TREND OF CYBER CRIME IN NEPAL

APF Command and Staff College

Sanogaucharan, Kathmandu

A Thesis Submitted to

Department of Humanities and Social Sciences, Tribhuvan University

In Partial Fulfillment of Master Degree in Security, Development and Peace Studies

Submitted by

Sanjay Bhattarai

February, 2019

TREND OF CYBER CRIME IN NEPAL

APF Command and Staff College

Sanogaucharan, Kathmandu

A Thesis Submitted to

Department of Humanities and Social Sciences, Tribhuvan University

In Partial Fulfillment of Master Degree in Security, Development and Peace Studies

Submitted by

Sanjay BhaTTARAI

February, 2019

DECLARATION

I hereby declare that this thesis entitled **TREND OF CYBER CRIME IN NEPAL** submitted to the APF Command and Staff College, is entirely my original work under the guidance and supervision of my supervisor. I have made due acknowledgements to all ideas and information cited/extracted from different sources in course of preparing this research paper. The result of this research paper has not been presented or submitted anywhere else for the award of any degree or of any other purposes. I assure that no part of the content of this research paper has been published in any form before. I shall be solely responsible if any evidence is found against my research paper.

Signature: …….

Name: Sanjay Bhattarai

Date: 05, February,2019

LETTER OF RECOMMENDATION

I certify that this thesis entitled **TREND OF CYBER CRIME IN NEPAL** was prepared by Mr. Sanjay Bhattarai under my supervision. The researcher has fulfilled the criteria Preserved by the Central Department of Master's Degree in Security, Development and Peace Studies. I hereby recommended this thesis for the final evaluation and approval.

……..

Dr. Naresh Rimal

Supervisor

Date: o5, February, 2015

LETTER OF APPROVAL

This thesis entitled **TREND OF CYBER CRIME IN NEPAL** submitted by Sanjay Bhattarai has been accepted in partial fulfillment of the requirements for Master's Degree in Security, Development and Peace Studies.

EVALUATION COMMITTEE

…….

Supervisor: Dr. Naresh Rimal

Date:……

……..

External Examiner

Date: 05, February, 2015

……..

External Examiner

Date: 05, February, 2015

……..

External Examiner

Date: 05, February, 2015

ACKNOWLEDGEMENT

A deep sense of gratitude goes to Supervisor, Prof. Dr.Naresh Rimal, APF Command Staff College, for granting permission me to write this thesis on " Trend of Cyber Crime in Nepal", and also for his guidance, valuable suggestion, comment and encouragement in completion of this entire thesis. This form of the report is the outcome of his continuous encouragement in completion of this entire thesis.

I am indebted to all those who devoted themselves to bring the thesis in this topic. I thank all the resource persons and respondent for their contribution during the research work, I fell sincerely grateful to Additional Inspector General of APF (Retd.) Ravi Raj Thapa for his professional input and continuous guidance and encouragement.

It is matter of pleasure to acknowledge my sincere appreciation to Nepal Police, Crime Investigation Division and Central Investigation Bureau for provided essential material to make this thesis complete and respect to my friends and family members, for their dignified suggestions, guidance, and encouragement throughout the preparation of this paper, without which it would not be possible to come up in this form.

ABSTRACT

Over the last two decades, around the globe have moved into cyberspace and cloud environment in order to conduct their businesses. Many people spend a significant part of their daily life in cyberspace, creating and enjoying new types of social relationships which were not possible or financially affordable 20 years ago. However, criminals have identified rewards from online frauds therefore, the risks and threats have increased too.

As in Nepal, statistics shows that cybercrime has been rapidly increasing than that of before. A different analysis shows that in coming years the cybercrime which is very harmful as the physical harm would grow more than is present. With the collaboration of different vendors, the cybercrime in Nepal is trying to decrease. As can be seen the most common cybercrime in Nepal is fake profile marketing in social media like face book, twitter, Instragram and so on. Because nowadays people in Nepal are mostly involved in social media and had become a trend to have a fake profile of other for the stalking or bullying purposes, and also they don't know the consequences of having such crimes.

The study deals with primary data which are collected from questionnaires from security sector, victim person, students of college and also connected with the ways to controlling cybercrime In Nepal. The data shows that the trends of cybercrime in Nepal has been growing rapidly and deeply too. Securities concerning agencies are simultaneously trying to control such crime. Even the Nepal Police has been involving in the intent of decreasing the cybercrimes. Having strong laws in the field of cyber may help in stopping the trends of cybercrime in Nepal. The percentage of cybercrime is to be higher than it was in the previous. One should stay alert for the upcoming threats in the field of internet technology.

The trends of cybercrime in Nepal are more dangerous so need to be active than that of former and should also be focused on how to forbid the imminent threats and how can it be overcome in the future.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS / ACRONYMS

ATM	Automated Teller Machine
AUP	Acceptable Use Policy
CIB	Crime Investigation Bureau
CID	Crime Investigation Division
CEO	Chief Executive Officer
DDoS	Distributed Denial of Service
DoS	Denial-of-Service
ETA	Electronic Transaction Act
FAT	File Allocation Table
ID	Identity
IP	Internet Protocol
ISACA	Information System Audit and Control Association
ICT	Information and Communication Technology
IT	Information Technology
MoIC	Ministry of Information and Communication
PIN	Postal Index Number

CHAPTER I

INTRODUCTION

1. Background

At present cyberspace has been the important aspect of human life. The computerized system controls most of the fields like power delivery, communications, aviation, financial institutions, administrative and security services etc. They are used to regulate vital resources and store vital information too. Widespread use of internet and growth in the field of Information Technology (IT) using computers and handheld devices online has made the entire world a global village (Subedi, 2015). Most of the systems are connected to public domain, thus making accessibility in wider reach. However, public domains being open to all are vulnerable to cyber threats. Organized crimes in open cyberspace have scaled up to highest level and new domain of committing crime has evolved.

In 2011, the United Nations Department of Economic and Social Affairs had observed cyber crime as a complex transnational issue that requires global cooperation to ensure a safe internet. The Global Cyber Crime Status Report, released by Information System Audit and Control Association (ISACA) in January 2015 reveals that 83% of the people feel cyber crimes are among the top three threats facing organizations today. Organized cyber crimes have been launched in defence systems, financial systems, service delivery systems and other vital systems. These offensive activities in online world had led to evolve new dimension in terrorism commonly known as cyber terrorism (Panta, 2016).

In the Nepalese context, numbers of internet users are rising day by day. According to the Nepal Telecom Authority, internet users had reached about 15388770 and internet penetration is 58.08 % in Nepal till March 2017 (Panta, 2016, p. 17). Numerous online websites are serving the need of people, this has led to maximum consumption of national bandwidth. Government of Nepal has launched various web applications to reach out government service to public. Security forces of Nepal have also launched web interface to disseminate information to public interest. These systems

are always in constant threats from cyber terrorists and substantial challenge to cyber experts (Panta, 2016).

It has been expected and almost confirmed that along with the rise in the number of internet penetration the crime related to internet have increased. In context of Nepal it had its first exposure to computer systems as early as 1971. However, the real progress in the Information and Communication Technology (ICT) arena of the country can be considered to have happened only after 1995 (Chapagain, 2006).

The advancement of technology has enabled people around the world to use internet in their daily activities. In western world, one out of three people are now planning to conduct and promote their business through online as internet has become a platform to communicate with the customers. Though, in case of Nepal it may not be the same, however, it is raising (Pant, 2016).

Cyber crime is neither much hard to learn nor much difficult to commit. In modern society, computer technology can be learned like a language. Digital technology has surrounded our life to such a great extent that everybody is being acquainted with it., knowingly or unknowingly. Particularly the new generation, for whom computer knowledge is an essential part of curriculum and where knowledge diffusion is done with the help of computer, it is very easy for them to have accessible means to commit crime in cyberspace.

Real life instances are there where initially, computer is learned either out of curiosity, pleasure or compulsion and latter the knowledge gained is turned into delinquency. The user friendly software which guides a novice step by step, has added fuel to the fire making cyber delinquency much pleasant and effortless (Sharma, 2010, p. 146). This is true, particularly with regard to pornography, vulgar chatting and piracy. Today, anybody with minimum computer literacy is sufficient to have access to cyber criminality and the chances are very less of being trapped by the preventive agencies. These features make cyber crime more alarming and difficult to rein in (Sharma, 2010).

The Cyber Crime Division of Nepal Police has stated that the cyber related crime, especially; crimes through social sites have been increased where the perpetrators as well as the victims are generally kids. The official page of the Cyber Crime Division

of Nepal Police further states “reports of alleged computer crime have been a hot news item of late. Especially alarming is the realization that many of the masterminds behind these criminal acts are mere kids. In fact, children no longer need to be highly skilled in order to execute cyber crimes. "Hacker tools" are easily available on the Net and, once downloaded, can be used by even novice computer users. This greatly expands the population of possible wrongdoers. Children (and in some cases - their parents) often think that shutting down or defacing websites or releasing network viruses are amusing pranks. Kids might not even realize that what they are doing is illegal. Still other kids might find themselves hanging out online with skilled hackers who share hacking tools with them and encourage them to do inappropriate things online. Unfortunately, some of these kids don't realize that they are committing crimes until it is too late. Even more distressing and difficult to combat is the fact that some in the media portray the computer criminal as a modern day Robin Hood. Nothing could be further from the truth.”

1.2 Statement of Problem

Along with the rise of the internet users it is obvious that the number of crime is likely to increase. Nepal is not an exception. The Cyber Crime Division of Nepal Police is active in investigating and arresting the criminals since a long time back. The indicators of the criminal activities and their qualities as well as the quantities should be considered continually. Likewise the capacity of the government to counter such activities directly affects the trust of the general population upon it.

On the other hand, cyber crime is a new type of social crime. Defamation, rumors, extortion through blackmail and similar types of activities brings social disharmony which ultimately will affect the national unity and security. A nation with high incidence of crime, may it be in the real world or in the virtual world, can hardly prosper leading to disunity and underdevelopment. It is clear that an underdeveloped country always has a security threat.

Every country faces the cyber threat and cyber crime according to the level of development of the cyber space of that very country. The western world has its own range of cyber threat and the cyber crime which are being committed. The level of electronic transaction performed also dictates the level of cyber crimes committed.

Similarly, the cyber law and penal code regarding cyber offence of a country equally affects the level of commitment of cyber crime in the country.

In Nepal, Prior to 2004, cyber crimes were dealt under the Public Offence Act. Electronic Transaction Act (ETA) 2063 was passed in 2004 which is known as the cyber law. It protects users online against cyber crimes. Although the law is present, it serves little protecting the users online. The law has not been adequately amended as a need of time. The elements and dynamics of the web has been changing over time whereas the ETA remains constant.

Trend of cyber crime has changed in Nepal in comparison to previous years. Before, it was limited to data piracy, email blackmail, SMS blackmail, etc. whereas today it has reached a wide variety such as phishing , unauthorized access, online fraud, online illegal activities, etc. And there's whole another level of social media related crime going on.

