything difficult. It depends on the crime committed and whether there was evidence to charge the person using current statutes and the common law.

4.2.2.7. Perception on the challenges faced by the Namibian Police Force and the courts in dealing with cybercrimes.

***Lack of Legislation**:* Respondents 1, 2, 3, 4, 7, and 8 concurred that the biggest challenge was lack of legal framework that defined conducts as crimes. Respondents 1 and 3 stated that social media crimes were difficult to prove in the absence of a legal framework, because one has to know what crime was committed and what the required elements for such a crime are. As such people would continue to do as they please, because they know that there is no crime without a law. Cybercrimes could then increase and threaten human security of internet users. The law is supposed to limit citizens on committing crimes because they will fear prosecution.

Lack of infrastructures: Respondents 1, 3, 5, 6, and 8 identified lack of technological power to combat cybercrime as a major problem. Respondent 3 emphasised that the Namibian police lacked technological equipment and knowledge to deal with cybercrime and making it worse is that there was no framework that guided the police to handle reported and registered cases. Therefore the police fail to detect, monitor, prevent, and present cybercrimes evidence due to technological shortcomings.

Lack of a reporting mechanism*:* Respondents 1, 2, 4, 5, and 6 coincided that another challenge was the absence of the reporting mechanism that will help citizens to report cybercrimes to the relevant authority. Respondent 3 stated that the absence of law made citizens reluctant to report crimes because they know that the police would not do anything because there was no law that criminalised the act.

Lack of capacity*:* Respondents 1, 2, 3, 5, 6 and 7 agreed that there was lack of capacity for the police and public prosecutors to handle cybercrime. Respondent 1 stated that the police and prosecutors did not have skills to investigate and prosecute cybercrime. Respondent 5 added that there could be lack of capacity for the Namibian police, courts, CRAN and MICT as major stakeholders in combating cybercrime. As such, the lack of expertise on technical matters, such as preserving evidence, monitoring cybercrimes, detecting, preventing and investigating as well as prosecuting cybercrime cases remain cumbersome.

Respondent 7 claimed that it was important to prove allegations and in most cases the police lacked skills to testify in courts of law and some prosecutors have no cybercrime and social media experience to handle such cases. This means that many cases would be withdrawn and justice could not prevail if police cannot testify and present evidence to prove the accused person guilty.

Awareness challenge: Respondents 2, 3, 5 and 6 highlighted lack of awareness as a challenge. These respondents claimed that social media users lacked awareness of the danger of social media. The four respondents argued that some offenders commited crime not knowing that they were committing a crime either by posting photos of others or recording conversations, because there is no law that defines such acts as a crime. Respondent 3 stated that some social media users share contents about others on Facebook or WhatsApp viewing it as entertainment while some citizens do not know if their rights were violated on social media. Respondent 7 maintained that there could be a lack of social media and Internet users' education, especially among children.

***Service providers**:* Respondents 2 and 5 claimed that the process of dealing with cybercrime cases was cumbersome. When a complainant opened a case, service providers such as MTC were supposed to provide evidence and sometimes the police is supposed to get the search warrant from the court before the service providers release the information to the police in order to start the investigation. MTC and Telecom Namibia were sometimes unwilling to assist in tracing suspects or providing evidence needed by the police and courts and at other times they delayed investigation leading to evidence to be destroyed by the suspect.

***Unregistered sim cards**:* Respondents 3 and 7 commented that there were many unregistered sim card numbers and this was because most sim cards are bought in the street and Chinese shops. Any person can acquire a number and use it in one day to commit a crime and dispose of it leaving no trace. Respondent 7 also added that such unregistered cell phone numbers in most cases are used in committing crimes on WhatsApp groups and Facebook to blackmail, stalk and even to defraud others.

***Anonymity nature**:* Respondents 3, 5, and 7 coincided on the anonymity nature of cybercrime. They stated that anonymity of criminals made it difficult to trace them and the origin of the crime. Many people could circulate a sex video to many recipients and it would be impossible to charge all those people. Respondent 5 state that criminals hind their face and ensure that the police cannot be able to trace and link them to the crime.

Transnational challenge: Respondents 3, 4 and 7 agreed that the transnational nature of cybercrime impeded the prosecution of offenders. Respondent 4 added that it was difficult to determine the origin of the cybercrime due to its transnational or global aspect and the crime would go through multiple users by sharing and circulating such materials. Respondent 7 also claimed that it was difficult to have justice for a victim who was in Namibia while the offender was in another country.

Lack of evidence*:* Respondent 3 informed that the court work entirely depended on the police. The courts only worked on what they receive from the police, if the police cannot provide evidence then the offender cannot be prosecuted.

Jurisdictional power*:* Respondent 4 argued that jurisdiction power prove to be a problem. An offender might be in another country where the police does not have jurisdictional power to investigate that case, and as such the case would be withdrawn unless there was cooperation between the countries where the victim and offender are.

Expert willingness to testify*:* Respondent 4 remarked that some experts might be unwilling to testify in the court of law. For example, a medical doctor who treated a patient who was for instance physically assaulted or raped as a result of Facebook or WhatsApp conduct or being traumatised resulting from posts on social media may not be willing to testify. In the analysis of this, the patient might not receive justice if the medical doctor refuses to testify in court.

Lack of financial resources: Respondents 2, 4, and 5 posited that there was lack of financial resources to invest in technology and capacity building. High Technology might be necessary to monitor, detect, prevent and preserve electronic evidence of cybercrimes. In addition, money could be required to train cybercrime experts in Police, Justice and MICT who are the major stakeholders in social media crime combating.

4.2.2.8. Proposed strategies to deal with cybercrimes

Implementation of a law: All 8 respondents suggested that the government should speed up the formulation and passing of a cybercrime law to govern social media communications. Respondent 1 stated that the government should benchmark from other countries which were more advanced in cyber-security and laws. Respondent 2 added that MICT should involve the police in fighting cybercrime in the country; they should have policies and should push for the Cybercrime law to be passed to regulate social media contacts, ensuring that there was proper flow of information which was also secure. Respondents 3, 4, 5, 6 and 7 agreed that the law would define social media conducts as crime and provide punishment for each act.

***Capacity Building**:* All 8 respondents proposed that it was important to build capacity for all cyber security stakeholders. Respondent 1 suggested that the government should identify government units such as MICT and the Police to be trained and capacitated in cybercrime field and be able to lead the country's cyber security and assist in cyber investigation to ensure prosecution of cybercriminals. Respondent 2 added that training of police members should be a priority; basic, advanced, and in-service training in cybercrime area should be a must from all stakeholders to ensure proper handling, investigation and solving of cybercrime cases. Respondent 3 suggested that MICT should employ cyber specialists that can assist with the investigation by providing evidence and detecting or monitoring crimes on social media.

Technological infrastructure: Respondents 2, 3,4,5and 7 recommended that the government should build and invest in technological infrastructure and set up a mechanism to detect, monitor, investigate, gather evidence and prosecute cybercriminals. The government should allocate sufficient funds to cyber-security programmes.

***Awareness Campaign**:* Respondents 1, 3, 4, 5, 6, 7 and 8 suggested that the government should conduct a cybercrime awareness campaign. Respondent 1 stated that police and MICT should have a public platform on the radio or television to hear from members of the public what is happening on the ground as they were the most affected by social media threats. Respondent 2 added that awareness campaign was crucial to educate the community, therefore constant awareness to the community to know their rights, how they can be violated on social media and to report security threats was a necessity. Respondent 5 suggested that public education and awareness campaign through public meetings; radio or television programmes should be broadcasted in all languages to ensure inclusivity of all citizens. There must be moral education in schools, churches and radio programmes focusing of public indecency and obscenity.

Joint stakeholder's cooperation: Respondent 2 informed that there was a memorandum of understanding between CRAN and the Namibian Police Force which was still to be signed before they can work close to deal with social media criminals. This joint effort will curb the free ranging of criminals on social media. There was no MoU with MICT, which was another area that needed attention.

Service provider*:* Respondent 2 stated that service providers should be involved in the fight against social media crimes, and provide necessary support to the police and the courts. Respondent 4 proposed that the Namibian government should have an agreement with the social network companies that if Facebook is to be allowed in Namibia, certain contents are prohibited. This agreement would ensure control on the usage of social media. Other countries have such agreements, and some do not allow use of Facebook.

***Reporting of cybercrime**:* Respondent 3 proposed that the internet users should be encouraged to report crimes and should at least wait for the police to act because if there was evidence, the suspect would be arrested. Respondent 5 stated that there should be a monitoring and reporting mechanism to allow pro-activeness.

Registration of sim cards: Respondent 2 and 7 shared that all telecommunication companies such as MTC, Leo and Telecom Namibian should make sure that no sim card can be active if it was not registered verifying the owners Identity Document and proof of residence. This would allow all citizens and residents without registered cell phone numbers to register them and when such sim numbers were used in committing a crime on WhatsApp groups and Facebook the police would be able to trace the suspect and prosecute social media violations in the court.

4.3. Discussion of the findings

The primary objective of the study was to design a strategy for the social media implications on human security in Namibia using a case study of Windhoek. The first part of discussion, section 4.3.1, presented the demographic information of the respondents, while 4.3.2 discussed the findings in line with the research questions of the study below:

1. What are the human security implications of social media crimes in Namibia?

2. In the absence of the supportive legislation, what are the challenges for the Namibian Police in dealing with social media crimes that are threatening human security?

3. What strategy should NAMPOL adopt to deal with cyber social media crimes?

The research questions were addressed by analysing empirical (qualitative questionnaire and interview) data and reviewing literature related to this study. The questionnaires and interview comprised the same 7 questions and one additional question on the interview which could not be applicable to the members of the public. Question 6 was addressed by analysing empirical data, while the rest of the questions were addressed by analysing both the literature review as well as the empirical data.

4.3.1. Profiles of the Respondents

This section presents data about the demographic characteristics of the respondents.

The details below reflect the respondents’ gender, age and research group categories.

Results presented at the beginning of this chapter, figure 1 and 2 showed respondents` gender representation. Furthermore, key informants interviewed were eight; three from Ministry of Justice (one Lawyer, one Prosecutor and one from Law Society of Namibia), 3 from the Namibian Police Force (one Legal Service Directorate, one Criminal Investigation Directorate and one Public Relations Division) and one from Communication Regulatory Authority of Namibia. All the respondents were selected because of their key functions in relation to the research questions.

4.3.2. Discussions of the Findings According to Research Questions

4.3.3.1. Human Security Implications: This section responded to;

Research Question 1: What are the social media implications or threats to human security of persons in Namibia? Provide description based on the outlined seven dimensions of human security:

Economic Security: Findings presented earlier showed that there were various economic security implications emanating from usage of social media, specifically Facebook and WhatsApp in Namibia. Common economic threats identified were; daily purchasing of expensive data to stay online, internet fraud through online shopping (buy and sell on Facebook pages, where interested buyers were requested to pay deposit of the products price upon ordering them), theft by false pretence/ fraud (many people deceived through buying of goods and products such as hair, car, houses, clothes and electronic items on Facebook and WhatsApp and they have not received their money or items back. An incidence of a man who paid a deposit of N$ 100 000.00 for a car advertised on Facebook only to have the seller vanish into thin air is a case in point. Another economic implication found was that Windhoek residents have a habit of posting their holiday locations and their wealth possessions and this put them in danger of being robbed of their properties and their houses to be broken by criminals while they were on vacations.

Individuals also hack other users' Facebook accounts and claim to be in emergency situations and request someone's Facebook friends to send them money on e-wallet, easy wallet and blue wallet. Cases of identity theft where individuals' identity were stolen from social media and their details were used to defraud them by stealing money from their bank accounts were also common. An incidence of someone who stole N$ 400 000.00 from someone's bank account was an example. Lastly, a majorityof Windhoek residents fell victim to financial scams such as My Life Change where people invested their money and they do not get it back, while some fell victims of scams of winning awards or scholarships messages on WhatsApp and Facebook and when they provide their banking details, they got defrauded.

The findings were supported by the findings of Singh (2014) who found that the human security threats of economic nature are perpetrated through hacking of critical informational systems of individuals or stealing their identity electronically, causing them economic loss. However, the situation of buy and sell on Facebook Page is a new finding where individuals lose money and valuable properties through theft under false pretence.

Similar findings were reported by UNODC (2013) who revealed that consumer victims of cybercrime in 24 countries across the world reported that they suffered average direct losses of between 50 and 850 US dollars as a result of a cybercrime incident(s) experienced in one year. Around 40 per cent of these costs were reported to consist of financial loss due to fraud, almost 20 per cent due to theft or loss, and 25 per cent to repairs. McAfee Inc (2014) as cited in Adesina (2017) also noted that the cost of cybercrime includes the effect of hundreds of millions of people having their personal information stolen.