1.3 Research Questions

Nepal, a landlocked country positioned in South Asia cannot be exceptional territory for commission of cyber crime. The incidence of cyber crime in Nepal is directly proportional to the level of progress made in Nepal in information technology. The internet users in Nepal have been rampantly increased. Increase in internet user has certainly increased the instances of cyber crime in Nepal. Newspaper reports, police reports, the database of the police, judicial decisions and data from scholars' articles support the fact that Nepal has been evidenced as a hub for increasing cyber crime in recent days. The media almost daily reports cases regarding cyber crime in Nepal, which however is not same when researcher examines the report of courts and police, which means that the instances of cyber crime are either unreported or the perpetrator is not invoked with offence. Thus this thesis broadly intends to highlight the trend of cyber crime in Nepal and actions have been taking to control such crime.

1.3.1 What are the trends of cyber crime in Nepal?

1.3.2 What are the actions taken so far to mitigate the cyber crime issue in Nepal?

1.3.3 What are the viable options to mitigate the issue?

1.4 Objectives of the Study

The objective of this study is to seek answers of those above mentioned research questions. All questions have answered in order to formulate specific research study. Thesis has primarily deals with the current trend and status of cyber crime in Nepal. This thesis aims to achieve the following objectives:

1.4.1 To provide the current status and trend of cyber crime in Nepal.

1.4.2 To analyze of actions taken by government, Policies, Act to mitigate the cyber crime in Nepal.

1.4.3 To identify possible options to mitigate the issue.

1.5 Significance of the study

The thesis will help everyone to understand about the current situation and trend of cyber crime in Nepal. What kind of activity is considered as cyber crime. Form this, every individual can take appropriate precaution to be safe from such activities and specially, everyone can prevent themselves from the unnecessary mental stress. It will also help to security offices to take knowledge about the status and trend of cyber crime in Nepal. With the help of viable option, they can take necessary actions to fight and mitigate such crime.

1.6 Limitation of the study

There are various limitations to the methodology employed in this thesis. The scope of the study is mainly confined within the analysis of current trend of cyber crime in Nepal. The crime that related to the cyber is recognized by Nepal is not so long enough. So, lack of sufficient books and literatures especially in the case of Nepal, this study is based on few books, journals, different web sites, publications, reports of Nepal Police and other stakeholders, perceptions of the related personal and public reports made by Nepal Police. Due to lack of sufficient research on cyber crime in Nepal, every aspect that related to the cyber crime could not cover in detail. Moreover much of the study has relied on the analysis of pre-existing literature and related questionnaires with cyber crime branch of Nepal Police and other concerned.

CHAPTER II

REVIEW OF THE LITERATURE

Defining cyber crime appears to be a necessary evil within the community of people involved in researching, investigating, and prosecuting their occurrence. Why people endeavor to define the term is not clear. Perhaps it is because the term held specific meaning years ago when there were fewer ways in which computer technology could be involved in criminal activity—and by hanging on to the term we are magically transported to the good ol' days. Maybe the media has used "cyber crime" as a term of convenience and now the term sits within the collective consciousness of the public, even though the public may feel the catchiness of the term but not understand the depth and breadth of the activities involved. Several scholars and authors have attempted to place definitional boundaries around the term cyber crime, but its meaning has grown as the range of criminal activity facilitated by computer was inevitably lumped under the cyber crime heading (Reyes, 2007).

Cyber crime has proliferated exponentially across the globe; those in the criminal justice field have lacked suitable and updated knowledge concerning the pedestrian reality of modern cyber crime. Popular media has created an image of cyber crime that suggests a lone hacker breaking through seemingly impossible security measures to access lucrative secret data. Crimes like these are very rare, but cyber crime is all too common. The cyber criminals use the internet for the purpose of committing fraud, harassment, download illegal pornography, or download stolen music far more than they use the Internet with the bad intention to violate the security of countries both at national and international level (Agustina, 2012).

Cyber crime is rising day by day. It is one of the most dangerous social offences in the world. If cyber users are careful, it can be reduced radically. Most of the cyber crime happens due to poor authenticity. So, users must have a good knowledge of strong password technique. It is more dangerous in developing countries than in developed countries due to the knowledge levels of users, the cases of cyber crime in developing and developed countries are different. Developed countries are facing cyber security issues such as data stolen, but in the developing and under developed countries, the

cyber security issues related to personal issues such as misusing social media accounts. In this way, most of the cases are related with poor authenticity, so both users and service providers should be careful of using authentication (Roka, 2017).

The rapid growth in Internet use in Asia, including a tenfold or more increases in access in China, Indonesia and India since 2002 has also been accompanied by significant increases in cyber crime.
The development of commercial-scale exploits toolkits and criminal networks that focus on monetization of malware have amplified the risks of cyber crime. (Broadhurst, 2013). Increasing no. of internet users from 2002 to 2017 also increasing the cyber crime in Asia Pacific which is shown in AppendixA.

The facilities of computer technology have not come out without drawbacks. Though it makes the life so speedy and fast, but hurled under the eclipse of threat from the deadliest type of criminality termed as 'Cyber crime' without computers, entire businesses and government operations would almost cease to function. This proliferation of cheap, powerful, user-friendly computers has enabled more and more people to use them and, more importantly, rely on them as part of their normal way of life. As businesses, government agencies, and individuals continue to rely on them more and more, so do the criminals Restriction of cyber crimes is dependent on proper analysis of their behavior and understanding of their impacts over various levels of society. Therefore, in the current manuscript a systematic understanding of cyber crimes and their impacts over various areas like Soci-eco-political, consumer trust, teenager etc.with the future trends of cyber crimes are explained (Das & Nayak, 2013).

Commonly used modes of social engineering are via the telephone or through the Internet, although face-to-face conversations also form part of the social engineer's repertoire of techniques. Social engineering attacks rely on the victim's natural human tendency to trust rather than rigidly following security policies. In general, security professionals agree that human beings are the weakest link in computer and network security; social engineers confirm this fact through their exploits (Bagyavati, 2009).

Through a variety of easy tricks, attackers can hijack a person's social network account to use as a launching pad for additional attacks against other users, other Web

2.0-based applications, and so on. Social networks can also be incorporated into micro botnets and, by rummaging through a page of misfired direct messages on Twitter, a motivated attacker can unearth the cell phone numbers of prominent people (Brenner, 2009).

The hottest new craze among teens and young adults on the Internet is social networking. But concerns related to teen use of social networking sites include unsafe disclosure of personal information, risky sexual behaviour, 'cyber bullying', involvement with dangerous communities and groups, and posting 'cyber threats'. Recent news coverage has raised significant concerns about interactions with strangers, especially sexual predators, on these sites. Many teens spend little time, if any, interacting with online strangers. The vast majority of teens are using social networking sites to engage with known friends and acquaintances from within their school and community. For some, their friendship network may expand to include others they meet in discussion groups. These friends likely are ones with whom they share mutual interests (Willard, 2007).

Various web sites have sprung up for the sole purpose of providing a place for users to express themselves, share with like-minded individuals, discover new things, and communicate with others. There have been numerous instances of sexual predators and child molesters posing as children to network with young victims on MySpace.com. MySpace was also recently discovered to be compromised by attackers spreading malware on exploited profile sites. MySpace has taken steps and implemented security measures to minimize this problem, but users should still be cautious and aware. While not directly related to a social network, Craigslist, the popular regional classified listings site, was recently used by a predator to lure a victim to her death. After listing a job opening for a babysitter / nanny, and arranging a meeting with the potential nanny, the killer then murdered the prospective nanny. Photo sharing sites are used by thousands of families to post and share family photos. It is possible to restrict access and only let users you identify view the pictures, but many users are proud of their kids and their photographic skills and allow the general public to view the photos as well. Child molesters and sexual deviants can search through these sites and bookmark their favorite photos of young boys and girls (Bradley, 2009).

in their study ‘Safety issues in Orkut for Girls’ found out that most girls do not take much precautionary steps to stay safe until they were affected, they were not very suspicious about strangers sending them friend requests until they were affected, they were not much aware of the different types of cyber crimes and cyber laws and they were not aware of the different types of cyber crimes and cyber laws (Bharkavi and Sheeba, 2009).

Leyden (2014) in the article ‘Social networkers risk losing their identities’ says many adult users of social network sites such as MySpace and Facebook expose themselves to risk from identity thieves and hackers. He points out that the focus of concerns over social networking sites has so far focused on incidents where online predators have used the sites to "groom" potential child victims for abuse (Leyden, 2014).

Thakuri (2014), in his dissertation Status of Cyber Security in Nepal states that cyber crime is any illegal act committed by using a computer network where Computer is involved in the facilitation or commission of a criminal act. The Internet is an extremely popular way for criminals to commit acts involving computers because it is more time efficient, reach more people, less expensive to contact individual people and can be more difficult to locate and prosecute offenders. It is Unlawful acts where in the computer is either a tool or a target or both. Expressing the steps of Government of Nepal for the prevention of cyber crime, he states, that the government has enforced Electronic Transaction Act on 8th December 2008 with a view to make legal provisions for authentication and regularization of the recognition, validity, integrity and reliability of generation, production, processing, storage, communication and transmission system of electronic records by making the transactions to be carried out by means of electronic data exchange or by any other means of electronic communications, reliable and secured (Thakuri, 2014).

Cyber crime is one of the fastest growing areas of crime around the globe. It can be committed residing in any part of world against individual/institution situated in other part. Advancing technologies have made people easier to commit these crimes. More and more criminals are exploiting the speed, convenience of the modern technology to commit more diverse types of crimes. Nepal is not an exception when it comes to threat of cyber crime. Increasing internet and computer users, and the growth of technology has resulted the use of computers for cyber crime. Most Nepalese use

computers and internet for entertainment purpose and are not aware of the risk they are involved in. They probably do not have the knowledge of cyber security. As many as 560 cases of cyber crime have been registered in the first six months of the fiscal year 2017, according to the Metropolitan Crime Division in Teku,, most of such cases took place through the social networking sites such as Facebook, Twitter and Viber. With the development of technology, the cases of cyber crime were on the rise in the city. The Division had received a total of 830 complaints related to cyber crime in fiscal year 2016 (Cases of cyber crime registered in six month," 2017).

Nepalese society has become dynamic along with the development in new technology. With the increase of computer users, misuse of technology has also increased, which has increased the cyber crimes in Nepal. A Cyber Crime is an act of creating, distributing, altering, stealing, misusing and destroying information through the computer without the use of physical force and against the will or interest of the victim. It can be committed by any person living in one part of the world against another person or institution living in another part of world. According to Kathmandu District Court, total 50 cases has been filed in fiscal year 2015/16 out of which 19 cases of harassment of women were reported. Only 27 cases has been filed in fiscal year 2016/17 out of which 14 cases of harassment were reported. This shows that people are not going to court for getting to court either because they are unaware about cyber crime and cyber law or they feel that their dignity will be hampered if they go to court for such issues. Girls are more victimized by cyber crime in Nepal (Dhakal, 2018).

By viewing thoroughly all above subscribed literatures, the gap here apparently exists to address the research problem. With the unavailability of adequate and genuine literatures in domestic context about cyber crime allow research problem needed be further investigated. As per the record of the crime investigation department of Nepal Police, the trend of cyber crime in Nepal is increasing day by day. However, there is Electronic Transaction *Act* (ETA) 2063 has been formulated in Nepal to control such type of crime. Due to the poor implementation of law, lack of public awareness/education and fear to be embarrassed to file the case against, the incidents of cyber crime is amplifying each day. To control such type of crime, Nepal Police has taken initiative and established the cyber crime investigation branch.

CHAPTER III

RESEARCH METHODOLOGY

This study employs a descriptive and analytical approach. The data that used in this paper are based on primary and secondary source. Primary data have collected form questionnaires from different concerned stakeholders and secondary data have collected from library books, e-books, newspaper and internet. Internet websites used to extent in search of relevant inputs.

3.1 Research Plan and Design

The research design refers to the overall strategy to integrate the different components of the study in a coherent and logical way, thereby, ensuring us to effectively address the research problem.

This constitutes the collection, measurement, and analysis of data. A research design is the set of methods and procedures used in collecting and analyzing measures of the variables specified in the research problem. Research design is the framework that has been created to find answers to research question.

The study has adopted exploratory method in order to ensure the evidence obtained from different sources. Primary and secondary sources have used to generate absolute findings.

Qualitative data analysis is the main instrument for this study. The study has conducted to analyze the trend of cyber crime in Nepal. Therefore this research work is exploratory and descriptive in nature. The overall research work has been conducted through collection of primary and secondary data.

3.2 Study Area

The area of this study has based on the fundamental material of the concern subject matter. Facts have collected from questionnaires. So this research materials have based on the primary as well as secondary data based obtained from books, journals,

articles and websites. The main area of study has focused on discovering the trend of cyber crime in Nepal correlated with action taken to mitigate such crime.

3.3 Source of Data

Specifically, I have collected data from security agencies of Nepal, related individual, Library books, e-books, newspaper and internet websites that are used to great extent in search of relevant inputs.

3.4 Data Processing, Analysis and Presentation

Primary and secondary data collected from different sources have analyzed, processed with peculiar presentation and conclude for appropriate findings. Unnecessary information beyond from objective have removed and concise editing has carried out through detail analysis.

CHAPTER IV

RESULT AND DISCUSSION

4.1 General

In this chapter the general trends of cyber crimes those are being faced in Nepal are dealt. The activities which are considered as cyber crime by law are described in a sequential manner. At first the concept of cyber crime in the world perspective will be established and then in the Nepalese perspective would be defined. Similarly the cyber related crimes those are in practice will be dealt. Basically, the cases which are more often reported to the cyber crime division of Nepal Police are dug in detail and discuss on action taken so far to mitigate or control such crime in Nepal by different concerned.

4.2 Overview on Cyber Crime

Cyber crime is the emerging crime around the globe which has unique modus operandi and can be committed being domiciled in any part of world against individual/institution situated in other part. Technocrats are well affirmed with the threat of cyber crime so are constantly working to develop new technology so as to prevent cyber crime, i.e. the world stands at a crossroads for developing defence mechanisms against it. Most cyber crimes, however, do not involve violence but rather greed, pride, or play on some character weakness of the victims. It is difficult to identify the culprit, as the net can be a vicious web of deceit and can be accessed from any part of the globe. For these reasons, cyber crimes are considered as "white- collar crimes" (Phulara, 2004). Furthermore, cyber crime produces high returns at low risk and (relatively) low cost for the perpetrators. The rate of return on cyber crime favors the criminal; the incentive is to steal more. The rate of return per victim on cyber crime can be very low, but because the costs and risks of engaging in it are even lower, cyber crime remains an irresistible criminal activity.

Cyber crime can generally be divided into two broad categories – crime that are facilitated by computers or the internet, and crimes against computers or computer system (Ferrera, 2012). Cyber-crime is an extension of traditional crime but it takes

place in cyberspace -- the nonphysical environment created by computer systems. By utilizing globally connected phone systems and the world's largest computer network, the Internet, cyber-criminals are able to reach out from just about anywhere in the world to just about any computer system, as long as they have access to a communications link. Ability of world wide access has resulted into territory-less dimension of cyber crime. Cyber crime, therefore, has an international aspect that creates many difficulties for nations that may wish to halt it or simply mitigate its effects. Moreover, cyber-crime is generally understood as the use of a computer-based means to commit an illegal act. One typical definition describes cyber-crime as "any crime that is facilitated or committed using a computer, network, or hardware device." (Gabrys, 2002). As cyber crime is not bound by physical borders the criminal can found anywhere around the world – which itself has made cyber crime as universal natured crime.

The criminal activities to constitute as cyber crime is itself not clearly developed and there is no exhaustive list providing all set of cyber crime. There are number of definition of cyber crime which has separate specification of crime categorizing as cyber crime. The scope of criminal activities and their social consequences can be summarized by a typology of computer-related crime that comprises of two sets of crimes, i.e., conventional crimes, in which computers are instrumental to the offence, such as online attacks on computer networks, destruction of databases etc and conventional criminal cases in which evidence exists in digital form, such as cyber-vandalism and terrorism, insertion of viruses, worms, defamation, extortion, etc (Broadhurst, 2006).

Cyber crime is a set of criminal activities perpetrated by using computer and internet. This includes anything from downloading illegal music files to stealing millions of dollars from online bank accounts. Cyber crime also represents non-monetary offenses, such as creating and distributing viruses on the other computers or posting confidential business information on the internet, without authorization. Thus, cyber crime may be defined as an offence in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offence (child pornography, hate crimes etc) (Sharma, 2010).

Cyber crime is any illegal act committed by using a computer network where Computer is involved in the facilitation or commission of a criminal act. The Internet is an extremely popular way for criminals to commit acts involving computers because it is more time efficient, reach more people, less expensive to contact individual people and can be more difficult to locate and prosecute offenders. It is Unlawful acts where in the computer is either a tool or a target or both (Singh, 2014).

There are some amazing facts about cyber crime such as:-

4.2.1 cyber crime is global phenomenon which does not have any territorial barriers or jurisdictional restrictions, there is non-existence of any physical evidence, evidence of cyber crime is in digital format identified only by trained and skilled person, perpetrator of cyber crime largely be technocrats.

4.2.2 cyber crime is new approach identified by perpetrator such as electronic vandalism, transnational crime, electronic money laundering, counterfeiting, etc which includes computer network attack as well as electronic approach of committing traditional crimes and there is no requirement of disclosure of identity – can manage anonymity.

4.2.3 Cyber crime has now surpassed illegal drug trafficking as a criminal money spinner.

4.2.4 Someone's identity is stolen every three seconds as a result of cyber crime.

4.2.5 In the absence of sophisticated security package our unprotected pc can become infected within four minutes of connecting to the internet.

4.3 Types of Cyber crime

There are literally a dozen ways in which a cyber crime can be perpetrated. In order to protect from that threats, need to know about the different ways in which computer can be compromised and privacy infringed. In this section, discuss a few common tools and techniques employed by the cyber criminals. This isn't an exhaustive list by any means, but will give a comprehensive idea of the loopholes in networks and security systems, which can be exploited by attackers, and also their possible motives for doing so.

4.3.1 Hacking

In simple words, hacking is an act committed by an intruder by accessing computer system without permission. Hackers (the people doing the 'hacking') are basically computer programmers, who have an advanced understanding of computers and commonly misuse this knowledge for devious reasons. They're usually technology buffs who have expert-level skills in one particular software program or language. As for motives, there could be several, but the most common are pretty simple and can be explained by a human tendency such as greed, fame, power, etc. Some people do it purely to show-off their expertise – ranging from relatively harmless activities such as modifying software (and even hardware) to carry out tasks that are outside the creator's intent, others just want to cause destruction.

Greed and sometimes voyeuristic tendencies may cause a hacker to break into systems to steal personal banking information, a corporation's financial data, etc. They also try and modify systems so that they can execute tasks at their whims. Hackers displaying such destructive conduct are also called "Crackers" at times.

They are also called "Black Hat" hackers On the other hand; there are those who develop an interest in computer hacking just out of intellectual curiosity. Some companies hire these computer enthusiasts to find flaws in their security systems and help fix them. Referred to as "White Hat" hackers, these guys are against the abuse of computer systems.

They attempt to break into network systems purely to alert the owners of flaws. It's not always altruistic, though, because many do this for fame as well, in order to land jobs with top companies, or just to be termed as security experts. "Grey Hat" is another term used to refer to hacking activities that are a cross between black and white hacking.

Some of the most famous computer geniuses were once hackers who went on to use their skills for constructive technological development. Dennis Ritchie and Ken Thompson, the creators of the UNIX operating system (Linux's predecessor), were two of them. Shawn Fanning, the developer of Napster, Mark Zuckerberg of Facebook fame, and many more are also examples.

4.3.2 Virus Dissemination

Viruses are computer programs that attach themselves to or infect a system or files, and have a tendency to circulate to other computers on a network. They disrupt the computer operation and affect the data stored – either by modifying it or by deleting it altogether. “Worms” unlike viruses don’t need a host to cling on to. They merely replicate until they eat up all available memory in the system. The term “worm” is sometimes used to mean self replicating “malware” (MALicious softWARE). These terms are often used interchangeably in the context of the hybrid viruses/worms that dominate the current virus scenario. “Trojan horses” are different from viruses in their manner of propagation.

They masquerade as a legitimate file, such as an email attachment from a supposed friend with a very believable name, and don’t disseminate themselves. The user can also unknowingly install a Trojan-infected program via drive-by downloads when visiting a website, playing online games or using internet-driven applications. A Trojan horse can cause damage similar to other viruses, such as steal information or hamper/disrupt the functioning of computer systems.

How does this happen? The malicious code or virus is inserted into the chain of command so that when the infected program is run, the viral code is also executed (or in some cases, runs instead of the legitimate program). Viruses are usually seen as extraneous code attached to a host program, but this isn’t always the case. Sometimes, the environment is manipulated so that calling a legitimate uninfected program calls the viral program. The viral program may also be executed before any other program is run. This can virtually infect every executable file on the computer, even though none of those files’ code was actually tampered with. Viruses that follow this modus operandi include “cluster” or “FAT” (File Allocation Table) viruses, which redirect system pointers to infected files, associate viruses and viruses that modify the Windows Registry directory entries so that their own code is executed before any other legitimate program.

Computer viruses usually spread via removable media or the internet. A flash disk, CD-ROM, magnetic tape or other storage device that has been in an infected computer infects all future computers in which it’s used. Computer can also contract

viruses from sinister email attachments, rogue web sites or infected software. And these disseminate to every other computer on network.

All computer viruses cause direct or indirect economic damages. Based on this, there are two categories of viruses:

1) Those that only disseminate and don't cause intentional damage

2) Those which are programmed to cause damage.

However, even by disseminating, they take up plenty of memory space, and time and resources that are spent on the clean-up job. Direct economic damages are caused when viruses alter the information during digital transmission. Considerable expenses are incurred by individuals, firms and authorities for developing and implementing the anti-virus tools to protect computer systems.

4.3.3 Logic Bombs

A logic bomb, also known as "slag code", is a malicious piece of code which is intentionally inserted into software to execute a malicious task when triggered by a specific event. It's not a virus, although it usually behaves in a similar manner. It is stealthily inserted into the program where it lies dormant until specified conditions are met. Malicious software such as viruses and worms often contain logic bombs which are triggered at a specific payload or at a predefined time. The payload of a logic bomb is unknown to the user of the software, and the task that it executes unwanted. Program codes that are scheduled to execute at a particular time are known as "time-bombs". For example, the infamous "Friday the 13th" virus which attacked the host systems only on specific dates; it "exploded" (duplicated itself) every Friday that happened to be the thirteenth of a month, thus causing system slowdowns.