Personal Security: Personal security results presented showed that all respondents agree that social media poses a serious personal security to Facebook and WhatsApp users. Spreading of hate speech, cyber bullying, defamation of character, violation of privacy and dignity of others by posting sex videos and naked pictures of others on social media were the most common threats towards one’s personal security. Moreover, respondents also indicated that sharing physical location and posting personal information on WhatsApp and Facebook leads to physical attacks by those who have intention to harm other persons because they can easily find them, and it also leads to housebreaking cases which is common in Windhoek. Some respondents noted that social media platforms were often used by criminals in human trafficking directed to women and children and social media was rated as the cause of some passion killing cases because of posts or information shared causing men to be violent and brutal towards their partners. On the other hand, the results showed that social media has been facilitating commission of crimes such as grooming, kidnapping, human trafficking and robbery.

The results were consistent with the findings of a study by Singh (2014) and UNTFHS (1999) who believe that the personal aspect of human security was so vital for people as their security from physical violence. The personal security threats take several forms such as gangs against other individuals or gangs (crime, street violence). In another related study Mengu and Mengu (2015) found that the incidents of violence on social media such as porn sites, especially child porn, visual material displaying excessive violence, campaigns of abuse towards individuals and institutions very much on the ascendancy. Similar studies by Sinca and Mascas (2015) and Hughes (1997) as cited in Gitonga (2014) also reveal that social media was a new technique used by traffickers. The Internet was therefore becoming the biggest market for the buying and selling of sexual services

Dwivedi (2018) found that by posting personal information on social networking services, the user created a hazard to personal security. For example, revealing that you would be away from home, especially if your address was posted in your profile, increased the risk that your home could be burglarized.

Community security: Results on community security shows that 15 respondents agreed that Facebook and WhatsApp enabled individuals to share fake news that caused confusion in the community. They observed that people lacked humanity, when at accident scenes as they are interested in taking pictures and videos to share on social media instead of rescuing victims. Twelve respondents gave an example of a boy who was killed by bull dogs in 2015 in Windhoek while people were in their cars taking videos. Five respondents believed that their children were not safe; they faced danger of grooming for sex and kidnapping. A total of 10 respondents claimed that Facebook and WhatsApp were destroying legal marriages through exposure of infidelity. Aggrieved parties in such relationships often resort to divorce or suicide and this break up families.

Another 7 respondents believed that social media facilitates crimes putting community security at risk. Some 5 respondents highlighted hateful tribal speeches as destroying unity among community members. Similarly, 9 respondents expressed concern with immorality such as distribution and circulation of pornographic and obscene materials. Most of the respondents complained that Facebook was eroding Namibian cultures because young people were copying western cultures. Another community security threat identified was recruitment of criminals on social media for human and drug trafficking, terrorism and other criminal activities. Lastly, some respondents maintained that social media allowed citizens to express and demand rights to activities prohibited by laws which could destroy the community such as the transgender rights which was raised up on social media.

The finding was supported by the results of a study by Kamp (2016) who found that the biggest change impacting the media industry today was how consumers are getting their news. Due to the lack of regulations and standards, abuse in forms of spreading false information and rumors, defamation and hate speech could hardly be prevented. Similar findings were also reported by Nsude and Onwe (2017) who found that social media also became a platform for the dissemination of false reports and sometimes, these false reports spread so quickly. The same study revealed that terrorist groups used chat rooms, dedicated servers and websites and social networking tools as propaganda machines, means of recruitment and organization, for training grounds and for significant fundraising through cybercrime. However, issues of culture erosion and transgender rights were new findings in the study.

Environmental Security: The findings of the study showed that social media has implications on environmental security. The posts that individuals update and share on Facebook or WhatsApp could pose threats to wildlife with criminal activities such as illegal hunting and poaching of endangered species (rhino and elephants). Some believe that images might be shared on social media may incite criminals to engage in illicit trading of natural resources (timber), mineral recourses (diamonds), and illegal fishing in case of marine resources. However, there was no study found on the impact of social media towards the environmental security dimension.

Food Security: The findings of this study on food security showed that social media indeed impacted upon food security. Individuals spread rumors about food poisoning and declare some foods not safe for consumption without consultation with the Ministry of Health which is mandated to make such pronoucements. Respondents claimed that anybody could make up a video of how certain foods were processed in an unhealthy manner, such as can fish, rice and post it on social media and when individuals watch such videos they might stop eating fish and rice. There was an outbreak of listeriae bacteria on processed polony and individuals misled others on Facebook stating that even other processed foods should not be consumed. This was a serious food security concern in Windhoek; because some individuals could only afford buying certain foods and others rely on particular foods for survival. Nevertheless, there was no study found on how social media affected food security.

Health Security: The results presented on health security indicated that social media affects the health of individuals in many ways. Respondents claimed that individuals sell products on Facebook and WhatsApp status such as diet pills, remedies for hypertension, diabetics and many other diseases. Majority of people selling such products do not provide prescription and warnings on the side effects of the products, and as a result some consumers get health complications, while others stop taking medically proven remedies and this puts their health at risk. Sixteen respondents informed that many fake pastors and witch doctors or traditional healers took advantage of Facebook to advertise themselves as healers of many diseases including cancer and HIV/ADIS. As a result many people on ARV treatment drop their medications and seek help from pastors and traditional healers who only give them herbs to drink or smoke and so called anointed oil and water which allegedly cast demons from the patients. Diseases spread when the pastors and witch doctors have sexual relationships with married women and men when seeking to be healed. Ten respondents further stated that social media was very addictive and many youths spent time alone on Facebook and WhatsApp and do not get enough sleep. Importantly, Facebook and WhatsApp increased stress among teenagers when they get bullied at school and homes.

Few studies support the findings on social media implications on health security. The addiction results supports the findings by Amedie (2015) on the study conducted by psychologist Dr. Mark Becker, of Michigan State University, who found a 70% increase in self- reported depressive symptoms among a group using social media and a 42% increase in social anxiety. Clearly excessive social media usage leaves one prone to be at a higher risk of depression, anxiety, and ultimately stress.

A similar study by Pozza, Pietro, Morel and Psaila (2016 **),** and Williams and Pearson (2016) also support the findings on cyber bullying, that new technologies have resulted in a rise in cyber bullying cases in recent years. Cyber bullying can result in depression, loss of confidence, fear, isolation and relationship problems, self-harming and suicide. Victims can experience psychological maladjustment, social isolation and feelings of unsafe.

Political Security: The result showed that social media has implications on political security of individuals. Majority of the respondents claimed that individuals can discuss sensitive political security agendas on Facebook pages and WhatsApp groups which can influence individuals to join terrorist groups, overthrow the government and commit sedition. Hateful speeches towards political leaders can lead to bad governance and corruption in the country, and majority will suffer the effect of such bad governance. One study conducted in Nigeria by Nsude and Onwe (2017) supports the terrorist findings, stating that many lives have been lost through Boko Haram insurgency. In Nigeria, Boko Haram leaders continue to use Facebook, YouTube, Twitter and other Jihadist networks as a means of recruitment and organization, for training grounds and for significant fund-raising through cybercrime. However, there are no other political security related studies found apart from terrorist activities involving social media.

4.3.3.2. This section responded to Research **Question 2: Briefly shareyour experience of the cybercrime situation in Namibia specifically those committed on Facebook and WhatsApp.**

The results showed that respondents agreed that cybercrime was a serious matter in Namibia, and most of the people lacked knowledge of cybercrimes, hence they have fallen victim to fraud, their accounts being hacked, being defamed, blackmailed, bullied and mostly their privacy being violated on Facebook and WhatsApp platforms. The results further showed that the common trend in Windhoek is exposing of individual sexual acts, mostly nude videos and pictures of people being shared on Facebook and WhatsApp without the consent of the victims and this has reputational harm. The exposing of individuals put their lives in danger through domestic violence and passion killing which also became common in Windhoek in the past years. Further, cyber bullying was also on the increase among young children and this affected their academic performance. Respondents stated that many people lost their money through online shopping, identity theft, theft under false pretence when buying items and products and hacked accounts. Despite these incidences, people blindly continue to trust people they do not know and they become victims of fraud and theft every day.

Some respondents informed that criminals explore the use of social media and approach unsuspecting victims under false pretence and rob them of their properties or groom them. However, some believe that the cybercrime situation in Namibia was normal compared to other countries such as South Africa.

In support to the findings, Barman (2015) found that privacy is infringed when a hacker accesses a person's profile by hacking their account on a particular social networking website. Another study by Rose as cited in Punjabi (2014) also found that there are greater chances of private information becoming public, which opens users to serious security risk as the information is easily transferred between social media sites. Supporting the findings was another related study by Morgan (2017) who found that cybercriminal activity could be one of the biggest challenges that humanity will face in the next two decades. Cybercrime costs include damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, and post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm.

Another study by Mengu and Mengu (2015) also support the findings, revealing that there are incidents of violence on social media. Porn sites, especially child porn, visual material displaying excessive violence, campaigns of abuse towards individuals and institutions or black propaganda, negative labelling, misdirecting people by establishing contact with fake identities (for instance, kidnapping or enslaving women and children on the pretext of employing them as well as the theft on social media (idea or money) are other cybercriminal activities.

4.3.3.3. This section responded to **Research Question 3: To what extent are the following social media crimes committed on WhatsApp and Facebook in Namibia?** Rate each crime from 1 to 5, 1 being most prevalent and 5 the least.

Results presented in Table1 and 2 showed a list of some of the social media crimes committed in Windhoek through WhatsApp and Facebook whereby respondents were requested to rate the crimes according to their occurrence from 1 to 5 (1 being the most prevalent and 5 the most least). The combined results of table 1 and 2 showed that the most prevalent social media crimes rated 1 were; Distribution and circulation of obscene materials 94.4%, followed by cyber bullying 72.2%, defamation of character 66.6%, hate speech 61.1.%, cyber stalking and pornography 55.5%, sexting 50%, identity theft and internet fraud 44.4%. The prevalent crimes rated 2 were; breach of privacy 44.4%, and child pornography 33.3%. While the moderate crimes rated 3 are; grooming 50%, identity theft and phishing 27.7%. Hacking of personal computers and accounts 33.3% and drug and human trafficking 27.7% appear to be the least prevalent crimes rated 4, while cyber terrorism happen to be the least prevalent social media crime.

A related study conducted by Wong (2005) supports the result that distribution of obscene materials was prevalent. Globally, the third largest crime in 2003 was publication of obscene materials on the internet at fifty-eight cases. This represented 9.9% of reported crimes, supporting the results is another study by OECD (2012) who found the cyber bullying prevalence rates across countries. High prevalence rates of cyberbullying were recorded in Australia at 6.6% from year 4 to 9 in 7 500 schools, 21% of 652 young persons aged 11-17 United States, 11% of grade 6-8 ,50% of teens aged 13 to 18 .55% of student aged 12 to 15 China, 65% aged 11 to 14 United Kingdom, 22% aged 11 to 16 Europe, Iceland with 15% of 9-16 year-olds, Estonia with 31% of 6-14 year-old.

Similar studies that support the results on the prevalence of defamation on social media are findings by UN (2013) who found that a number of countries in Northern Africa and South-Eastern Asia noted cybercrime trends of 'more and more frequent use of social networks for defamation and propaganda,' as well as 'an upward trend in acts related to reputation and privacy' and 'libellous online postings'. The results matched the findings of Kobek (2017) who posited that in 2013, Mexico held the number one position in the world for pornographic material involving minors. UNODC (2013) added that during information gathering for cybercrime, acts involving child pornography were reported to constitute almost one third of the most commonly encountered cybercrimes for countries in Europe and the Americas. The same study by Kobek (2017) contradict the result on human trafficking by stating that an estimated 800,000 adults and 20,000 children are trafficked for sexual exploitation, where some of the children become part of Mexico´s lucrative US$30 million a year pornography industry.

The results of internet fraud and sexting being prevalent was supported by the findings of a study by Davis (2010) who reveal that in North Carolina the most frequently investigated computer crimes by an average reporting agency were fraud related (79.3%), criminal threatening (8.5%), and online enticement of minors/child pornography (4.9%). Moreover, the results dispute the findings of a study done by UN (2002) which revealed that concerns were also expressed about the increase in identity theft, in which personal data are used to allow offenders to impersonate the individual whose data were stolen.

Contrary to the results, the findings of a study by King and Sutton (2014) as cited in Williams and Pearson (2016) found that there was an association between terrorist acts and a rise in hate crime incidents in the US. Convincingly, they show that following the 9/11 terrorist attack, law enforcement agencies recorded 481 hate crimes with a specific anti-Islamic motive, with 58 percent of these occurring within two weeks of the attack (4 percent of the at risk period of 12 months).

The results show that the crimes with less prevalence percentage in Ghana, defamation and cyber stalking were the ones with high percentages in Namibia. The results thus opposed the findings of a research carried out in Ghana with 200 students in Sunyani Senior High School which revealed that the most prevalent forms of cybercrime is hacking 20%, credit fraud 18%, identity theft 11%, pornography 10%, sweetheart swindle (social networking) 7.5%, defamation 5% and cyber stalking 3.5%, among other forms (Warner, 2011) as cited in Barfi, Nyagorme and Yeboah, 2018).

4.3.3.4. This section responded to **Research Question 4: In your opinion, how are the social media crimes committed on Facebook and WhatsApp platforms?**

The results from the study showed various ways of how social media crimes are committed on Facebook and WhatsApp. Criminals would advertise services or products for sale such as flats, houses and vehicles which they do not have and they will ask interested clients to pay certain amounts of money as a deposit. Some respondents claimed that some people hack Facebook users' accounts and unfriend them after they have tampered with their private settings. They steal the users' identity for selfish reasons. While Facebook allows anyone to search for anybody they are interested in even if they are not their friends on Facebook, the consequence is that criminal-minded people can post unwanted pictures and videos on anybody's profile. Others befriend people on Facebook with the intention to groom them for sex or prostitution.

Five respondents also claimed that criminals create fake Facebook accounts and approach unsuspecting victims under false pretence to defraud them. Sixteen respondents informed that a majority of people have a habit of sharing pornographic materials to many Facebook and WhatsApp users and mostly circulate images and videos of others while having sex. These acts humiliate and shame the victims. This habit also constitutes a breach on other people's privacy by invading their personal life, recording videos and pictures of individuals without their consent and uploading them on Facebook. Three (3) respondents added that Windhoek residents developed a habit of sharing confidential information about others such as health records and extort them for money. Eight (8) respondents claimed that some individuals pretend to sell products online and when they receive money from clients they block their numbers and de-activate their Facebook accounts.

Another 8 respondents concurred that Facebook and WhatsApp platforms are used by criminals to locate and trace targeted people to commit crimes such as robbery. The results further showed that there are individuals who share news about death of others on Facebook or WhatsApp while the relatives are not officially informed. Four (4) respondents stated that many people receive messages that they have won certain amounts of money or scholarships and they should send banking details and some transport money to send the award, and and the recipient is duped in the process. Some respondents stated that anybody could just post hateful speeches or statements that defame the next person on Facebook.

The results were supported by a study done by Mengu and Mengu (2015) who found that porn sites especially child porn, visual material displaying excessive violence, campaigns of abuse towards individuals and institutions or black propaganda, negative labelling, misdirecting people by establishing contact with fake identities (for instance, kidnapping or enslaving women and children on the pretext of employing them as well as theft on social media (idea or money) were on the increase. Another study by Amedie (2015**)** also supported the findings that social media fosters a false sense of online "connections" and superficial friendships leading to emotional and psychological problems. Social media has become a tool for criminals, predators and terrorists enabling them to commit illegal acts. A similar study by Sinca and Mascas (2015) support the findings stating that Facebook plays an important role in the grooming of victims. These networks allow criminals to directly contact victims to pretend to be their age to gain their trust and then reaching them to the moment of being sold and exploited.

4.3.3.5. This section responded to **Research Question 5: What is Namibia's legal position with regard to cybercrime?**

The results showed 17 respondents agreed that Namibia does not have any legal framework for cybercrime. However, the Bill was being drafted and would be passed soon. Supporting the findings was the study by Council of Europe (2015) who found that majority of African States (30) did not have specific legal provisions on cybercrime and electronic evidence in force. Draft laws or amendments to existing legislation reportedly had been prepared in at least 15 States (Burkina Faso, Djibouti, Ethiopia, Guinea, Kenya, Lesotho, Mali, Morocco, Namibia, Niger, South Africa, Swaziland, Togo, Tunisia, and Zimbabwe). Another study also supported the findings, claiming that the Namibian parliament had intended to table the new Transactions and Cybercrime Bill in 2017, which was placed on the parliamentary agenda by Minister of Information and Communication Technology. However, the bill was removed from the agenda and it was unclear why it was pulled and when it would be placed back on the parliamentary agenda again (Links, 2018).

4.3.3.6. This section responded to **Research Question 6: How does the Namibian**

Police deal with reported social media crimes in the absence of cybercrime legal framework?

Results showed that all 18 respondents coincided that the police cannot do anything unless the crime committed was defined under common law or statutory laws. Both respondents emphasised that there was no crime if there is no law. The cybercrime law was supposed to define crimes and their elements. Two (2) respondents state that there was a cybercrime unit established within the Namibian Police Force. However, the absence of the law made successful prosecution of cybercriminals difficult, with the unit depending on the crime committed and whether there is evidence to charge the person using current statutes and the common law.

Supporting the results were the findings of Ajayi (2015) who posited that the enforcement of cybercrime laws has largely been hampered due to inadequate legislations and the ineffectiveness of the same where there are extant laws in place for cybercrimes. Another study by Goodman and Brenner (n. d) also states that the laws of most countries do not clearly prohibit cybercrimes. Downing (2005), as cited in Brown (2015) also supports the findings that many cybercrime offenders have evaded prosecution due to weaknesses in substantive criminal laws that do not address technological means of offending.

4.3.3.7. This section responded to **Research Question 7: May you please name some of the challenges faced by the Namibian Police and courts in dealing with social media crimes which threaten human security?**

Lack of Legislation: The results from the study indicate lack of legislation as a concern. Thirteen (13) respondents concurred that the biggest challenge is lack of legal framework that defines conducts as crimes. These respondents stated that social media crimes are difficult to prove in the absence of a legal framework, because one has to know what crime is committed and what are the required elements for such a crime. As such people will continue to do as they please, because they know that there is no crime without a law. Cybercrimes will then increase and threaten human security of internet users. The law is supposed to limit citizens on committing crimes because they will fear prosecution.

This result was supported by the findings of Ajayi (2015) who found that the enforcement of cybercrime laws have largely been hampered due to inadequate legislations and the ineffectiveness of the same where there were extant laws in place for cybercrimes. Goodman and Brenner (n. d) also support the results by claiming that that the laws of most countries do not clearly prohibit cybercrimes.

Lack of infrastructures: Results show that 6 respondents identified lack of technological power to combat cybercrime as a major problem. The respondents emphasised that the police lack technological equipment and knowledge to deal with cybercrime and that there was no framework that guides the police to handle reported and registered cases. The police thus find it difficult to detect, monitor, prevent, and present cybercrimes evidence due to technological shortcomings. Supporting the findings were the study done by Bromby (2006) as cited in Brown (2015) who found that many cybercrimes were sophisticated and well-conceived, requiring police to apply technological expertise and deductive reasoning to unravel complex 'modus operandi' and substantiate elements of an offence. Kubic (2001) as cited in Kader and Minnaar (2015), also claim that in some cases, local police forces do not understand or cannot cope with technology. A similar study by Wall (2011) complements the results that the relationship between the police and technology is long-standing and complex. The police’s responsive and localised nature always meant that they fell behind in their access to, and use of, technology. The challenge was that law enforcement agencies do not have the facilities to keep up with criminals, especially with regards to offences that require high policing.

Lack of a reporting mechanism: The results revealed a lack of reporting mechanism as a challenge. Respondents coincided that there was no a reporting mechanism that will help citizens to report cybercrimes to the relevant authority. This made citizens reluctant to report crimes because they would know that the police would not do anything because there was no law that criminalised the act, so they do not report. This result was matched by the one of UNODC (2013) who found that one global private sector survey suggests that 80 per cent of individual victims of core cybercrime does not report the crime to the police. Underreporting derives from a lack of awareness of victimization and of reporting mechanisms, victim shame and embarrassment, and perceived reputation risks for corporations. In support, Wall (2011), UNODC (2013), and Ajayi (2016) concur that the most revealing challenge was the under-reporting of cybercrimes to the police.

Lack of capacity: Results showed that 9 respondents agreed that there was lack of capacity for the police, lawyers and public prosecutors to handle cybercrime cases. The respondents stated that the police did not have skills to detect, prevent and investigate cybercrime and the courts lacked the same expertise to prosecute such. As such the lack of expertise on technical matters, such as preserving evidence, monitoring cybercrimes, detecting, preventing and investigating as well as prosecuting cybercrime cases remained cumbersome.

Some respondents claimed that it was important to prove allegations and in most cases the police lacked skills to testify in court of law and some prosecutors have no cybercrime and social media experience to handle such cases.

This result was matched by the findings of a study by UNODC (2013) who found that both law enforcement investigators and prosecutors mean that ‘brought to justice’ rates are low for cybercrime offenders. Very few countries were able to provide data on persons prosecuted or convicted. Courts showed minimal levels of specialization for cybercrime, many countries only specialized in judicial services. Majority of cases were handled by non-specialized judges, who, in many countries did not receive any form of cybercrime-related training. also in support UNODC (2013), Pieterse (2015), Akuta et al (2008) as cited in Mushumba (2016) overlapped in supporting the results that in many countries, investigation of cybercrime and crimes involving electronic evidence were not well resourced and suffered from a capacity shortage. Some 70 per cent of specialized law enforcement officers in less developed countries were reported to lack computer skills and equipment.

Lack of awareness: Four (4) respondents highlighted lack of awareness as a challenge. They stated that there was a lack of awareness from the victims and most of them did not know the danger of social media and that their rights were being violated in certain ways while on Facebook and WhatsApp. They added that some offenders committed crime not knowing that they were committing a crime either by posting photos of others or recording conversations, because there was no law that defined such acts as crime. The four (4) respondents maintained that there was lack of social media and internet users' education, mostly among children.

The findings of Doshora, (2011) support the results that one important reason that the Act of 2000 was not achieving complete success in Delhi was the lack of awareness about their rights among the citizens. Another study by Gharibi and Shaabi (2012) agree with the results that different types of cyber threats in social networks happen due to the fact that most of the users are not concerned with the importance of the personal information disclosure and thus they were under the risk of over disclosure and privacy invasions.

Service providers: The results show that there was a challenge posed by service providers. Two (2) respondents claimed that the process of dealing with cybercrime cases was cumbersome. Once a person opened a case, the service providers such as MTC were supposed to be involved to provide evidence and sometimes the police was send back to get the search warrant from the court before the service providers released the information to the police in order to start the investigation. As such service providers were sometimes unwilling to assist in tracing suspects or providing evidence needed by the police and courts and sometimes, they delayed investigation leading to evidence being destroyed by the suspect. Matching the results was the finding by UNODC (2013) who found that many countries noted that significant challenges were faced in obtaining information from service providers. Service providers do not store computer data for ‘long enough’, and that it ‘takes too much time for the subscriber to provide the data to the police.

Lack of financial resources: Three (3) respondents informed that there was lack of financial resources to invest in technology and capacity building. High Technology could be necessary to monitor, detect, prevent and preserve electronic evidence of cybercrimes. In addition, money might be required to train cybercrime expertise in police, justice and MICT who were the major stakeholders in social media crime combating. Akuta *et al*., (2008) support the results by asserting that the most serious challenge in Botswana was the lack of resources and the limited capacity available to train police officers to investigate. A study by Wall (2011) matched the findings that over a century readers of the Police Review and other contemporary police journals were regularly told by police correspondents that they lacked the resources to obtain the latest technologies that would help them to respond to criminals. And a similar study by Keane (2016) found that resources have not followed; nor have they been sufficient to enable proactive as well as reactive policing, or been devolved to local police forces to address low-value, high-volume cybercrime.

Unregistered sim cards: Two (2) respondents commented that there were many sim card numbers which were not registered in Namibia and this was because most of the sim cards were bought in the street and in Chinese shops, thus any person could acquire a number and use it in one day to commit a crime and dispose of it leaving no trace. The unregistered cell phone numbers were in most cases used on WhatsApp groups and Facebook to blackmail, defame, stalk and defraud others. The researcher has not come across studies that identified unregistered cards as a challenge for policing cybercrime.

Anonymity nature: The results showed that 5 respondents indicated anonymity of social media as a challenge. They stated that anonymity of criminals made it difficult to trace them and the origin of the crime. For instance, many people would circulate a sex video to many recipients and it was impossible to charge all those people. Criminals hid their faces and ensured that the police cannot be able to trace and link them to the crime. Related to the findings is the study by Ajayi (2016) who found that one of the greatest impediments against global efforts towards stemming the whirlwind of cybercrimes remained the anonymous nature of the identity of cybercriminals. Another study conducted by Pieterse (2015) supported the results by adding that the challenge facing law enforcement in relation to the cybercrime phenomenon was in essence a faceless one, as it was extremely complex to determine the true identity of a cybercrime perpetrator or identify the geographical location from where the cybercriminal operates or predict a pattern of behaviour.

Transnational challenge: Five (5) respondents informed that the transnational nature of cybercrime hindered the prosecution of cybercrime offenders. These respondents added that it could be difficult to determine the origin of the crime due to the transnational or global aspect of cybercrime and the crime could go through multiple users by sharing and circulating such materials. Respondents also claimed that it proved difficult to have justice for a victim who was in Namibia while the offender was in another country.