Logic bombs are usually employed by disgruntled employees working in the IT sector. It may have heard of "disgruntled employee syndrome" wherein angry employees who've been fired use logic bombs to delete the databases of their employers, stultify the network for a while or even do insider trading. Triggers associated with the execution of logic bombs can be a specific date and time, a missing entry from a database or not putting in a command at the usual time, meaning the person doesn't work there anymore. Most logic bombs stay only in the network

they were employed in. So in most cases, they're an insider job. This makes them easier to design and execute than a virus. It doesn't need to replicate; which is a more complex job.

4.3.4 Denial-of-Service Attack

A Denial-of-Service (DoS) attack is an explicit attempt by attackers to deny service to intended users of that service. It involves flooding a computer resource with more requests than it can handle consuming its available bandwidth which results in server overload. This causes the resource (e.g. a web server) to crash or slow down significantly so that no one can access it. Using this technique, the attacker can render a web site inoperable by sending massive amounts of traffic to the targeted site. A site may temporarily malfunction or crash completely, in any case resulting in inability of the system to communicate adequately. DoS attacks violate the acceptable use policies of virtually all internet service providers.

Another variation to a denial-of-service attack is known as a "Distributed Denial of Service" (DDoS) attack wherein a number of geographically widespread perpetrators flood the network traffic. Denial-of-Service attacks typically target high profile web site servers belonging to banks and credit card payment gateways. Websites of companies such as Amazon, CNN, Yahoo, Twitter and eBay! are not spared either.

4.3.5 Phishing

This a technique of extracting confidential information such as credit card numbers and username password combos by masquerading as a legitimate enterprise. Phishing is typically carried out by email spoofing. The malware would have installed itself on computer and stolen private information. Cyber-criminals use social engineering to trick into downloading malware off the internet or make fill in your personal information under false pretenses. A phishing scam in an email message can be evaded by keeping certain things in mind.

Not all phishing is done via email or web sites. Vishing (voice phishing) involves calls to victims using fake identity fooling into considering the call to be from a trusted organization. They may claim to be from a bank asking to dial a number (provided by VoIP service and owned by attacker) and enter account details. Once do

that, account security is compromised. Treat all unsolicited phone calls with skepticism and never provide any personal information. Many banks have issued preemptive warnings informing their users of phishing scams and the do's and don'ts regarding your account information. Those of reading Digit for long enough will remember that we successfully phished hundreds of readers by reporting a way to hack other people's gmail accounts by sending an email to a made up account with anyone own username and password.

4.3.6 Email Bombing and Spamming

Email bombing is characterized by an abuser sending huge volumes of email to a target address resulting in victim's email account or mail servers crashing. The message is meaningless and excessively long in order to consume network resources. If multiple accounts of a mail server are targeted, it may have a denial-of-service impact. Such mail arriving frequently in mail inbox can be easily detected by spam filters. Email bombing is commonly carried out using botnets (private internet connected computers whose security has been compromised by malware and under the attacker's control) as a DDoS attack.

This type of attack is more difficult to control due to multiple source addresses and the bots which are programmed to send different messages to defeat spam filters. "Spamming" is a variant of email bombing. Here unsolicited bulk messages are sent to a large number of users, indiscriminately. Opening links given in spam mails may lead to phishing web sites hosting malware. Spam mail may also have infected files as attachments. Email spamming worsens when the recipient replies to the email causing all the original addressees to receive the reply. Spammers collect email addresses from customer lists, newsgroups, chat-rooms, web sites and viruses which harvest users' address books, and sell them to other spammers as well. A large amount of spam is sent to invalid email addresses.

Sending spam violates the acceptable use policy (AUP) of almost all internet service providers. If system suddenly becomes sluggish (email loads slowly or doesn't appear to be sent or received), the reason may be that mailer is processing a large number of messages. Unfortunately, at this time, there's no way to completely prevent email bombing and spam mails as it's impossible to predict the origin of the next attack.

4.3.7 Web Jacking

Web jacking derives its name from “hijacking”. Here, the hacker takes control of a web site fraudulently. He may change the content of the original site or even redirect the user to another fake similar looking page controlled by him. The owner of the web site has no more control and the attacker may use the web site for his own selfish interests. Cases have been reported where the attacker has asked for ransom, and even posted obscene material on the site.

4.3.8 Cyber Stalking

Cyber stalking is a new form of internet crime in our society when a person is pursued or followed online. A cyber stalker doesn’t physically follow his victim; he does it virtually by following his online activity to harvest information about the stalkee and harass him or her and make threats using verbal intimidation. It’s an invasion of one’s online privacy.

Cyber stalking uses the internet or any other electronic means and is different from offline stalking, but is usually accompanied by it. Most victims of this crime are women who are stalked by men and children who are stalked by adult predators and pedophiles. Cyber stalkers thrive on inexperienced web users who are not well aware of netiquette and the rules of internet safety. A cyber stalker may be a stranger, but could just as easily be someone you know.

Cyber stalkers harass their victims via email, chat rooms, web sites, discussion forums and open publishing web sites (e.g. blogs). The availability of free email / web site space and the anonymity provided by chat rooms and forums has contributed to the increase of cyber stalking incidents. Everyone has an online presence nowadays, and it’s really easy to do a Google search and get one’s name, pseudonym, contact number and address, contributing to the menace that is cyber stalking. As the internet is increasingly becoming an integral part of our personal and professional lives, stalkers can take advantage of the ease of communications and the availability of personal information only a few mouse clicks away. In addition, the anonymous and non-confrontational nature of internet communications further tosses away any

disincentives in the way of cyber stalking. Cyber stalking is done in two primary ways:

Cyber stalking has now spread its wings to social networking. With the increased use of social media such as Facebook, Twitter, Flickr and YouTube, profile, photos, and status updates are up for the world to see. Online presence provides enough information for to become a potential victim of stalking without even being aware of the risk. With the “check-ins”, the “life-events”, apps which access personal information and the need to put up just about everything that we’re doing and where we’re doing it, one doesn’t really leave anything for the stalkers to figure out for themselves. Social networking technology provides a social and collaborative platform for internet users to interact, express their thoughts and share almost everything about their lives. Though it promotes socialization amongst people, along the way it contributes to the rise of internet violations.

4.3.9 Data Diddling

Data Diddling is unauthorized altering of data before or during entry into a computer system, and then changing it back after processing is done. Using this technique, the attacker may modify the expected output and is difficult to track. In other words, the original information to be entered is changed, either by a person typing in the data, a virus that’s programmed to change the data, the programmer of the database or application, or anyone else involved in the process of creating, recording, encoding, examining, checking, converting or transmitting data.

This is one of the simplest methods of committing a computer-related crime, because even a computer amateur can do it. Despite this being an effortless task, it can have detrimental effects. For example, a person responsible for accounting may change data about themselves or a friend or relative showing that they’re paid in full. By altering or failing to enter the information, they’re able to steal from the enterprise. Other examples include forging or counterfeiting documents and exchanging valid computer tapes or cards with prepared replacements. Electricity boards in India have been victims of data diddling by computer criminals when private parties were computerizing their systems.

4.3.10 Identity Theft and Credit Card Fraud

Identity theft occurs when someone steals our identity and pretends to be us to access resources such as credit cards, bank accounts and other benefits in our name. The imposter may also use our identity to commit other crimes. “Credit card fraud” is a wide ranging term for crimes involving identity theft where the criminal uses our credit card to fund his transactions. Credit card fraud is identity theft in its simplest form. The most common case of credit card fraud is our pre-approved card falling into someone else’s hands.

He can use it to buy anything until report to the authorities and get card blocked. The only security measure on credit card purchases is the signature on the receipt but that can very easily be forged. However, in some countries the merchant may even ask us for an ID or a PIN. Some credit card companies have software to estimate the probability of fraud. If an unusually large transaction is made, the issuer may even call us to verify.

Often people forget to collect their copy of the credit card receipt after eating at restaurants or elsewhere when they pay by credit card. These receipts have credit card number and signature for anyone to see and use. With only this information, someone can make purchases online or by phone. We won’t notice it until we get our monthly statement.

4.3.11 Salami Slicing Attack

A “salami slicing attack” or “salami fraud” is a technique by which cyber-criminals steal money or resources a bit at a time so that there’s no noticeable difference in overall size. The perpetrator gets away with these little pieces from a large number of resources and thus accumulates a considerable amount over a period of time. The essence of this method is the failure to detect the misappropriation. The most classic approach is “collect-the-round off” technique. Most calculations are carried out in a particular currency are rounded off up to the nearest number about half the time and down the rest of the time. If a programmer decides to collect these excess fractions of rupees to a separate account, no net loss to the system seems apparent. This is done by carefully transferring the funds into the perpetrator’s account.

Attackers insert a program into the system to automatically carry out the task. Logic bombs may also be employed by unsatisfied greedy employees who exploit their know-how of the network and/or privileged access to the system. In this technique, the criminal programs the arithmetic calculators to automatically modify data, such as in interest calculations.

Stealing money electronically is the most common use of the salami slicing technique, but it's not restricted to money laundering. The salami technique can also be applied to gather little bits of information over a period of time to deduce an overall picture of an organization. This act of distributed information gathering may be against an individual or an organization. Data can be collected from web sites, advertisements, documents collected from trash cans, and the like, gradually building up a whole database of factual intelligence about the target.

4.3.12 Software Piracy

Thanks to the internet and torrents, we can find almost any movie, software or song from any origin for free. Internet piracy is an integral part of our lives which knowingly or unknowingly we all contribute to. This way, the profits of the resource developers are being cut down. It's not just about using someone else's intellectual property illegally but also passing it on to friends further reducing the revenue they deserve.

Software piracy is the unauthorized use and distribution of computer software. Software developers work hard to develop these programs and piracy curbs their ability to generate enough revenue to sustain application development. This affects the whole global economy as funds are relayed from other sectors which results in less investment in marketing and research. The following constitute software piracy:

i. Loading unlicensed software on your PC

ii. Using single-licensed software on multiple computers

iii. Using a key generator to circumvent copy protection (McQuade, 2006)

iv. Distributing a licensed or unlicensed ("cracked") version of software over the internet and offline

4.4 Trend of Cyber crime in Nepal

The frequency of news for Consultation with the cyber crime division of Nepal police revealed that the Social media, mostly Face book, related crimes are in rise in the current period. Most of the time, the perpetrators are in search of the novice users who are very enthusiastic for making friends in the social media and who are very unaware about the privacy issue of the social media. They easily fall prey to the perpetrators. Blackmailing for the purpose of ransom or sexual abuse are rise in the present context. The discussion also revealed that the victims are Female of young age most of the time. According to the data of the Crime Division of Nepal Police the trend of Social Site crime is in increase. The data of total reported social media related crime in Crime investigation Bureau and crime investigation Department of Nepal Police are given below in table .