Two (2) respondents claimed that jurisdiction power proved to be a problem, as an offender might be in another country where the police did not have jurisdictional power to investigate that case. As such the case would be withdrawn unless there was cooperation between the countries where the victim and offender were. The results were supported by previous studies of Rosewarne (2012), and Choudhury, Basak and Guha (2013) who found that cybercrime was borderless by nature; hence this made criminal investigations more complicated for law enforcement authorities. Cybercrime was a global criminal phenomenon which blurred the traditional distinction between threats to internal and external security and did not respond to single jurisdiction approaches to policing. Snell (2015) also supports that cybercrime was often transnational with the offenders operating in a different country to that in which the victim lived and the police were working. The use of proxy servers, physical distance, international politics, and lack of legislation and national agreement to give up suspects for trial in another country, all make it difficult to investigate cybercrimes and often impossible to bring the offenders to justice.

Lack of evidence: Three (3) respondents informed that the court work entirely depended on the police. The courts only worked on what they received from the police, and if the police cannot provide evidence then the offender cannot be prosecuted. In addition, the police lacked skills to gather and preserve and present evidence in court of law. Supporting the results was a study by Mislan, (2010) as cited in Brown (2015) who found that despite the pervasiveness of digital information, many police officers and prosecutors were hesitant to collect and present intangible sources of evidence. In support, Ajayi (2016) also found that the nature of evidence, that is forensic, needed in the prosecution of cybercrimes was expensive because of the high- tech equipment, materials and expertise involved to carry out such investigations, travelling and interpreting cost due to language barriers as opposed to gathering of evidence in terrestrial crimes.

4.3.3.8. This section responded to **Research Question 8: Please propose some strategies that should be adopted by the Namibian Police, MICT, and CRAN to deal with social media crimes.**

Adequate legislations

The result showed that all 18 respondents suggested that the government should speed up the formulation and passing of a cybercrime law to govern social media communications. Some respondents stated that the government should benchmark from other countries who were more advanced in cyber security and laws. Respondents believed that the law would define social media conduct as crime and provide punishment for each act. Moreover, all respondents commented that the cyber legal framework would guide the Namibian Police and courts in dealing with cybercrime, thereby making arresting, investigation and prosecution effective and efficient. The only study that supported the results was the finding of Seger (2012) who maintained that states should adopt legislation that was harmonised with international standards in order to criminalise conduct and provide law enforcement with procedural law tools for efficient investigations

Capacity Building

The results showed that 12 respondents proposed that it was important to build capacity for all cyber security stakeholders. They added that the government should identify government units such as MICT staffs, courts and the Police to be trained and capacitated in cybercrime field and be able to lead the country's cyber security and assist in cyber investigation to ensure prosecution of cybercriminals. Some respondents suggested that training of police members should be a priority, both basic and advanced in- service training in cybercrime area should be a must from all stakeholders to ensure proper handling, investigation and solving of cybercrime cases. Some suggested that MICT should employ cyber specialists that can assist with the investigation by providing evidence and detecting or monitoring crimes on social media.

A study by Cassim (2011) supports the findings that states should introduce specialised law enforcement and training skills. There should also be continuous research and training of personnel in the security, finance, judicial and police enforcement sectors to keep abreast with evolving technology. Another study that supports the result was conducted by Snell (2015) who posits that the Mainstream Cybercrime training in South Africa was designed to enable all police officers and staff to be able to respond to digital crime.

Technological infrastructure

The results showed that 6 respondents proposed that the government should build and invest in technological infrastructure and set up a mechanism to detect, monitor, investigate, gather evidence and prosecute cybercriminals. The government should allocate sufficient funds to cybersecurity programmes. Matching the results was the study by Chander (2015), who revealed that in India, some intelligence agencies and Mumbai Police have set up social media monitoring labs. Delhi Police was also contemplating such a cell and has floated ·expression of interest for implementation of “Open Source Intelligence (OSINT)” solution.

Awareness Campaign

The results revealed that 11 respondents suggested that the government should have a cybercrime awareness campaign. Some respondents proposed that the police and MICT should have a public platform on the radio or television to hear from the members of the public what was happening on the ground as they were the most affected by social media threats. There could be a need for constant awareness to the community to know their rights, how they could be violated on social media and to report personal security threats. In most cases women spoke about wrong things in the society and men hardly do, therefore all people should speak out how they were affected by social media crimes and let the nation know the negative effect of social media".

Respondents also suggested that public education and awareness campaigns through public meetings, radio or television programmes should be broadcasted in all languages to ensure inclusivity of all citizens. Some said there must be moral education in schools, churches and radio programmes focusing on public indecency and obscenity. Individuals should learn to be ethical and not post or circulate obscene materials".

The results were fully reinforced by previous studies of the UN cybercrime surveys report findings which stated that all stakeholders highlight the continued importance of public awareness-raising campaigns, including those covering emerging threats, and those targeted at specific audiences, such as children (UN 2013). Similar findings by Cassim (2011) support the same by stating that it was imperative to educate the public about the threat of cybercrime as ignorance has been mooted as one of the main reasons that Africans fall victim to cybercrime. Livingstone et al. (2011) as cited in Hof and Koops (2011) suggested that stimulating digital literacy and safety skills should therefore be a primary policy objective.

Joint stakeholder’s cooperation

Respondent 2 informed that there was a memorandum of understanding between CRAN and the Namibian Police Force which was still to be signed before they can work closely to deal with social media criminals. This joint effort would curb the free ranging of criminals on social media. There was no MoU between the Namibian Police and MICT which could be needed as well. Matching the results were the findings of a study done by UNODC (2013) which found that public-private partnerships are central to cybercrime prevention. Private sector entities are most often involved in partnerships, followed by academic institutions, and international and regional organizations. Partnerships are mostly used for facilitating the exchange of information on threats and trends, but also for prevention activities, and action in specific cases.

International cooperation

The results showed that 3 respondents informed that the state should benchmark from other countries on how they are dealing with cybercrime. They added that Namibia should sign extradition treaties and have international cooperation to ensure that transnational social media crimes are policed effectively. Respondents further proposed that Namibia should network with other countries on how they were dealing with cyber criminals, and if she required technical assistance, to have treaties with advanced states in cybersecurity. The result was supported by Choudhury *et al.,* (2013) who held that more centralized coordination at regional and interregional levels could be needed to streamline the fight against cybercrime. Another study by UNODC (2013) also found that due to the volatile nature of electronic evidence, international cooperation in cybercrime matters required timely response and the ability to request specialized investigative actions. Formal cooperation among countries required using bilateral instruments as the legal basis.

Service providers

The results showed that 2 respondents proposed that service providers should be involved in the fight of social media crimes, and provide necessary support to the police and the courts. They added that the Namibian government should have an agreement with the social network companies, that for instance if Facebook was to be allowed in Namibia, certain contents should be proscribed. Such an agreement would ensure control on the usage of social media. Other countries have such agreements, and some do not allow use of Facebook.

Reporting of cybercrime

The findings on reporting of cybercrime showed that 3 respondents proposed that the internet users should be encouraged to report crimes and they should at least wait for the police to act because if there was evidence, the suspect would be arrested. Respondents stated that there should be a monitoring and reporting mechanism to allow pro-activeness.

Some studies support the findings and proposethe way of reporting cybercrime. India has established cybercrime reporting mechanism, a system that involves registering complaints with the local police stations or cybercrime cells (Ernst & Young, 2015). Mashiloane (2014) as cited in Kader and Minnaar (2015) inform that the proposed South African Police Service (SAPS) Cyber Centre would implement a cybercrime reporting mechanism for the enhancement of the public and organisational understanding of the scope, threat, trends and collation of data in order to detect pattern of organised criminality.

Registration of sim cards

The results revealed that 2 respondents suggested that all telecommunication companies such as MTC, Leo and Telecom Namibian should make sure that no sim card could be active if it is not registered verifying the owners Identity Document and proof of residence. This would allow all citizens and residents without registered cell phone numbers to register them and when such sim numbers were used in committing a crime on WhatsApp groups and Facebook the police would be able to trace the suspect and prosecute such social media cases in the court. There was no study found on registration of sim cards.

4.3.3. Summary of chapter 4

This chapter discussed the findings of the study organised according to the Research Questions 1-8 of the study. Section 4.3.1 introduced the chapter and outlined how the chapter was organised, while section 4.3.2 summarised the profiles of the respondents of both phases 1 and 2 during data collection.

Data gathered on the demographic profiles of the respondents showed that the participants were from various categories (Members of the public, Namibian Police Force, Communication Regulatory Authority of Namibia, Ministry of Justice, Ministry of Information Communication and Technology as well as the Law Society of Namibia.)

Section 4.3.3.1 answered research Question 1: The social media implications on human security of persons in Namibia and providing effects towards economic, personal, community, environmental, food, health and political security aspects. The findings revealed that social media have serious implications or threats to human security in all those aspects, but severe threats are notable on economic, personal and health security.

Section 4.3.3.2 responded to research Question 2 about the experience of cybercrime situation in Namibia, specifically those committed on WhatsApp and Facebook. The results showed that cybercrime situation could be becoming worse and uncontrollable. The most common trend was exposing individual's sexual life by sharing private sex videos and pictures on Facebook and WhatsApp as well as sharing of fake news.

Findings reported above in Table 1 and 2 in section 4.3.3.3 showed that the most prevalent social media crimes were distribution and circulation of obscene materials- 94.4%, followed by cyber bullying- 72.2%, defamation of character- 66.6%, hate speech- 61.1.%, cyber stalking and pornography- 55.5%, sexting- 50%, identity theft and internet fraud- 44.4%. The prevalent crimes rated 2 were breach of privacy- 44.4%, and child pornography- 33.3%, while the moderate crimes rated 3 were grooming- 50%, identity theft and phishing- 27.7%. Hacking of personal computers and accounts- 33.3% and drug and human trafficking- 27.7% appeared to be the least prevalent crimes rated 4, while cyber terrorism was rated with 77.7% as the most least prevalent social media crime.

Section 4.3.3.4 responded to research Question 4 about how social media crimes were committed in Namibia on WhatsApp and Facebook platforms. Respondents highlighted that individuals befriended others on Facebook with the intention to defraud. Some people lose money on online shopping; others through traditional healers and witchdoctors who claim to heal various diseases. Some Facebook and WhatsApp users have a habit of defaming others by exposing them on social media by uploading and sharing sex or nude videos and pictures. The results showed a high tendency of distributing and circulating obscene materials and sharing fake news.

Section 4.3.3.5 answered research Question 6 about Namibian's legal position with regards to cybercrime:

Findings showed that Namibia does not have a cybercrime legal framework in place; however there was a draft bill which has to go to parliament.

Section 4.3.3.6 responded to a question about how the Namibian Police Force delt with the reported social media cases in the absence of the cybercrime legal framework. The results showed that the Namibian police could not do much when there was no law. However, the statutory and common laws can be used to deal with cases that were defined there.

Section 4.3.3.7 answered the question about the challenges faced by the Namibian police and courts in dealing with social media crimes that threaten human security. The results revealed that technological power, inadequate funds, lack of capacity for police officers, lawyers and prosecutors, transnational and anonymity nature of cybercrime, extradition problems, lack of awareness and reporting mechanisms were some of the challenges.

Section 4.3.3.8 responded to a question about strategies that could be adopted by Namibian Police, MICT and CRAN to deal with social media crimes. The findings provided strategies such as investing in technological power, building capacity for police and courts, allocating sufficient funds for cybersecurity, raising awareness through public meetings, radio and television. The results suggested international cooperation, joint stakeholders and service provider's cooperation to reduce cybercrime. The next chapter presents a summary of the study, conclusions and recommendations.

CHAPTER 5: SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.1. Introduction

This chapter summarises the findings of the study, offers conclusions and recommendations that may be used to combat social media conducts that threaten human security of internet users in Namibia. The chapter also suggests advice for further research. The study intends to design a strategy for social media implications on human security in Namibia. Below were the research questions that guided the study and in each section important findings and comments are outlined. The research questions were:

Research Question 1: What are the human security implications of social media crimes in Namibia?

Research Question 2: In the absence of a supportive legislative, what are
the challenges for the Namibian Police in dealing with social media crimes
that are threatening human security?

Research Question 3: What strategy should NAMPOL adopt to deal with cyber social media crimes?

What follows is a summary of the findings of the study, conclusions and recommendations.

5.2 Summary of the Research Findings in Chapter 4 Based on the Research Questions

This section would be organised according to the research interview and questionnaire questions used in the study.

5.2.1 Social media implications on human security

The results presented in chapter 4, section 4.3.3.1 answered research Question 1: The social media implications on human security of persons in Namibia and providing effects towards economic, personal, community, environmental, food, health and political security aspects. The findings revealed that social media has serious implications or threats to human security in all those aspects, but severe threats are notable on economic, personal and health security. The notable economic threats took the form of theft by false pretence, identity theft, fraud, embezzlement, hacking of personal accounts and demand money from befriended users, online shopping, replacing and repairing of stolen and damaged properties and financial scams, while personal implications were human rights violations, violation of privacy, defamation of character, cyber stalking, physical attacks, hate speeches and using others identities to commit crimes. Community security was threatened through shared fake news, lack of humanity and sharing of obscene and pornographic materials, eroding cultures and traditions, tribalism posts and organised crimes.