TABLE 1

Total Reported Cases in Nepal Police Crime Investigation Division

Cases	073/074	074/075	075/076 (Till Mangsir)
Social Network	22	50	61
Illigal Data Access	1	0	0
ATM	1	0	2
Hacking	1	2	3
SMS Threat	1	11	20
SMS Lottery Fraud	0	3	4
Copy Right	0	0	0
Youtube	0	1	3
Total	26	67	93

Source: Nepal Police, Crime Investigation Division

TABLE 3

Total Reported Cases in Nepal Police Crime Investigation Bureau

Cases	**073/074**	**074/075**	**075/076 (Till mangsir)**
Social Site (Facebook) Issue	28	51	50
Internet/Computer Fraud	6	-	1
E-mail Forensics	-	2	-
ATM Issue	3	-	-
VSA Report	13	11	9
Website Issue	1	-	-
Unauthorized Access	1	-	2
Publication of Illegal Material in Electronic Form	1	-	-
Data Retrieval	2	5	-
Others: Missing Person located through social media /	2	1	3
Total	57	70	65

Source: Nepal Police, CIB

Above mentioned tables show that the trends of cyber crimes in Nepal are increasing day by day. Total cases registered in Nepal police were 93 in fiscal year 2073/074. Likewise there were 134 cases registered in FY 074/ 075. Similarly, 158 cases were registered in FY 075/076 (till Mangsir).

In total, numbers of filed cases have shown that the trend of cyber crime has increasing frequently in Nepal which is shown in below graph.

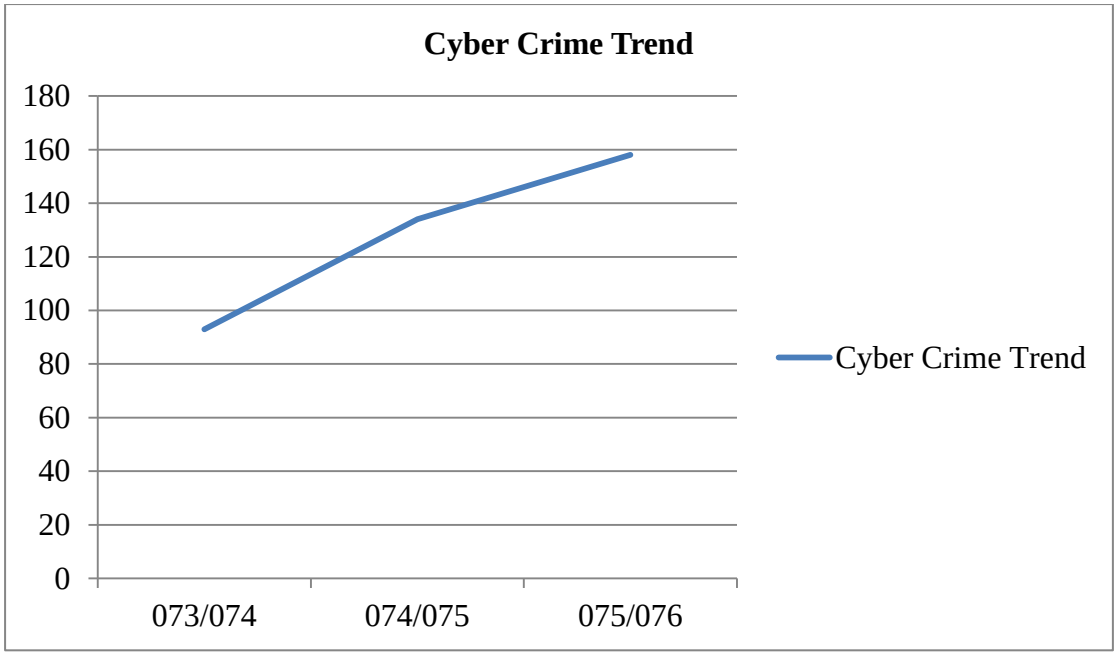

Figure: 3

Source: Nepal Police CID & CIB

In total, social media related cases were increased per Fiscal Year which has shown in below chart.

Rate of cyber crime registered in Nepal Police (from FY 072/073 to FY 074/075)

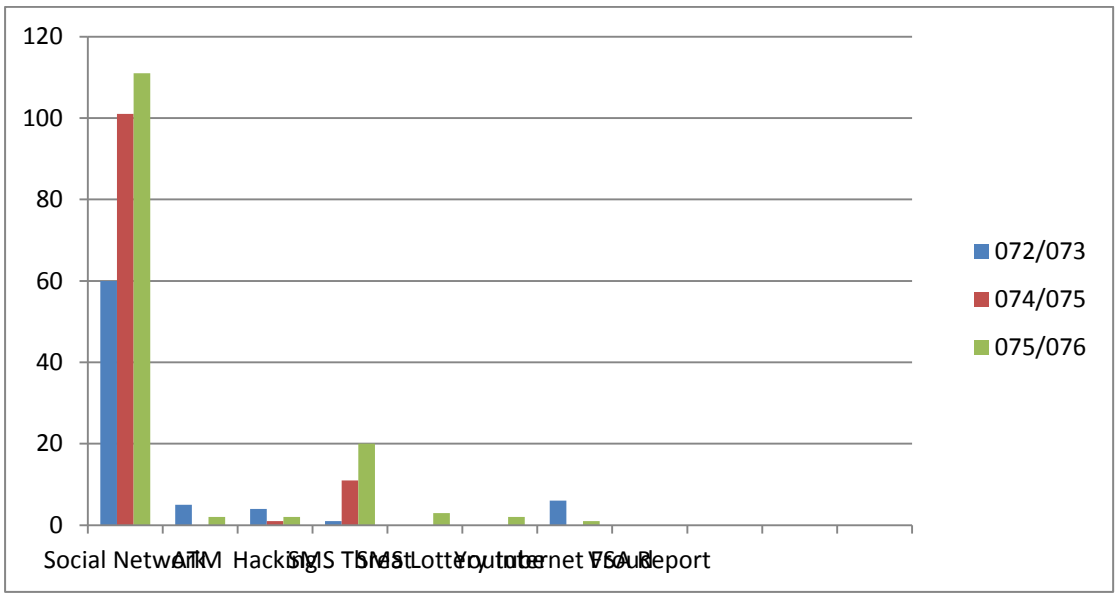

Figure 2: Rate of cyber crime registered in Nepal Police

Source: Nepal Police Crime Investigation Department

According to the DYSP pashupati Ray, Cyber crime Branch, Central Investigation Bureau, there are a lot of causes related to the cyber crime which are not registered in police record. Because there are only two authentic offices which look after the cases of cyber crime and they are located in Kathmandu. The cases in district, either that are settle without registered or send to CIB or CID. Due to the lengthy process to investigate, victims are not wanted to register the case. This is also assist to happened cyber crime.

The search engines are the ones which make out job easier. It does same to some fanatic, curious and criminal minded chap by fetching ways and tricks to crack face book passwords. When somebody tries to know how to crack the face book password in any search engine it is overwhelmed by the tricks and methods. Different sites are serving for this. Thus, it makes easy for any novice person to enter into other's account. Similarly in Nepal, it is common for the persons to download others image, create a fake profile on the name of the person who he/she try to defame and post sexually explicit material on that account. This type of crime is very difficult to investigate and bring the culprit to the proper justice (Ray, 2019).

In another instance, the email or SMS Lottery frauds are in rise since about years. The officer who is looking after these issues said that these issues are very difficult to investigate and control. The criminals use various tactics to get money from the victims. They have even started to call in various languages (Hindi and English) which make the targets to believe that they are the winners of the Lottery Program. Similarly, some are being fraud by the fraudulent activities in the name of gifts from abroad. Some criminals have even taken money from the victims in the name of clearing taxes in the Indian Custom for the valuable gifts they have sent. It is found that for this activity the money exchanges of the bordering town of India have been used.

Secondly, most of the Nepalese people they don't have knowledge about the cyber crime. For this first a survey about the knowledge of cyber crime among the people of Bharatpur 02, Chitwan along with Balkumari Secondary School's students with some questionnaires (Which are mentioned in appendix) were taken which includes both victim and non victim people. Random questions about cyber crime were asked to least 10 people in the locality. Among them half of the people were unaware about

the cyber crime i.e 5 out of 10. Even they were unknown about social media related crimes. Besides that some of educated people 3 out of 10 were quite aware about the cyber crime which is trending nowadays as compared to past. They mostly knew about social media related crimes, piracy related crime for instance copying someone code to make duplicate one and also fake website marketing. The satisfaction level of these people towards the Nepal police was almost low.

On the other hand a set of questions was asked to one of the victim person who was a higher secondary level student. The case was fake profile (facebook) that is related to social media crimes .The victim was unknown about the crime before victimized and was unware about how to deal with such issues which create a kind of negative impact in his/her life like spreading unwanted messages to various unknown people. Finally the victim got some advice from his/her friends about reporting in Nepal police who work with close coordination with internet service providers to ensure security and hopefully got out of that issues.

According to the Nepal Police Crime Investigation Department and CIB, there were 111 cases of dishonor through the social media have been registered in fiscal year 2075/076, among which the division has filed the case under Cyber Crime and Public Offence act against nine people (Ray, 2019). Among the whole spectrum of cyber crime in Nepal, financial crimes are yet another problem.

Blackmailing is yet another kind of rising crime in Nepal, according to the Cyber crime cell of metropolitan police. The most vulnerable target to this kind of activity is from young to middle aged girls and women. It is found in many cases that the criminal would start affair with the target and gain so much trust that the target is ready to project herself nude in the live video chatting. These kinds of videos would be recorded by the criminals and use it to blackmail the target for money or sexual abuse. Concerned authority states that such kinds of incidents are happening more and reported less because of fear of losing reputation. There are some instances which are related to that crime.

The social network's romance is not limited to linking relationships and love sharing with its thread. It has been so tasty to have a relationship with unrecognized friends using social networks, stirring love by stirring out a thread of interrupted

conversations. However, the tragedy of eradicating sexual hunger is also increasing in the Nepali society by giving physical torture and handling the image of the secret creating obstructive circumstances (Ray, 2019).

Some teenagers have shown courage to register a complaint of Cyber Crime against the use of a secret adventure as a weapon. Uniquely, various complaints registered in such cases have been transformed as a cyber crime. Most of the victims registered with cyber crime appear to be under 18 years of age. Because of Nepali social perception and practices very less in number of such cases which are prone to personal public image are being formally filed (Malla, 2019). Criminal Code, Article 18 has established clear provision of imprisonment in the case of sexual intercourse either in consent of victim or not for 10 to 12 years (Criminal (code) Act, 2017).

The following are some representative cases filed in Kathmandu Metro Police Station:

Kathmandu police arrested a teenager from Teku on December 5. According to the police, a case on which they have given a code name -26 premises (c) to protect the identity of victim. The research conducted by the investigator, revealed that the psychology of existing generations is deteriorated by virtual relation especially via mobile network and thus the family is being tortured in turn. According to the teenagers arrested, they are being trapped by the results on which they were self engaged with the acts before. This story is a complicated situation in a teenager's life in Kathmandu. A boy named Prabesh Poudel, who was reading Plus 2 in a college of Kathmandu, sent a friend request to a girl from a fake Facebook account and engaged in relation that ultimately translated into physical amusement. On one of the Premier days, they had sexual relations in a hotel of Sundhara. At that time, the teenager with the behavior of the boy came to know that the love was for sexual relations. And more than that, the boy said that he had some secret photos of their relation. Later the relationship between teenagers and girls turned to break up.

Pradeep got a secret sexual intercourse with a teenager and shared this video through a mobile application emo to his another girlfriend [named Rojy as 26 premises (y)] who again mistakenly forwarded to her father’s and relatives’ social account. As soon as the news came out in social media, she felt like a sky fell on her. The girl, who was under mental stress till the day of calamity, took a lot of courage after receiving the

help of friends and family members and filed a complaint in Kathmandu Police on December 15. Police immediately arrested Roji .