Environmental security could be affected in many ways such as damage to the environment and biodiversity, deforestation, poaching and illegal hunting, sand mining and illegal and illicit trading of natural, mineral and marine resources such as timber, diamonds and fish. Meanwhile health security is compromised (by the replacement of true medication with herbs and spiritual oils and water from witch doctors and religious pastors, getting sexually involved with pastors and traditional healers in expectation of getting healed, selling of medical untested products such as pills for losing weight, high blood pressure and other diseases. Food security might be threatened when individuals spread rumors about food, poisoning or share videos misinterpreting how certain foods were processed and declaring some food products not good for human consumption. Lastly, political security could be at stake through sedition, overthrowing of government, terrorist recruitment through Facebook, and political instability due to different political parties opinions and interests.

5.2.2. Cybercrime situation in Namibia

Section 4.3.3.2 responded to research Question 2 about the experience of cybercrime situation in Namibia, specifically those committed on WhatsApp and Facebook. All respondents agreed that the cybercrime situation in Namibia was becoming worse and uncontrollable. The most common trend was exposing individuals’ sexual lives by sharing private sex videos and pictures on Facebook and WhatsApp, hate speech and defaming others and sharing of fake news. This is happening because Namibian people do not understand the danger of social media, and some do not know if their rights were being violated on Facebook and WhatsApp.

5.2.3. Prevalence of social media crimes in Namibia

Findings reported above in Tables 1 and 2 in section 4.3.3.3 showed that the most prevalent social media crimes were the distribution and circulation of obscene materials 94.4%, followed by cyber bullying 72.2%, defamation of character 66.6%, hate speech 61.1.%, cyber stalking and pornography 55.5%, sexting 50%, identity theft and internet fraud 44.4%. The prevalent crimes rated 2 were breach of privacy 44.4%, and child pornography 33.3%. While the moderate crimes rated 3 were grooming 50%, identity theft and phishing 27.7%. Hacking of personal computers and accounts 33.3% and drug and human trafficking 27.7% appear to be the least prevalent crimes rated 4, while cyber terrorism happen to be the most least prevalent social media crime.

5.2.4. Commission of social media crimes in Namibia

Results presented in chapter 4, section 4.3.3.4 responded to research Question 4 about how social media crimes were committed in Namibia on WhatsApp and Facebook platforms. Respondents highlighted that individuals befriended others on Facebook with intention to defraud them. As a result, some people lost money on online shopping; others through traditional healers and witchdoctors who claim to heal various diseases. Some Facebook and WhatsApp users have a habit of defaming others by exposing them on social media by uploading and sharing sex or nude video and pictures. The results show a high tendency of distributing and circulating obscene materials and sharing fake news.

5.2.5. Cyber legal framework in Namibia

The findings in chapter 4, section 4.3.3.5 answered research Question 6 about Namibia's legal position with regard to cybercrime. Findings showed that Namibia does not have any cybercrime legal framework in place. However, there was a draft bill which has to go to parliament.

5.2.6. Policing cybercrime in the absence of cybercrime law

Section 4.3.3.6 responded to a question about how the Namibian Police Force deal with the reported social media cases in the absence of the cybercrime legal framework. All respondents stated that there was a challenge for the Police when there was no law, as there could be no crime when there was no law in place. Respondents further explained that when a crime committed falls under statutory or common law such as defamation of character, then the police can use the statutory and common laws to deal with cases.

5.2.7. Challenges faced by the police in dealing with cybercrime

Section 4.3.3.7 answered the question about the challenges faced by the Namibian police and courts in dealing with social media crimes that threatened human security. The results revealed that technological power, inadequate funds, lack of capacity for police officers, lawyers and prosecutors, transnational and anonymity nature of cybercrime, extradition problems, lack of awareness and reporting mechanisms are some of the challenges.

5.2.8. Strategies to deal with cybercrime

Section 4.3.3.8 responded to a question about strategies that could be adopted by Namibian Police, MICT and CRAN to deal with social media crimes. The findings provided strategies such as investing in technological power, building capacity for police and courts, allocating sufficient funds for cyber security, raising awareness through public awareness campaigns on radio and televisions. The results suggested international cooperation, joint stakeholders and service providers' cooperation to reduce cybercrime.

5.3 Conclusions

Based on the summary, it may be concluded that the study successfully answered the research questions. The three research questions were further divided into eight research and interview questions and the findings were discussed in line with those questions. The first question proved that social media negatively impacted upon human security. The most common affected dimensions of human security were economic through hacking of accounts, identity theft, theft under false pretence through online shopping, buy and sell and embezzlement. Personal security was threatened when individuals posted defamatory contents and statements about others on Facebook and WhatsApp, breach of privacy, physical attacks when individuals shared their location on social media. Similarly, health security was also at stake since many people sold medical products on Facebook and some of the patients who were on different treatment quit them and took the untested medical pills to relieve their pain. Equally, witch doctors and church pastors took advantage of patients, hence they advertised on Facebook that they cured certain diseases such as HIV/AIDS and cancer and when approached by patients they told them they were afflicted by demons they should take anointed oil and water or herbs to cure them.

Facebook and WhatsApp accelerated the commission of crimes and it allowed organised crimes such as drug and human trafficking, robbery and kidnapping, thereby affecting community security. The environment was also facing serious threats of wildlife poaching, cutting down of trees for timber and mining sand for constructions and bricks businesses. In other cases, some individuals discourage others from consuming certain food products by spreading rumors on poisoning, and sharing disgusting videos of food processing.

According to the results, the researcher concludes that the situation was getting worse, time to time users of Facebook accounts are hacked, some people lost their money through false pretence and others were bullied online. It is evident that the most devastating trend is circulation and distribution of obscene materials, sharing of fake news, breaching of privacy and exposing others' private conversations, nude pictures and sex videos. In addition, the result showed that distribution and circulation of obscene materials was rated as the most committed social media crime 94.4%, followed by cyber bulling 72.2% and then defamation of character 66.6 percent. Grooming happened to be a moderate crime rated 3 with 50%, while cyber terrorism was rated high with 77.7 as the most little prevalent social media crime in Namibia. This trend was supported by findings presented in chapter 2 and 4; Dwivedi (2018), Kamp (2016), Kobek (2017), Williams and Pearson (2016), Wong (2005) as well as UN (2013).

The researcher further concluded that the crimes committed on Facebook and WhatsApp platforms were also the same as some of those offline crimes, such as fraud, hate speech, defamation of character, bullying and theft under false pretence. However, other crimes like cyber stalking, internet fraud, hacking, and pornography require usage of internet and smartphone which the majority of Namibians have and most of them have access to. Just as revealed by a previous study by Links (2018) and the results of this study, conclusion could also be reached that Namibia does not have any legal framework for cybercrime and it was necessary for the government to speed up the passing and enacting of the law. The absence of the cybercrime framework hinders the duties of the police, because the police cannot arrest or detain any person who commits a cybercrime without a law that define such an act as a crime, unless the said crime was defined under common law or statutory laws.

In the final analysis, the police and courts have been faced with numerous challenges ranging from technology, capacity to investigate and prosecute, lack of a law, lack of awareness among citizens, transnational and jurisdictional nature of cybercrime, anonymity nature, extradition challenge, lack of financial resources and service provider’s cooperation in combating cybercrimes. The conclusion was also made that the cyber security stakeholders should ensure that the cybercrime bill was passed; ensure public education to raise awareness on the danger of social media. Moreover, the government should invest in technological equipment and capacity building to ensure that police investigators and prosecutors acquire necessary skills to deal with cybercrime cases. Lastly, the government should sign international treaties on cybercrime and ensure that cooperation was achieved with other countries, service providers and other relevant stakeholders. The literature identified and supported the findings on the challenges and strategies to be employed to deal with cybercrime included Ajayi, (2016), Doshora, (2011), Kader & Minnaar (2015), Kubic (2001) as cited in Kader & Minnaar (2015), Wall (2011), UN (2013) and UNODC (2013)). The next section presents the recommendations.

5.4 Recommendations

The following were the general recommendations that could be considered by the Namibian Police, MICT, CRAN, Justice and Legislature in order to combat social media crimes that threaten human security in Namibia.

5.4.1 General Recommendations

In view of the prevalent social media implications on human security in Namibia, particularly economic, personal, community and health threats, the study recommends that online safety or social media education was needed for all internet users. Therefore the Ministry of Information Communication and Technology, Communication Regulatory Authority and the Namibia Police Force should lead the cybersecurity education in the country to prevent economic losses, and protect internet users from human rights violations on personal and all human security threats. The study found that the absence of a cyber legal framework allows and increases human security threats caused by social media usage ranging from fraud, hacking, identity theft, breach to privacy and defamation of character, hate speech, cyber bullying and circulation of obscene materials. Therefore, this study justified the need to pass and enact the cyber legal framework which could criminalise acts and impose punishment for cybercrimes in Namibia.

Specific recommendations were as follows:

(a) The results of the study revealed that Namibia does not have a cyber legal framework in place except for a draft bill. Findings of a previous study by Kalunde (n. d) strongly believe that cyber-criminals around the world are constantly seeking loopholes through which to perform illegal or illicit businesses. Any country that has inadequate cyber-law is essentially offering a safe- haven for cyber-criminals to act with impunity. It was against these findings that the researcher recommends a speedy implementation and enactment of draft cybercrime bill into a law, which could prevent human security threats posed by social media usage in Namibia and which would also define cybercrimes and their elements, and provides punishment for such offences. The law would guide law enforcement agencies on how to deal with social media crimes.

(b) The study recommends social media education through print and visual media and public meetings. This initiative would raise awareness among social media users by informing them of their rights, safety tips, and cybercrimes and encourage them to report social media crimes to the police. The literature shows that many residents with access to internet use social media to hurt each other posting hate speeches, defame others, violate their rights by hacking their accounts, and defraud them through theft under false pretence.

Literature shows that one global private sector survey suggests that 80 per cent of individual victims of core cybercrime do not report the crime to the police. Underreporting derives from a lack of awareness of victimization and of reporting mechanisms, victim shame and embarrassment, and perceived reputation risks for corporations (UNODC, 2013). The researcher suggests that awareness campaign on social media implications on human security should be prioritised in Namibia.

(c) The study recommends that capacity building for investigators and prosecutors should be given most attention to ensure that they get relevant skills to detect, investigate, gather evidence and present it and be able to prosecute the offenders.

This step would allow justice to prevail as the police and courts would have expertise to perform their duties and finalise cybercrime cases. The literature shows that a comprehensive model of cybercrime investigations was important for standardising terminology, defining requirements, and supporting the development of new techniques and tools for investigators (Kader and Minnaar, 2015).

(d) The study further recommended that the government should invest in technology to be able to monitor, detect and prevent serious security threats. While investing in technology, it was also imperative to benchmark from advanced countries in terms of cyber security in order to gain more knowledge and expertise in the field of cyber security.

(e) The study recommends that the Namibian government should have agreements with service providers such as Facebook and WhatsApp which prohibit sharing and posting of prohibited contents such as pornographic and obscene materials. The Namibian Police should be able to filter whatever was being posted on social media by Namibians as this will promote ethics and morality among citizens.

(f) Lastly, the researcher recommends the registration of all sim card numbers for Telecom, Leo and MTC. All cell phone numbers should be registered before they could be activated to be used for communication. This would make it easier for the police to trace social media criminals by getting proof of a number involved in a crime from telecommunication companies. Moreover, all residents with existing unregistered cell phone numbers should be given a period to register and after such period all unregistered numbers should be deactivated.

The researcher has confidence that the above recommendations would result in the implementation of an effective strategy for the social media implications on human security in Namibia, aimed at combating cybercrimes and reducing the impacts thereof.

5.4.2 Originality of the Study

This was the first study to inquire on the social media implications on human security of internet users in Namibia at a master degree level. The study identified the social media implications on human security (economic, personal, community, food, health, political and environmental)and the challenges faced by the Namibian police in dealing with social media crimes as well as the strategies to combat such crimes.

5.4.3 Contributions of this Study

This study was the first to investigate how social media threatens human security in Namibia, therefore it could serve as a future reference point to academics interested in research in the area of cyber security and other security studies. Previous studies on social media are done by media studies and Language studies focusing on the usage of languages, whereas this study educates the social media users of their rights while interacting with others as well as the impact of social media crimes. This study therefore creates security awareness to all social media users in Namibia. Lastly, this study may contribute to the speedy implementation cybercrime law in the country given the implications on human security.