The police initially prepared case to file under Electronic Transaction Act 2063 but after confirming that the girl under the age of 18, therefore filed under Juvenile Act 2075. The offender Pradeep allegedly involved in taking the pictures of the victim having permanent address of Tanahun is absconding with teenage videos and photographs, and the police is in search of him. This incident does not show just how the love developed from the social network is going to be an accident; it is also believed that using social network is being abused as an abusive force. Surprisingly, there is also a growing trend of teenager than above (Sapkota, 2019).

According to Journalist Janak Raj Sapkota Sub-editor at Kantipur Publications Nepal others incident registered in the police station in Poush are more remarkable. It is mentioned in the report filed by a teenager reading in Class 11, how the relation between twisted as a crime. The girl was requested to add Vimal Raut unknown for her as a friend on Jestha in Face book. She added him without any hesistation. The relationship started with the conversation, and in the last year, she met Vimal at Palung of Makwanpur, her own village. One day after that meeting, Bimal called him at Shikhar peak, nearby Palung, had a physical relation in the nearby forest. After such a relationship, they became more intimate. On the other hand, while making a conversation with the video call, Vimal took a shower, saying, "Open the cloth and show me the secret organs." finally she did which one turned into a blunder for her life. Than Bimal recorded her naked showering video and with that he repeatedly exploited sexual assault by showing that secret video. After months of mourning, Bimal kept on threatening to her to publicize that video and photos to social networks. Bimal sent the secret video and photo to teenager's sister and relative's via Facebook address.

Police arrested Bimal Raut at Birendra Chowk on August 1. 2018 after receiving the complaint of such a tragedy of the teenager. During the statement, Bimal accused that she had relationship with other person and not answering his call and further said that her nude photo and video then he sent to her sister and relatives. Bimal's statement explains how adolescent teenagers are getting rid of the relationship of social relations, and what crime is being done by impulsion-making decisions.

According to the police officer investigating the issue, the photographs of sexual activity in social network which actually starts in consent being in affair that later abused by a partner is a current tendency of of cyber crime related to teenagers.

Another incident registered in Kathmandu, a teenager girl reading in Suryabinak, Bhaktapur municipality at grade 10. A boy named Susbas Thapa was known as football player became friends that turned into love and sexual relations. He further threatened her to have the intercourse but when she denied threatened to publicize her sexual video.

When a teenager started to get away from the drought, she started to receive a lot of mental torture from the boy. One day, the video of her secret time came to the Facebook. The teenager made a complaint on which both Raut and Subash were charged as offender. Police arrested Subash from the Emadol of Lalitpur on December 9. The police statement said that the girl has a relationship with the teenager and claimed to be sexually conservative. In this incident, the victim demanded that boys should be punished under electronic transaction Act. On the basis of sexual intercourse, the age of teenager was 15 years 11 months and 28 days.

Sushil adhikari, who was working as a child psychologist working in Baal Ejalas, Lalitpur district court, said that the problem is in height because of disintegration of joint family structure and teenagers growing in single family are getting frustrated. Based on his experience, he said, 'Parents have not been able to spend time, seems bitter in social harmony".

The opinion of Psychologist Nagendra Thagunna is not different than officials. He said that abuse of social networking is not new these days. Dr. Nagendra's explanation about the change in hormones in teenage age and insufficient knowledge is the basic cause of such happenings. He said that such incident is happening in the tragedy that is not monitored by the social community. The change in hormones in these age has made them bacterial, curious, and risky (Sapkota, 2019).

Sapkota (2019) further added that the married women are also victimized by cyber crime. In the case of cyber crime registered in Nepal, a crime story of sexual abuse and assault account remarkable. In such cases both teenagers and married are engaged. For instances a woman from a Yadav caste of Naxal met with Rajiv Kumar

Karna at Naxal and made friend in Facebook. At the same time Rajeev suddenly strangled her and took pictures. The man then started to threaten her to go to the bathroom in night. She denied that made Rajiv aggressive and threatened publicize those in social networks or to pay Rs 12 thousand.

One day her husband and son also came to know about their sexual relations. Then the women reached to the Metropolitan Police with the help of her husband. The District Police Office Dhanusha on the request of Metro Police arrested Rajiv. The victim filed the case against the accused charging defaming her character through the social network.

Another case of a women whose husband had business in Kathmandu and she was living in Jhapa alone. At that time her brother-in-law came home and requested for sexual intercourse with her and she agreed but when he frequently asked for she denied. In return he threatened to make all those secret publicly she afraid and get back to her husband in Kathamandu. The man followed to her. Here too he asked for the same. In the police station, she had told that he again threatened to publicize pornography and kill her husband and son. After this incident, the women reached the police with the help of her husband. According to the police statement, the man himself uploaded those pornography from Social Network. In this incident, the police have also registered a case under both the attempt of rape and the Electricity Law Act (Sapkota, 2019).

There are several types of cyber crime going on in Nepal at the present context. Among them the social media related crimes are at rise and being uncontrollable day by day.

These are happening due to the unawareness in the internet/social media users or limited ability of the concerned authority to address the problem. It is believed that there are many more cases which are being unreported because of unawareness or fear of losing the prestige.

Therefore cyber crime especially victimize girl and women is increasing day by day. To control such activities, there is also a need for further social debate regarding such incident that is being continued through the misuse of social networking.

4.5 Common type of cyber crime in Nepal

4.5.1 Social Media Related Cyber Crime

Social Media related cyber crime in Nepal includes using Porn Content in social Media or creating fake profiles to intentionally harm someone with the use of Facebook, Twitter, Instagram or any social Media Platform. In the year 075076, a total of 111 cases of Social Media Cyber crimes were reported. With the trending use of Social Media, the number of cases has increased to 100 in 2074/075. It has been seen that the number of female victims is more. Using Naked Pictures in social Media to take revenge has been the most cases in Nepal.

4.5.2 Piracy Related crime

Any Content which has been copied to make a duplicate copy is considered as Piracy. Using unauthorized trademarks and copying source code without having the License to use it is considered Piracy Crime.

Example, the font used in Company logos can also be related to piracy crime, if the font is not listed free for business purposes. Even though this related crime is not a possibility in today's context of Nepal, but we can see a various example of Font piracy. Read a story of Font Piracy. Also, Source Code piracy case have been heard in Nepal lately.

Since the case has not been solved, the whole story is an unsolved mystery. It has been allegedly reported that a software company filed a case against a Media House for copying their source code.

4.5.3 Fake Profile Marketing

Creating or using a fake profile, fake website or email to create a bad image or inappropriate marketing is also considered as cyber crime. We can see various examples of fake profiles, fake websites, and spam emails. Spreading unwanted and inappropriate message using fake profile is considered a Fake Profile Marketing. This rule also implies to businesses where a fake product is sold. Marketing of fake duplicate product using the name of a different brand also comes under the Fake Marketing Cyber Crime.

4.5.4 Threatening Using Email

Email threat is not much common cyber crime in Nepal. If an email contains a threat or warning in mentality to harm or disturb any individual or any organisation, this is considered as a cyber crime.

4.5.5 Website Hacking

Website Hacking means taking control from the website owner to a person who hacks the website. Nowadays most of the government websites are attacked by hackers. Many governmental websites including the president's website were hacked.

Any complaint on website hacking can be a serious offence in terms of the cyber law in Nepal. Recently, a group of Nepalese hacker named Anonymous opnep breached into the server of Nepal Telecom.

Hackers gained access to all the details of NTC users that include username, citizenship name, father's name as well as other private information. Metropolitan Crime Division recently tracked the hackers down and arrested 18-year-old Bikash Paudel for hacking over 200 websites including the NTC website (Ray, 2019).

4.5.6 Unauthorized Access

Unauthorized access is one of the common issues in cyber crime world. Getting access to a website, programme, server, service, or other system using someone else's account or other methods is called Unauthorized Access. This type of cyber crime also likely to be increased in Nepal. Examples of the unauthorized use of computers include an employee using a company computer to send a personal e-mail or someone gaining access to a bank computer and performing an unauthorized transfer.

4.5.7 Online Business of Restricted Materials

The business involving the buying and selling of illegal or restricted materials can be a case of cyber crime. One interesting case had come up when a Nepali citizen named Kirtan Pokhrel was arrested for creating an event related to sexual tourism. The Event was named Bunga Bunga which promised to have girls of ages 13 to 17 (Bhattarai, 2017).

4.6 Actions taken so far to Mitigate Cyber Crime in Nepal

4.6.1 General

As Nepal is a late starter in the arena of cyber space it has also introduced its cyber security act lately. However, it seems that it has not caught up the pace of the development of cyber related software as well as hardware. In this chapter the endeavors of Government of Nepal to mitigate the lapses in the sector of cyber security and electronic transaction will be discussed.

In this era of information technology, people think internet as their basic rights. In the last few years, use of internet and computer is rapidly climbing up. According to the Nepal Telecom Authority, internet users has reached about 16.67 millon and internet penetration is 64 percentage in Nepal till 2018. However, along with the massive use of the internet, a new means for crime or terrorism has also evolved. The cyber crimes in Nepal are rising as the Internet becomes more common place for common people. According to the Metropolitan Police Crime Division, which handles cases of cyber crime, bringing the guilty to book is next to impossible for the police unless a victim categorically identifies the suspect.

The data presented by the Metropolitan Police Crime Division does not reveal actual status of the cyber crime in Nepal because most of the issues are not reported may be due to lack of awareness that they have become victims. Those who realize what has happened are often undecided to lodge a complaint, mainly, due to ignorance of existing laws and regulations or because of fear of getting insulted in the society.

4.6.2 Nepalese Legal Regime Governing Cyber crime

Cyber law is the law that includes a variety of issues related to the internet and other communication technology, including intellectual property, privacy, freedom of expression, and jurisdiction. The Cyber law governs the legal issues of cyberspace. Cyberspace is the electronic medium of computer networks, in which online communication takes place. Cyberspace is a very wide term that includes: computers, computer networks, the Internet data software etc.

Cyber laws are very important. They provide security to not only the intellectual property of IT companies but also helps to maintain the privacy of the internet users. They check the programs of corporate to make the internet a neutral platform, help to create standard models of use which helps to create tailored facilities to the citizens in order to boost the economy, and so on. There are so many laws in Nepal which related to control cyber crime.

4.6.2.1 Electronic Transaction Act, 2008

There was no separate and independent law related to computer crimes prior to the enactment of the Electronic Transaction Act, 2008 (hereinafter referred to as 'ETA') and all the computer related crimes were tried under the traditional law of crimes, i.e. Country Code and sector specified criminal laws. Because of increasing use of computer in commission of different crimes and commission of crime against computer, it posed practical problem for the regulating agencies to regulate cyberspace transaction of citizens. ETA was promulgated by parliament of Nepal recognizing the expediency to make, legal provision for authentication and regularization of the recognition, validity, integrity and reliability of generation, production, processing, storage, communication and transmission system of electronic records by making the transactions to be carried out by means of electronic data exchange or by any other means of electronic communications, reliable and secured.45 Furthermore, the act was promulgated for controlling the acts of unauthorized use of electronic records or of making alternation in such records through the illegal manner(Electronic Transaction Act, 2008)

Under definition clause of the act , certain terminology related to cyber crime has been defined which includes definition of computer, computer database, computer network, data, access, electronic record, computer accessory and so on. Major part of ETA governs provision related to electronic record and digital signature, controller and certifying authority, digital signatures and certificates, subscriber's duties and rights, government use of digital signature, network service and constitution of tribunals. However, chapter 9 under ETA explicitly provides provision related to offence relating to computer (Electronic Transaction Act, 2008).

Broadly, ETA has criminalized eleven types of act as cyber crime where the act has mixed the offences related to computer and offence related in obtaining certification license for digital signature under the same heading of 'offence related to computer'. In context of this dissertation, the crime that has been included as cyber crime are : to pirate, destroy or alter computer source code, unauthorized access in computer materials, to damage to any computer and information system, publication of illegal materials in electronic form, to disclose confidentiality, to commit computer fraud, abetment to commit computer related offence and accomplice of offence.

In more detail, section 44 of ETA has criminalized the act of piracy, destruction or alteration of computer source code. If any person knowingly or with mala fide intention, pirates, destroys, alters computer source code to be used for any computer, computer program, computer system or computer network or cause, other to do so, shall be liable with punishment with imprisonment not exceeding three years or with a fine not exceeding two hundred thousand rupees or with both. Clarification of the section 44 has provided that 'computer source code' means the listing of programs, computer command, computer design and layout and program analysis of the computer resources in any form.

Section 45 of ETA has criminalized the act of unauthorized access in computer material. If any person with an intention to have access in any program, information or data of any computer, uses such a computer without authorization of the owner of or the person responsible for such computer or even in the case of authorization, performs any act with an intention to have access in any program, information or data contrary to from such authorization, such a person shall be liable to the punishment with the fine not exceeding two hundred thousand rupees or with imprisonment not exceeding three years or with both depending on the seriousness of the offence.

Section 46 has criminalized the act of damaging any computer and information system. If any person knowingly and with a mala fide intention to cause wrongful loss or damage to any institution destroys, damages, deletes, alters, disrupts any information of any computer source by any means or diminishes value and utility of such information or affects it injuriously or causes any person to carry out such an act, such a person shall be liable to the punishment with the fine not exceeding two thousand rupees and with imprisonment not exceeding three years or with both.

Section 47 has criminalized the act of publication of illegal materials in electronic form. Although constitution of Nepal has guaranteed freedom of expression, 58 ETA limits the freedom of expression. Pursuant to ETA, if any person publishes or displays any material in the electronic media including computer, internet which are prohibited to publish or display by the prevailing law or which may be contrary to the public morality or decent behaviour or any types of materials which may spread hate or jealousy against anyone or which may jeopardize the harmonious relations subsisting among the people of various castes, tribes and communities shall be liable to the punishment with the fine not exceeding one hundred thousand rupees or with the imprisonment not exceeding five years or with both.

Section 48 has criminalized the act of disclosure of confidentiality. If any person who has an access in any record, book, register, correspondence, information, documents or any other material under the authority divulges or causes to divulge confidentiality of such to any unauthorized person, he/she shall be liable to the punishment with a fine not exceeding ten thousand rupees or with imprisonment not exceeding two years or with both, depending on the degree of offence.

Section 52 of ETA has criminalized the act of commission of computer fraud. If any person with an intention to commit any fraud or any other illegal act, creates, publishes […] of acquires benefit from the payment of any bill, balance amount of any one's account, any inventory or ATM card in connivance of or otherwise by committing any fraud, amount of the financial benefit so acquired shall be recovered from the offender and be given to the person concerned and such an offender shall be liable to the punishment with a fine not exceeding one hundred thousand rupees or with an imprisonment not exceeding two years or with both.

Section 53 of ETA has criminalized abetment to commit computer related offence. A person who abets other to commit an offence relating to computer under the act or who attempts or is involved in the conspiracy to commit such an offence shall be liable to the punishment with a fine not exceeding fifty thousand rupees or with imprisonment not exceeding six months or with both, depending on the degree of the offence. Section 54 of the ETA has criminalized punishment to the accomplice. A person who assists other to commit any offence under the act or acts as accomplice,

by any means shall be liable to one half of the punishment for which the principal is liable.

Furthermore, the act stipulated extra-territorial jurisdiction in case of cyber crime. If any person commits any act which constitutes offence under the act and which involves the computer, computer system or network system located in Nepal, even though such an act is committed while residing outside Nepal, a case may be filed against such a person and shall be punished accordingly. Furthermore, for the offence committed by a corporate person, such an offence shall be deemed to have been committed by a person who was responsible as chief for the operation of the corporate body at the time of committing such an offence. However, if the person acting as chief proves that such an offence was committed without his/her knowledge or that he/she has exercised all reasonable efforts to prevent such and offence, he/she shall not be liable to the guilty. The act under cyber crime may also deem to be criminalized under other laws. If any act deemed to be an offence under ETA and also deemed to be offence under the other laws prevailing, it shall not be deemed to have been hindered by ETA to file a separate case and punish accordingly67 -- for example the online defamation can be tied under laws for defamation, online prostitution can be filed under laws prohibiting prostitution, online gambling under laws prohibiting gambling in Nepal and so on.

4.6.2.2 Banking Offence and Punishment Act, 2008

Banking Offence and Punishment Act, 2008 is the law governing banking operation and transaction. Section 6 of the act has prohibited obtaining or making payment by way of abuse or unauthorized use of a credit card, debit card, automated teller machine (ATM) card or other electronic means. The person committing this crime shall be punished with recovery of amount and punishment up to five years depending on the amount of money (Banking Offence and Punishment Act, 2008).

4.6.2.3 Children's Act 1992

Children's Act, 1992, promulgated to protect and promote children's rights, to far extent has addressed the prohibition of child pornography broadly. Section 16(2) of the act prohibits making photograph of child for the purpose of engaging a child in immoral profession. Section 16(3) prohibits publication, exhibition or distribution of

photograph or personal events or description of a child tarnishing the character of such child. Section 53 of the act provides punishment for the person committing such crime including seizure of the photograph and reasonable compensation to children for adverse effect on character of child (Children act, 1992).

4.6.2.4 Copyright Act, 2002

Copyright Act, 2002 has addressed the crime related to copyright where the act has protected copyright of expression of ideas including computer program.

The act has also stipulated punishment for breach of copyright protection such as reproduction of copies of work, advertise or publicize by copying a work belonging to another person with a motive of taking advantage of reputation gained by that work, make work of other by changing the form and language of work with motive of deriving economic benefit, to import/produce/rent any equipment or device prepared with intention of circumventing any device and other act related with infringement of copyright. Furthermore, the act has prohibited importation of copies of work or sound recording, either made in a foreign country or sourced otherwise, into Nepal for business purpose shall not be permitted if preparation of such copies would be considered illegal if they were prepared in Nepal. The act has prescribed punishment to perpetrator with monetary fine, imprisonment and compensation (Copyright Act, 2002)

4.6.3 Initiation to Establishment of Cyber crime Bureau

In the present, the Central Investigation Bureau(CIB) and MPCD(Metropolitan Police Crime Division) of Nepal Police works on the cases of cyber crime. The recent cyber crimes unveil the weakness of the country's cyberspace. According to a reliable source in Nepal Police, an effective cyber bureau is going to be established to deal with the cyber crimes.

The groundwork for which has already been laid out. The bureau also plans to work with internet service providers to ensure cyber security. With this, the bureau plans to secure the cyberspace and enhance awareness among users of malware infection (Sapkota, 2017).

4.6.4 Awareness Program

Due to the rising of cyber crime in Nepal, various agencies have been involving in awareness programs to make aware the Nepalese people especially to women and children.

The main agency in the field of cyber security is ICT FRAME which has been conducting various awareness program in Nepal. Firstly, the concept of Cyber Security Awareness in Nepal has been conceptualized by Prof. Dr. Ramhari Subedi who lives in Washington DC and also he is the founder president of dcnepal dot com and the first appointed Cyber Security Advisory of Central Department of Nepal Police. The organization has been launching its awareness campaign nationwide as well as it has been conducting the program internationally. The program has been conducted in Kathmandu, Jhapa, Chitwan and Tanahau (Aryal, 2017).

Likewise, Government of Nepal, Department of Information Technology has been conducting various training related to cyber crime and cyber security awareness to the government employees. As per the official website of department, every fiscal year the T, R & d section of department is providing at least 15 training program from IT, security and management related discipline in order to strengthen their skill at work place .

Similarly, to alert from different banking risk, on June 12, 2018, Nepal Bankers' Association, in coordination with Microsoft, organized a program on "Perils of Cyber Crime". Representatives from Nepal Rastra Bank and CEOs, along with senior management from the member banks were invited to the program. The event was chaired by Mr. Chinta Mani Siwakoti, Deputy Governor, Nepal Rastra Bank. Program was focused to raise awareness by stressing IT related risks including rising cases of cyber crime ("Perils of Cyber Crime," 2018).

4.7 Problems and Challenges to control Cyber crime in Nepal

The estimated number of internet users in the early years of the twenty-first century is over a billion. In this global village, consumers, companies, and governments from around the world must further develop ways to protect the sensitive personal and business information and detect those, whether Nepal or abroad, that conspire to

exploit technology for criminal gain. Most of the developing countries like Nepal have limitations in access to information and the available access is not affordable because of the inadequacy of the existing infrastructure as well as the non-availability of appropriate education. The challenges are posed by the lack of an integrated computer security system and education about computer security. Here are some points which focus the problem and challenges of Nepal to control cyber crime.

4.7.1 **Inadequate legislation**

Of course the Government of Nepal has felt the need of proper legislation on the cyber matter and has enacted some rules to codify the scope of cyber, however it seems inadequate. Nepal government started its milestone journey in IT development in 2063 BS.

The existing legislation is inadequate in many ways. Some of the most common forms of cyber crime are not covered by the law. For example, no punishment exists for sending offensive messages, which is very common in Nepal. Cyber-squatting, or purchasing domain names to benefit from another's trademark or brand, does not come under Nepal's cyber-laws. Similarly, phishing, or the act of electronically obtaining private information for financial or personal benefit, lacks legal coverage. This endangers every Nepalese internet users, as internet fraud can take the form of deceptive messages for personal and financial benefit (Panta, 2017).

Regarding the publication of illegal materials in the electronic form the Act article 47 (1) does have addressed the matters against "public morality and decent behavior" but it can be defined in many ways. In the present context people are disregarding other's dignity which is considered as the fundamental right of every citizen.

As far as dignity is concerned, many a times a question is raised in terms of defaming of the politicians as well as public figures in the social sites. Of course it is a matter of concern however it is common understanding in the public that public figures basically, politicians are their chosen objects whom they have right to correct through any means. Hence, mocking them in the social sites are not considered as illegal.

The present legal framework also does not cover cyber crimes like cyber-stalking, cyber-terrorism and child pornography. Child pornography, given its propensity to

proliferate through the internet, must be specially addressed through specific provisions regarding Nepal's commitment to international conventions on children rights (Panta, 2017).

4.7.2 Weak Enforcement

The biggest hindrance to cyber crime prosecution in Nepal is weak law enforcement. Even with the media reporting on a rise in the number of cyber crimes, the official response has been slow and dull (Panta, 2017). Although the present Act does touch on a few important issues, the enforcement part is minimal because of several reasons which are discussed in the subsequent paragraphs.