REFERENCES

Adesina, O. S. (2017). Cybercrime and Poverty in Nigeria. Vol. 13, No. 4, pp. 19-29

Adeyemi-Suenu, A. (2014). Human security in Africa: issues and problems. International Letters of Social and Humanistic Sciences. (Online). Vol. 24, 89-93. Retrieved from www.scipress.com/ILSHS.24.89.doi:10.18052/

Ajayi., E.F.G. (2016). Challenges to enforcement of cyber-crimes laws and policy. Journal of Internet and Information Systems. Retrieved http://www.academicjournals.org/JIIS. DOI 10.5897/JIIS2015.0089.

Amedie, J. (2015) .The Impact of Social Media on Society. *Advanced Writing: Pop Culture Intersections*. Retrieved from http://scholarcommons.scu.edu/engl_176/2

Barfi, K.A., Ngagorme, P. &Yeboah, N. (2018). The Internet Users and Cybercriem in Ghana: *Evidence from Senior High School in BrongAhafo.* (E-journal) Library Philosophy and Practice.

Barman, N. (2015).Legal Implications of Cyber Crimes on Social Networking Websites.International Journal of Scientific and Research Publications, Volume 5, Issue 12.

Bennett. J. T. (2016). The Harm in Hate Speech: A Critique of the Empirical and Legal Bases of Hate Speech Regulation. Hastings Constitutional Law Quarterly.Vol. 43.3. pp. 445-465.

Bhatia, M. S. &Srivastava, S. (2010). Cyber Laws. Delhi Psychiatry Journal Vol. 13 No.1

Bowen, G.A. (2008). Qualitative research. Naturalistic inquiry and the saturation concept: a research note. London: SAGR publication. DOI: 10.1177/1468794107085301

Brenner, S.W. (2001). State Cybercrime Legislation in the United States of America: *A Survey, Journal of Law and Technology*. Volume 7, Issue 3http://scholarship.richmond.edu/jolt/vol7/iss3/4.

Brown.C.S.D. (2015).Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice. International Journal of Cyber Criminology Vol 9 Issue 1.

Cassim, F. (2009).Formulating specialized legislation to address the growing spectre of cybercrime: a comparative study. ISSN 1727-3781 vol.12, No.4: PER.

Cassim. F. (2011). Addressing the growing spectre of cyber-crime in Africa:

evaluating measures adopted by South Africa and other regional role players.

CGI (2014). Tomorrow's Force: *How technology can help the police evolve to support a changing society.* CGI GROUP INC

Chander, M. (2014). Social Media: *Analysis of New Challenges and Opportunities for Indian Law Enforcement Agencies.* Article in Police Journal.

Council of Europe (2015). The state of cybercrime legislation in Africa. An overview

Creswell, J.W. (2013). Qualitative inquiry and research design. *Choosing Among Five Approaches (3rd ed.).*United Kingdom: Sage Publications.

Creswell, J.W. (2014). Research Design. *Qualitative, Quantitative and Mixed Methods Approaches (4th ed.).* United Kingdom: Sage Publications.

Cybercrimes and Cybersecurity Bill. B.6 (2017). Retrieved from www.justice.gov.za/legislation/bills/CyberCrimesBill2017.pdf

Das, S. & Nayak, T. (2013). Impact of Cybercrime: Issues and Challenges. International Journal of Engineering Sciences & Emerging Technologies. Volume 6, Issue 2, pp: 142-153. IJESET

Donegan, R. (2012). Bullying and Cyber bullying: History, Statistics, Law, Prevention and Analysis. The Elon Journal of Undergraduate Research in Communications. Vol. 3, No. 1

Doshora, K. (2011). Cyber Crime in the Society: *Problems and Preventions. Journal of Alternative Perspectives in the Social* Sciences Vol 3, No 1, pp. 240-259.

Dwivedi, D. (2018). Social media and social networking: A challenge to human security. International Journal of Academic Research and Development. Volume 3; Issue 1; pp. 803-806.

EA (2018). Social Media Policy. Retrieved from http://www.equestrian.org.au/

Edappagath, M.A. (2001) Cyber laws in Information Age. Asia-Pacific Regional Workshop on Equal Access of Women in ICT Seoul, R.O. Korea.

Ernst & Young (2015). Strategic National measures to combat cybercrime: perspective and learning for India.

Esther Snell, E. (2015). Policing Cybercrime. MSc.Royal Holloway

Etikan, I., Musa, S.A., & Alkassim, R.S. (2016). Comparison of Convenience Sampling and Purposive Sampling. American Journal of Theoretical and Applied Statistics. Vol. 5, No. 1, 2016, pp 1-

4. Doi:10.11648/j.ajtas.20160501.11

Finnan, D. (2015) Lack of laws governing cybercrime making Africa a safe haven for cybercriminals: Interview

Gharibi, W. &Shaabi, M. (2012).Cyber Threats in Social Networking Websites. International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.1, DOI: 10.5121/ijdps.2012.3109

Gitonga.W. (2014). The prevalence of internet crimes on women students at the university of Nairobi. Degree of Master of Arts in Gender and Development Studies of the University of Nairobi. Nairobi

Goodman, M.D. & Brenner, S.W. (2001).The Emerging Consensus on Criminal Conduct in Cyberspace.

Harding, J. (2013). Qualitative Data Analysis from start to finish. London: Sage Publication

Hof. S. &Koops.B. (2011). Adolescents and Cybercrime: Navigating between Freedom and Control. Retrieved http://www.psocommons.org/policyandinternet/vol3/iss2/art4.DOI:10.22 0 2/1944-2866.1121

Irshad1, S. & Tariq Rahim Soomro, T.R. (2018).Identity Theft and Social Media.*International Journal of Computer Science and Network Security,* Vol.18 No.1.

ITU (2012). Understanding cybercrime, phenomena, challenges and legal response. Telecommunication Development Sector.

Kader, S., & Minnaar, A. (2015). Cybercrime Investigation: Cyber-processes for detecting of cybercriminal activities, cyber-Intelligence and evidence gathering. Southern African Journal of Criminology. NO. 5/2015.

Kalunde, S.M. The status of Cybercrime in Tanzania Strasbourg, France.Presented at the Octopus Conference on Cooperation Against Cybercrime & 10th Anniversary of the Budapest Convention.

Kamp. M. (2016).Reality Check.Assessing the Impact of Social Media on Political Communication and Civic Engagement in Uganda. Konrad Adenauer Stiftung.

Keane, E (2016).The challenge to policing in investigating cybercrime. Scottish Justice Matter

Kobek, L.P. (2017). The State of Cyber security in Mexico: An Overview. Wilson Centre.

Kovacs, A. &Hawtin, D. (2013). Cyber security, Cyber surveillance and online human rights.

Krubhala, P, Niranjana, P. & Priya, G.S. (2015). Online Social Network - A Threat to Privacy and Security of Human Society. International Journal of Scientific and Research Publications, Volume 5, Issue 4, Retrieved from: www.ijsrp.org

Kumar, R. (2011). Research Methodology. *A step-by-step guide for beginners (3rd ed.*). India: Sage publications

Leedy, P.D., & Ormrod, J.E. (2010). Practical Research: *planning and Design* (9t hed.). New Jersey: Pearson.

Links.F. (2018).Tacklig Cyber Security/ Crime in Namibia.*Calling for a Human Rights Respecting Framework.* Special Briefing Report No.20.

Lunker, M. Cyber Laws: A Global Perspective.

McGuire, M. & Dowling, S. (2013). Cyber-crime: A review of the evidence Chapter 2: Cyber -enabled Crimes- fraud and theft. Research Report 75: Home Office

Mendoza, D.K.O. (2017). The Vulnerability of Cyberspace - The Cyber Crime.Journal of Forensic Science and Criminal Investigation.Volume 2 Issue 1. Mexico Juniper Publishers

Mengu, M. &Mengu, S. (2015). Violence and Social Media.Athens Journal of

Mass Media and Communications, Vol. 1, No. 3

Ministry of Information and Communication Technology (2015). Caution against circulation of violent videos on social media. Windhoek. MICT Press Statement.

Minnaar, A. (2014). Crackers, Cyberattacking and Cybersecurity vulnerability. *The difficulties in combating the new cybercriminals.* South African Journal of Criminology. N02/2014

Minnaar, A. (2016) Organised crime and the 'new more sophisticated' criminals within the cybercrime environment: how 'organised' are they in the traditional sense? South African Journal of Criminology. 29 (2) 2016.

Morgan, S. (2017). Cybercrime Damages will cost the world $ 6 trillion annually by 2021. Cybercrime Report.Herjavec Group.

Namibian Police Force (2016). Annual Report

Namibian Police Force (2017). Creation, Distribution and Circulation of obscene, indecent and pornographic materials. Windhoek: NAMPOL Press Release.

National White Collar Crime Centre (2011).*Criminal use of social media*. U.S.A: Fairmont

Nbc News. (2017, January 26). Nampol warns against distribution of obscene material. Namibia: Namibia Broadcasting Corporation. Retrieved from https://www.nbc.na/news/nampol-warns-against-distributing-obscene-material.2318

Nfuka.E.N., Sanga, C. & Mshangi, M. The Rapid Growth of Cybercrimes Affecting Information Systems in the Global: *Is this a Myth or Reality in Tanzania?* International Journal of Information Security Science Vol. 3, No. 2

Nsude, I. & Onwe, E.C. (2017).Social Media and Security Challenges in Nigeria:

The Way Forward. *World Applied Sciences Journal.* IDOSI Publications (6): 993-999, DOI: 10.5829/idosi.wasj.2017.993.999

Nueman, W.L. (2000). Social Research Methods. *Qualitative and quantitative Approaches* (4th ed.). United States of America: Allyn & Bacon.

Ossip.S.M (2017).Cyber threats and cybercrime, a disruption of human security?MA in International Relations. Leiden University

Perry, M.B. (2015). Emotional and Social Effects of Cyber bullying on Adolescents.Master of Education.Gordon Albright School of Education.

Plooy-Cilliers, F., Davis, C. & Bezuidenhout, R. (2014). Research Matters. Cape Town: Juta & Company Ltd.

Prasanthi, L.P. &Ishwarya, T.A.S. (2015). Cyber Crime: Prevention & Detection. *International Journal of Advanced Research in Computer and Communication Engineering*.IJARCCE Vol. 4, Issue 3, pp.45-48

Republic of Philippines (2017). Cybercrime Prevention Act of 2012. (2017):15t h Congress of the Philippines.

Republic of South Africa (2017).*Cybercrimes and Cybersecurity Bill*.B6-2017.

Ritchie, J., Lewis, J., Nicholls, C. M. & Ormston, R. (2014).Qualitative Research Practice (2nd ed.). *A guide for social science students & Researchers*. London: SAGE Publication Inc.

Seger, A. (2012). *Cybercrime strategies. Discussion paper*. Strasbourg: Council of Europe

Sekaran, U. (2003). Research Methods for Business. *A Skill Building Approach (*4t h ed.). United States of America: John Wiley & Sons, Inc.

Shank, G. D. (2006). Qualitative Research. *A Personal Skills Approach* (2nd ed.). New Jersey: Pearson Prentice Hall.

Șinca. G.M. &Mascas, I.V. (2015). Human security in social media - just a click away.*AGORA International Journal of Administration Sciences*, Retrieved from: http://univagora.ro/jour/index.php/aijas . No. 1), pp. 1-11.

Singh, J. (2014). Human Security: A Theoretical Analysis. International Journal of Political Science and Development. Vol. 2(8), pp. 175-179. Retrieved from http://www.academicresearchjournals.org/IJPSD/Index.html, DOI: 10.14662/IJPSD2014.041

Snell, E. (2015). Policing Cybercrime. Master of Science: Royal Holloway

The Constitution of the Republic of Namibia 1990

Turck, L. (2016). An Investigation into the Utilisation of Social Media by the Saps in Resolving Crime.MA Thesis in Policing. University of South Africa.

UNDP. (1994). Human Development Report. New York: Oxford University Press.

UNESCO (2008). Human Security Approaches and Challenges. France: Published by the United Nations Educational, Scientific and Cultural Organization

United Nations (2009). Human Security in theory and practice. An overview of Human Security concept and the United Nations Trust Fund for Human Security. Retrieved from www.un.org/humansecurity

United Nations. Effective measures to prevent and control computer-related crime. Report of the Secretary-General.

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

UNTFHS (1999) Human Security in Theory and Practice: *An Overview of the Human Security Concept and the United Nations Trust Fund for Human Security.* United Nations

Wall, D.S. (2015). The changing cyber-threat landscape and the challenge of policing cybercrimes in the EU. Journal for Centre of criminal justice studies. United Kingdom: University of Leeds.

Wall, D. S. (2011). Policing cybercrimes*: Situating the PublicPolice in Networks of Security within Cyberspace. Police Practice & Research: An International Journal, 8(2):183 205*. Retrieved from: http://ssrn.com/abstract=853225

Warner, J. (2011). Understanding Cyber-Crime in Ghana: A View from Below. International Journal of Cyber Criminology (IJCC).Vol 5 (1): pp. 736–749. Harvard University. United State of America.

Welman, Kauger, Mitchell (2005). Research Methodology (3rd ed.). Cape Town: Oxford.

Williams, M. & Pearson, O. (2016). Hate Crime and Bullying in the Age of Social Media. Conference Report. Crown.

Wong, K. C. (2005). Computer Crime and Control in Hong Kong. Pacific Rim Law & Policy Journal Association. Vol 14.No. 2.pp 337-382.

World population review (2018). Population of cities in Namibia (2018). Retrieved from http://worldpopulationreview.com/countries/namibia-population/cities/

Yar, M. (2013). Cybercrime and society, 2nd ed. Los Angeles: Sage.

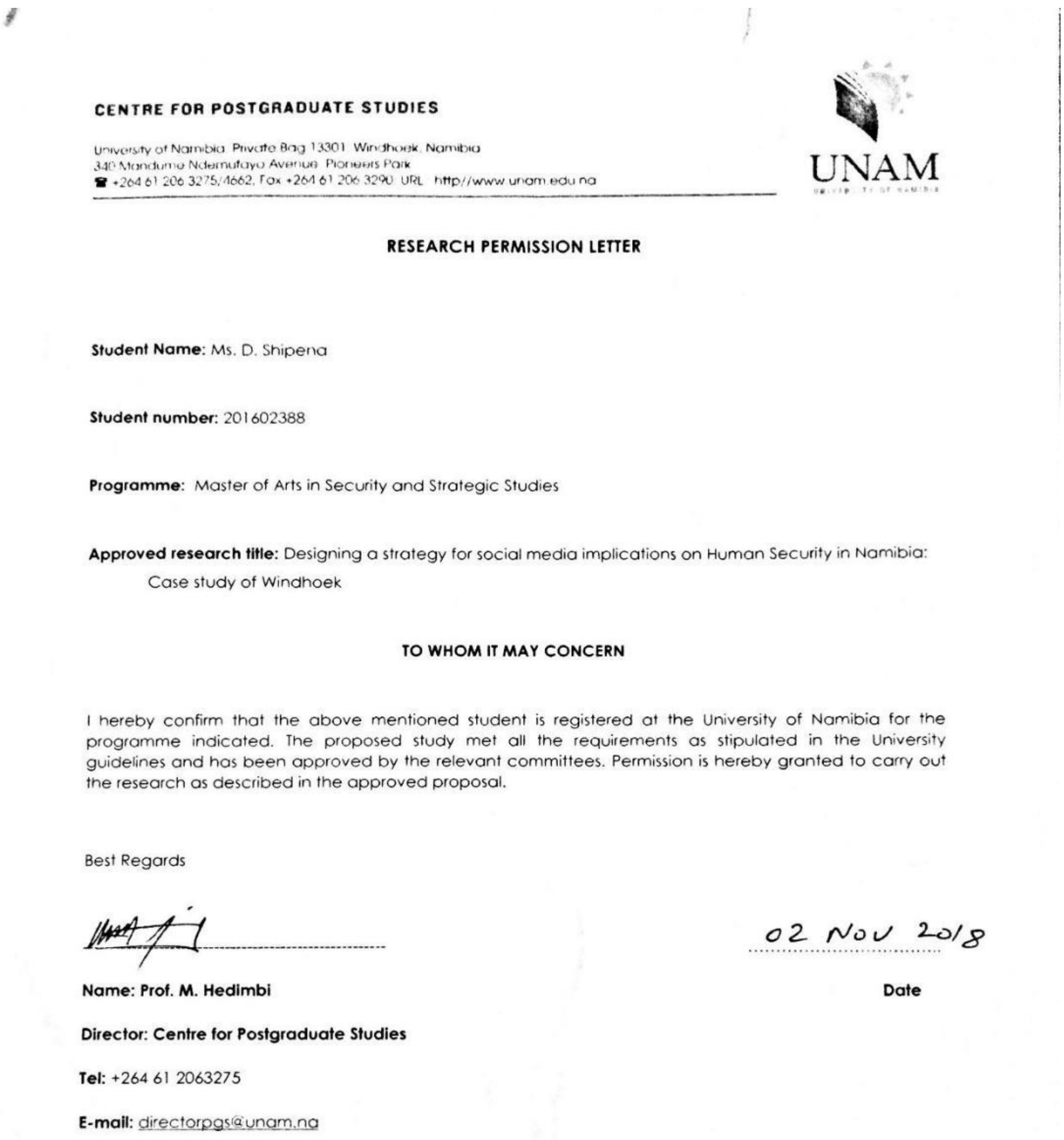
Yin, R. K. (2016). Qualitative Research from Start to Finish (2nd ed.). New York: The Guilford Press.

Yin, R.K. (2003). Case Study Research Design and Methods (2nd ed.). Applied Social Science Research methods. London: SAGE Inc.

Yong. P. Comparative Research on “Convention on Cybercrime” and Chinese Relevant Legislation.

APPENDICES

APPENDICE A: ETHICAL CLEARANCE



CENTRE FOR POSTGRADUATE STUDIES

University of Namibia, Private Bag 13301, Windhoek, Namibia
340 Mandume Ndemufayo Avenue, Pioneers Park
☎ +264 61 206 3275/4662, Fax +264 61 206 3290, URL: http//www.unam.edu.na

UNAM
UNIVERSITY OF NAMIBIA

RESEARCH PERMISSION LETTER

Student Name: Ms. D. Shipena

Student number: 201602388

Programme: Master of Arts in Security and Strategic Studies

Approved research title: Designing a strategy for social media implications on Human Security in Namibia: Case study of Windhoek

TO WHOM IT MAY CONCERN

I hereby confirm that the above mentioned student is registered at the University of Namibia for the programme indicated. The proposed study met all the requirements as stipulated in the University guidelines and has been approved by the relevant committees. Permission is hereby granted to carry out the research as described in the approved proposal.

Best Regards

02 NOV 2018

Name: Prof. M. Hedimbi **Date**

Director: Centre for Postgraduate Studies

Tel: +264 61 2063275

E-mail: directorpgs@unam.na

APPENDICES B: QUESTIONNAIRE AND INTERVIEW QUESTIONS

Informed consent for participation in an academic

Research study

University of Namibia

TOWARDS DESIGNING A STRATEGY FOR SOCIAL MEDIA IMPLICATIONS ON HUMAN SECURITY IN NAMIBIA: CASE STUDY OF WINDHOEK

Research conducted by:

Miss D. Shipena

(201602388)

Dear Respondent

This study is conducted in partial fulfilment of the Master of Arts in Security and Strategic Studies at the University of Namibia. You are therefore invited to participate in an academic research study conducted by Dortea Shipena. The purpose of the study is to design a strategy for social media implications on Human Security in Namibia: Case study of Windhoek.

Please note the following:

- This study is an <u>anonymous</u> survey. Your name will not appear on the questionnaire and the answers you give will be treated as strictly <u>confidential</u>. Care will be taken to ensure that you cannot be identified in person based on the answers you give.
- Your participation in this study is very important to us. You may, however, choose not to participate and you may also stop participating at any time without any negative consequences.
- Please answer the questions in the interview as completely and honestly as possible. This should not take more than 20 minutes of your time.

- The results of the study will be used for academic purposes only and may be published in an academic journal reference. We will provide you with a summary of our findings on request.

- Ethical clearance for this study has been obtained from the University of Namibia.

- Please contact my supervisor, Dr. Mude Torque at +263 77 9960299 or email him at mudetorque@gmail.com Dr. Fungai Bhunu. Shava at 061 207 2510 or email her at fbshava@nust.na if you have any questions or comments regarding the study.

We thank you for your valuable time.

Please complete all sections and questions.

SECTION A:

BIOGRAPHICAL INFORMATION

In this section, please indicate the most appropriate

Gender	Male	Female					
Age	20-29	30-39	40-49	50-59	60-65	Older than 65	
Category	Member of the public	NAMPOL	CRAN	MOJ	MICT	Legislature re	Law Society of Namibia

SECTION B: QUESTIONNAIRE GUIDE

Please answer all questions accordingly.

1. In your opinion what are the social media implications or threats to human security of persons in Namibia? For each applicable, please provide a brief description of effect.

Security threats	***Explain the effect/implications in short***
Economic/Financial	…………………………………………………………… …………………………………………………………… ………………………………………………………
Personal/Physical	…………………………………………………………… …………………………………………………………… …………………………………………………
Community security	…………………………………………………………… …………………………………………………………… ……………………………………………
Environmental security	…………………………………………………………… …………………………………………………………… ………………………………………………………
Food Security	…………………………………………………………… …………………………………………………………… ………………………………………
Health Security	…………………………………………………………… ……………………………………………………………
Political Security	…………………………………………………………… ……………………………………………………………
Any other (please name/explain)	……………………………………………………………

2. Briefly **share** your experience of the cybercrime (social media crimes) situation in Namibia specifically those committed on WhatsApp and Facebook.

…………………………………………………………………………………

…………………………………………………………………………………

3. To what extend are these social media crimes are committed on WhatsApp and Facebook in Namibia on a scale of 1 to 5? **Please rate all crimes 1 – being most prevalent to 5 being the least. Indicate** your rating with a number next to the crime.

Distribution/circulation of obscene materials		Grooming		Cyber bulling		defamation	
Child pornography		Cyber stalking		Pornography		Identity theft	
Hacking of PC		Sexting		Drug /Human trafficking		Hate speech	
Internet Fraud		phishing		Cyber terrorism		Breach of privacy	

4. In your opinion, how are above mentioned social media crimes committed on Facebook and WhatsApp platforms?

…………………………………………………………………………………

…………………………………………………………………………

5. Briefly share on Namibia’s legal position with regard to cybercrime?

…………………………………………………………………………

…………………………………………………………………………

6. How does the Namibian Police deal with reported social media crimes in the absence of the Cybercrime legal framework?

…………………………………………………………………………

…………………………………………………………………………

7. May you please name some of the challenges faced by the Namibian Police Force and the courts in dealing with social media crimes which threaten human security?

…………………………………………………………………………

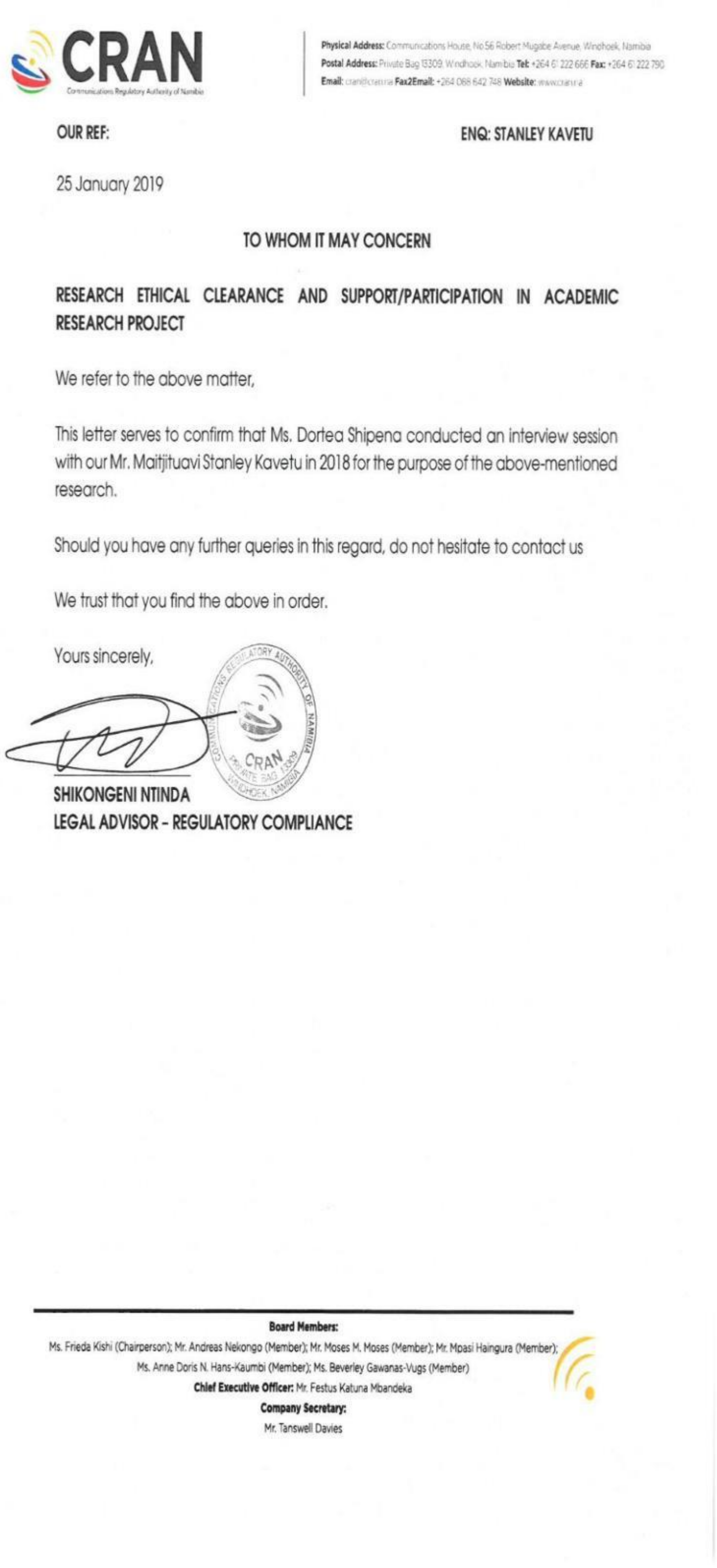
…………………………………………………………………………

8. Please propose some strategies that should be adopted by the Namibian Police Force, MICT and CRAN to deal with social media crimes?

....

....

APPENDICE C: CONSENT LETTER CRAN



CRAN
Communications Regulatory Authority of Namibia

Physical Address: Communications House, No 56 Robert Mugabe Avenue, Windhoek, Namibia
Postal Address: Private Bag 13309, Windhoek, Namibia **Tel:** +264 61 222 666 **Fax:** +264 61 222 790
Email: cran@cran.na **Fax2Email:** +264 088 642 748 **Website:** www.cran.na

OUR REF: **ENQ: STANLEY KAVETU**

25 January 2019

TO WHOM IT MAY CONCERN

RESEARCH ETHICAL CLEARANCE AND SUPPORT/PARTICIPATION IN ACADEMIC RESEARCH PROJECT

We refer to the above matter,

This letter serves to confirm that Ms. Dortea Shipena conducted an interview session with our Mr. Maitjituavi Stanley Kavetu in 2018 for the purpose of the above-mentioned research.

Should you have any further queries in this regard, do not hesitate to contact us

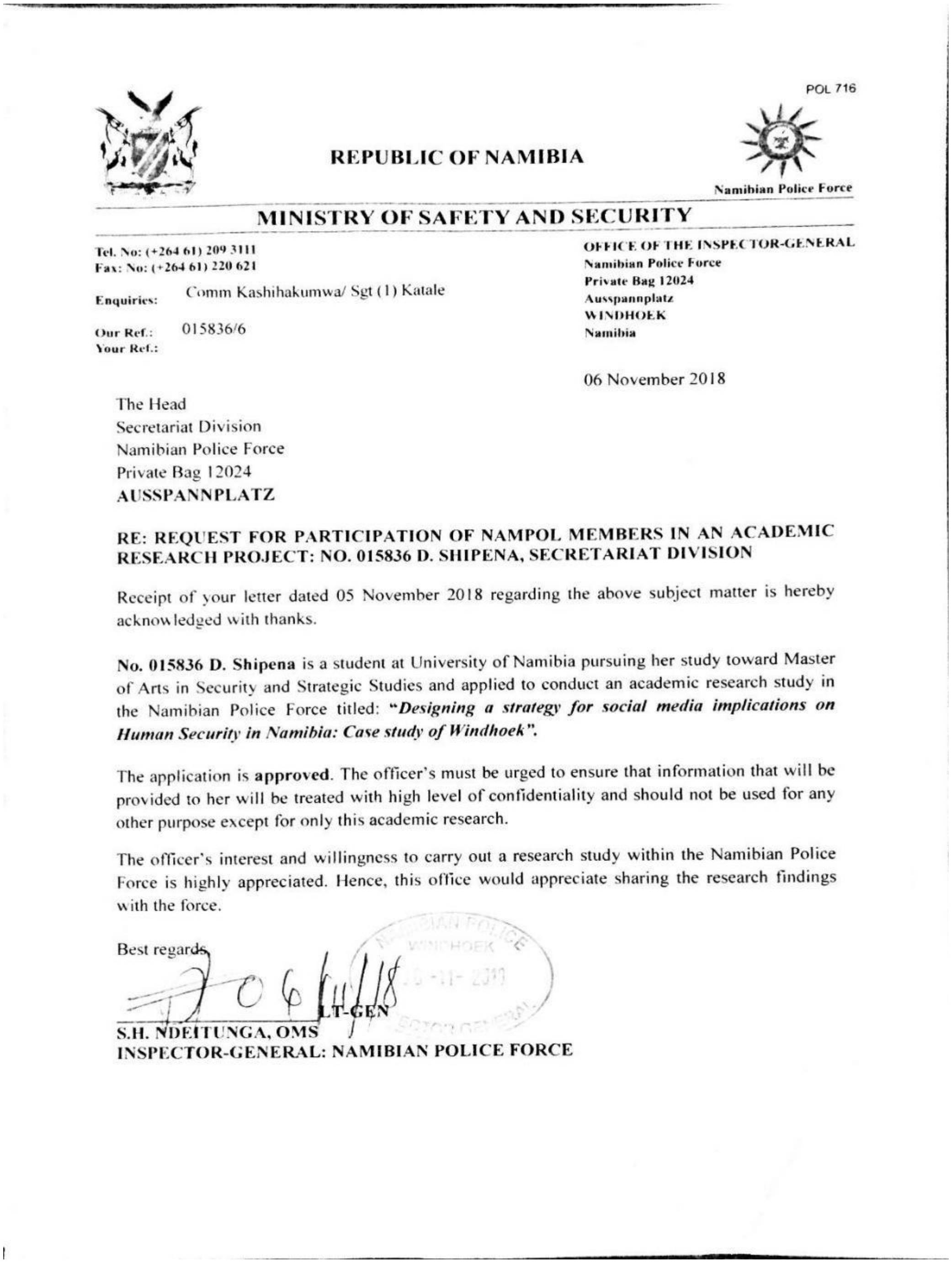
We trust that you find the above in order.

Yours sincerely,

COMMUNICATIONS REGULATORY AUTHORITY OF NAMIBIA
CRAN
PRIVATE BAG 13309
WINDHOEK, NAMIBIA

SHIKONGENI NTINDA
LEGAL ADVISOR – REGULATORY COMPLIANCE

APPENDICES D: CONSENT LETTER FROM NAMPOL



POL 716

REPUBLIC OF NAMIBIA

Namibian Police Force

MINISTRY OF SAFETY AND SECURITY

Tel. No: (+264 61) 209 3111
Fax: No: (+264 61) 220 621

Enquiries: Comm Kashihakumwa/ Sgt (1) Katale

Our Ref.: 015836/6
Your Ref.:

OFFICE OF THE INSPECTOR-GENERAL
Namibian Police Force
Private Bag 12024
Ausspannplatz
WINDHOEK
Namibia

06 November 2018

The Head
Secretariat Division
Namibian Police Force
Private Bag 12024
AUSSPANNPLATZ

RE: REQUEST FOR PARTICIPATION OF NAMPOL MEMBERS IN AN ACADEMIC RESEARCH PROJECT: NO. 015836 D. SHIPENA, SECRETARIAT DIVISION

Receipt of your letter dated 05 November 2018 regarding the above subject matter is hereby acknowledged with thanks.

No. 015836 D. Shipena is a student at University of Namibia pursuing her study toward Master of Arts in Security and Strategic Studies and applied to conduct an academic research study in the Namibian Police Force titled: ***"Designing a strategy for social media implications on Human Security in Namibia: Case study of Windhoek".***

The application is **approved**. The officer's must be urged to ensure that information that will be provided to her will be treated with high level of confidentiality and should not be used for any other purpose except for only this academic research.

The officer's interest and willingness to carry out a research study within the Namibian Police Force is highly appreciated. Hence, this office would appreciate sharing the research findings with the force.

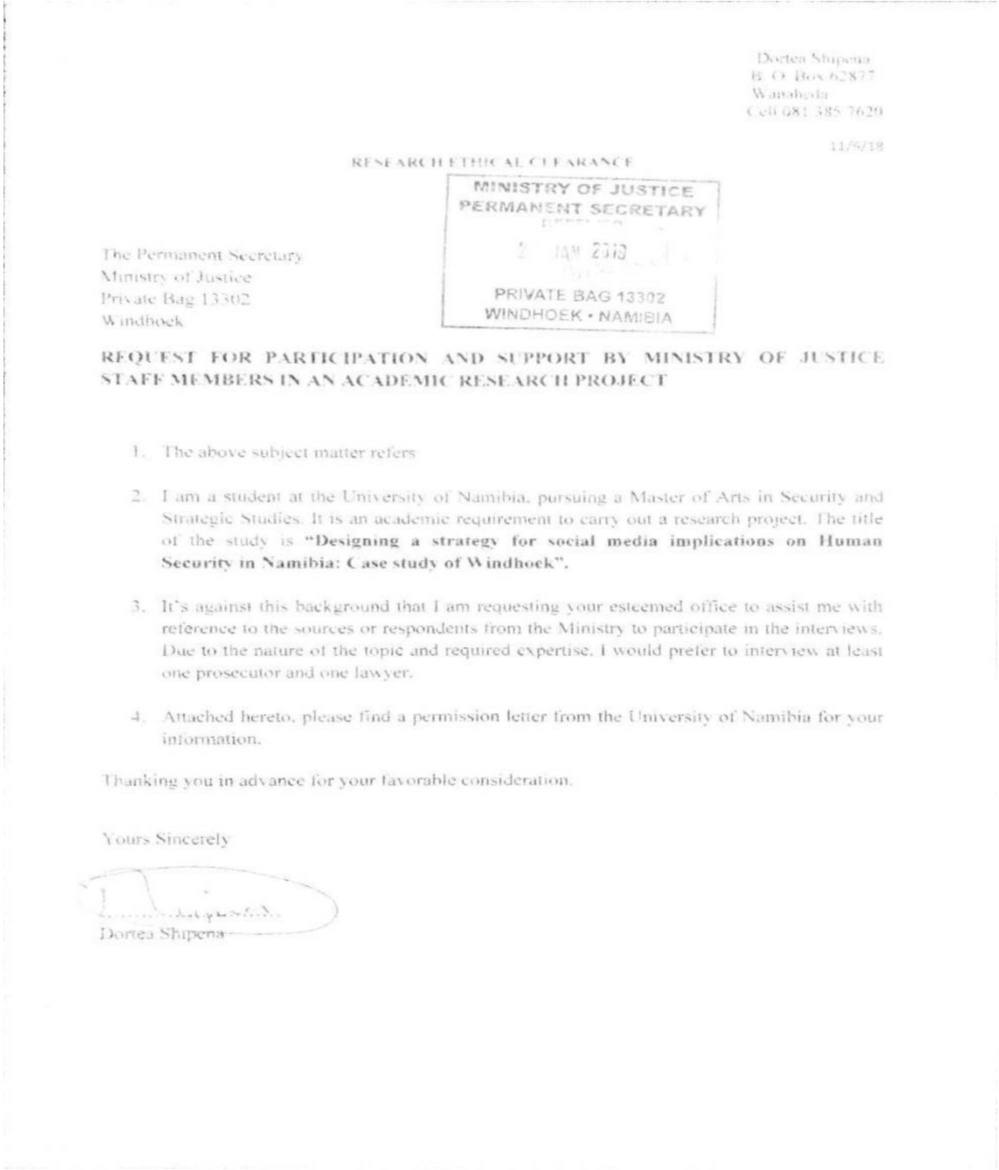
Best regards

06/11/18

NAMIBIAN POLICE
WINDHOEK
06-11-2018
INSPECTOR-GENERAL

LT-GEN
S.H. NDEITUNGA, OMS
INSPECTOR-GENERAL: NAMIBIAN POLICE FORCE

APPENDICES E: CONSENT L



Dortea Shipena
P. O. Box 62877
Wanaheda
Cell 081 385 7620

11/5/18

RESEARCH ETHICAL CLEARANCE

MINISTRY OF JUSTICE
PERMANENT SECRETARY
[illegible] JAN 2019
PRIVATE BAG 13302
WINDHOEK • NAMIBIA

The Permanent Secretary
Ministry of Justice
Private Bag 13302
Windhoek

REQUEST FOR PARTICIPATION AND SUPPORT BY MINISTRY OF JUSTICE STAFF MEMBERS IN AN ACADEMIC RESEARCH PROJECT

1. The above subject matter refers

2. I am a student at the University of Namibia, pursuing a Master of Arts in Security and Strategic Studies. It is an academic requirement to carry out a research project. The title of the study is **"Designing a strategy for social media implications on Human Security in Namibia: Case study of Windhoek".**

3. It's against this background that I am requesting your esteemed office to assist me with reference to the sources or respondents from the Ministry to participate in the interviews. Due to the nature of the topic and required expertise, I would prefer to interview at least one prosecutor and one lawyer.

4. Attached hereto, please find a permission letter from the University of Namibia for your information.

Thanking you in advance for your favorable consideration.

Yours Sincerely

Dortea Shipena