Firstly, both the police and judiciary have not developed sophisticated tools to investigate cyber crimes. At present, there are only two units that deal with cyber crimes and they are Cyber crime Investigation Cell, under Metropolitan Police Crime Division, at Teku Kathmandu is responsible for the investigation on the reports inside Kathmandu Valley and the Central Investigation Bureau (CIB) at Maharajgunj are responsible for the investigation of the reports outside the valley. Both of them are under strength. The infrastructure of the metropolitan crime division is so pitiful that it is clearly visible that the government has not paid proper attention to them. With such sub-standard infrastructure, which is psychologically very uncomfortable, one cannot and should not expect more from these investigators. Similarly, they prioritize the reports and are focused on some big issues. Because of this small cases of defamation get overshadowed.

On the other hand, these branches also do not have any sophisticated tool to investigate the cyber offences. The detailed staffs use their intelligence quotient to follow the chain to reach up to the offender and bring him/her to the jurisdiction of legislation. It was also discovered during the visit to the cell that the same persons are responsible to arrest the offenders which demands more staffs. In such situation the cell has only two to three persons to investigate the other issues. Paradoxically, even when cyber crime cell discovers a fake Facebook account, it can only block the account because Nepali law does not allow access to a user's IP address.

It has been recognized that electronic transaction within Nepal are not secure. Hence, Nepal government introduced electronic Transaction Act 2008. Some of the Nepal

Police units are undergoing investigation and law enforcement activities. Although it has filled the void space of unchecked electronic transaction law but some lapses exists. It is felt that there are still some gaps from where the breaches are happening. Basically, this legislation has not addressed the social media which is widely in use in the Nepalese electronic spectrum.

On the other hand, the enforcement part seems weak. Nepal Police is the only institution which is looking after the breaches without any technical manpower. With the ordinary human resources, available normal physical resources and that even understaffed are hindering the investigation and law enforcement part. On top of that every report does not get attention because of lack of resources.

4.7.3 Inadequate attention

Proper attention by parents is also a very good way to control the internet use by the children. Parental guidance in our atmosphere is comparatively less specially in use of internet either because of lack of knowledge or ignorance or negligence or may be due to high level of trust in their children. However, this seems to be very less in Nepal. In many cases this has created problem. The children are so free that they easily break social norms just for fun or adventure. Hence, parental attention is very inadequate.

4.7.4 Poor Authentication

In Nepal, most of the cyber crimes are related with social media. Most of the cyber crime cases are happen due to lack of poor authentication like easy password. Nepal has low literacy rate. Other important things are most of the social media users are from the poor academic background. They have no good knowledge about the cyber crime, its effects and how it happens. Most of the users use simple passwords in their account such as their name, their lover/beloved's name, own mobile number, etc. Most of the users have no knowledge about the use of symbols in their passwords such as the mix up of symbols like &, $, %, @, etc. By using the password hacker software the users can easily hack the password of others if they are using only alphabet or alphanumeric. But it is almost impossible to hack such a password that has the mix up of the alphabet, numbers and symbols. For example "nEp&l" is thousands time more secure than the password "nepal".

So due to the use of poor authentication, another users can easily hack or guess the password and misuse others resources. In most of the cyber crime cases of Nepal, it happens when the users have simple passwords. The criminals are using others' accounts by hacking or using fake accounts. In the case of Nepal, mostly the users are careless about their accounts. In other cases, some criminals have no results of their own work also. They are doing unethical things, but they are not aware of what they do whether it is ethical or not. In most of the cases after arresting by police or complaining by the victims, they realize that what they have done is unethical (Ray, 2019).

4.7.5 Lack of sufficient awareness Program

According to the Nepal Telecom Authority, internet users has reached about 16.67 million and internet penetration is 64 percentage in Nepal till 2018. However, along with the massive use of the internet, cyber security awareness programs are not sufficient. Various agencies they have been conducting cyber awareness programs only in city area. But in the village or remote area people who are illiterate also, have not access to get cyber security knowledge.

4.8 Outcomes

The major outcomes of this research are:-

1. Cyber technology has emerged as an invariable feature of modern life as individuals all over the globe interact with one another through cyberspace.

2. Social sites have become a medium to open up the dissatisfaction and the bitterness of mind by which anyone can harm anybody by defaming or assassinating the character which cannot be traced or tracked easily.

3. The rate of reported cyber crime, specially related to defamation through social site is increasing day by day in Nepal.

4. Although Government of Nepal has introduced Electronic Transaction Act, 2008, its implementation has not gone as expected.

5. The Anti cyber crime cell of Metropolitan Police Division of Nepal Police at Teku and Central Bureau of Investigation at Maharajgunj are dedicated for the

investigation of the breaches of cyber security. However, these cells seems to be severely under strength, under equipped and non-technical apparatus to investigate highly technical matters.

6. The Government of Nepal lacks any special body which is technically competent to look after the cyber space activities.

7. Awareness against the cyber crime has not been effective because of which the numbers of victims are also in increase.

4.9 Some Viable Ways to Control Cyber Crime in Nepal

Taking in concern the frequency and types of security breaches happening in the electronic media, especially, cyber space of Nepal and the existing legal framework and the law enforcement part it is felt that Nepal needs some focused vision for the prevention, investigation and punishment to make the cyber space secured. In this chapter some viable ways to control cyber crime is endeavored to be rectified.

4.9.1 Conduct Awareness Program and Raise Awareness

Awareness is the key to prevent any cyber crime. In the western world, almost all the countries seem to have focused on the awareness program to prevent the cyber crime. It is better to immunize rather than cure. To investigate and punish the number of breaches is costly in terms of men and material than conducting awareness program and prevent the breaches.

Schools in Nepal include computer education from very low level. The foundation of formal education of computer starts from here. It is therefore feasible to introduce the cyber law in the secondary level. At this level and above this the children are most likely to commit crimes in the cyber space. This is the level when the children are susceptible to adventurism. The aggressiveness against anybody can reach a level to retaliation at this level which may turn into defamation of the target, for instance. Another thing is, the knowledge gained at this level last long which may be helpful to reduce the cyber related crimes for a long term.

Similarly, regular advisory to the user of any electronic media is very important. Equally important is to adhere to the advisory.

For instance the Nepali Army mail domain has recently published an advisory mentioning: “Even though some phishing mail attacks like below is a constant threat and can only be protected from continuous Cyber Security Awareness Programs”. A list of do’s and don’ts were following this statement. This is very effective program to make the users immune to any cyber crime.

Last but not the least, people should also be made aware to report any violation of electronic act, may it be social or financial violation and the perpetrators must be brought into legal perimeter so that it can be ushered that there is a rule of law and no violators will be spared. This will bring up resilience in the community which is very essential for any government.

4.9.2 Manage Strong legal Provision

It has become very necessary to see cyber crime as a grave matter of concern. During threat analysis other threats are considered in legal documents, however, cyber crime seems to have got little attention in comparison. In a radio interview with the Spokes Person of Nepal Telecom revealed that the nation has not given adequate attention to prevent cyber crime in Nepal. He stated that the National Security Policy which was promulgated recently, have considered many things about other forms of security but didn’t uttered about cyber security. He has therefore requested the Ministry of Defense to review the Security policy and include the aspects of cyber security in it. Of course, it is very necessary to give attention to Cyber Security from which may be initiated from inside and outside the country.

It is also important to address the social media related policies in The Electronic Transaction Act 2008. Since social media has become the truth of the day, the word “Social Media” should be made visible in the articles of act rather than generalizing by keeping “electronic transaction”. Although it has filled some gaps on this aspect, incompleteness would make it lighter.

4.9.3 Establish a Strong Anti-Cyber Crime Cell

Firstly, the Ministry of Information and Communication (MoIC) in coordination and cooperation with the Ministry of Science and Technology should establish a cell, full of technical staffs, which will be dedicated in research and analysis of the cyber space

which is very essential for the national security of Nepal. This should provide any kind of technical assistance to the security bodies when necessary. This cell should also be active in suggesting the legislature in making and updating the legal policies and provisions. This will certainly enhance national capability in preventing and punishing the security breaches in the realm of cyber space.

Existing cyber crime cell of Metropolitan Police Crime Division and CIB is not adequate for investigation of cyber crimes. The ratio of reports on cyber crime is very high than the number of investigators in proportion. This makes the cell to give little or no attention to many of the cases. On the other hand this cell should be given extra technology and right to access the social site account for investigation. The nation should get reach to the social site manager so that this team can expedite their investigation to perform result oriented tasks. This would work in two ways. First, it would empower the state's legal system to work aggressively and efficiently and second, this would demoralize the criminal which will result in the decrease of such cases.

In the part of human resources, it is suggested that every provincial (as Nepal has entered into the federal system) police must have at least 150 persons strong anti cyber crime unit including Information Technology experts and persons to take action on the ground. This unit must be responsible for the investigation and prosecution of the cases. Similarly, every provincial constitution which will be made in the coming days, must consider cyber security at any corner so that it would be convenient to make suitable act in the provincial level.

CHAPTER V

SUMMARY AND CONCLUSION

5.1 Summary

A Cyber Crime is an act of creating, distributing, altering, stealing, misusing and destroying information through the computer without the use of physical force and against the will or interest of the victim. It can be committed by any person living in one part of the world against another person or institution living in another part of world.

Nepalese society has become dynamic along with the development in new technology. With the increase of computer users, misuse of technology has also increased, which has increased the cyber crimes in Nepal. The frequency of news for Consultation with the cyber crime division of Nepal police revealed that the Social media, mostly Face book, related crimes are in rise in the current period. The exemplary cases which include in previous chapter are some representative cases which is evidence to conclude that there is growing tendency of cyber crime in Nepal and there are different pattern of crime that is occurring in Nepal.

Making an observation of existing pattern and trend of cyber crime in Nepal, threat of cyber crime is still likely to grow in coming years because of certain factors. Firstly, there is increasing business that are potential victims of cyber-crime (such as e-commerce, online banking, online store), secondly there is rise in number of potential perpetrators, thirdly, because of lack of precaution the cyber world is being used by general people, fourthly, the law has not been adequately amended as a need of time, and fourthly, investigation and lack of cyber forensic has diminished the chance of being caught. Compared to last few years, the pattern of cyber crime has been changed today and that will certainly be different in upcoming years.

Now it is to be discussed matter to what degree the present Nepalese legal regime addresses the present or future of cyber crime. Although Nepal has been able to enact the specific cyber crime law, there are some loopholes which have posed as threat for effectively addressing cyber crime in Nepal. Furthermore, lack of awareness in regard to cyber crime is another reason for upgrading it. Victims themselves are not aware of

the laws and compensation that they get in case of being victim of cyber crime. Parents are also not to give proper attention to their child. They are so free that they easily break social norms just for fun or adventure. Besides that Most of the cyber crime cases are happen due to lack of poor authentication like easy password. And have no good knowledge about the cyber crime, its effects and how it happens.

Although, the Anti cyber crime cell of Metropolitan Police Division of Nepal Police at Teku and Central Bureau of Investigation at Maharajgunj are dedicated for the investigation of the breaches of cyber security, these cells seems to be severely under strength, under equipped and non-technical apparatus to investigate highly technical matters. In Nepal, there are only two units which look after the cyber crime in whole part of the country. As discussed earlier the law enforcement agencies have very important role in preventing and punishing. The current strength of police is very less or inadequate. On top of that the investigation is centralized. This makes the police in the district headquarters handicapped. On the other hand the police do not have right to technically interfere in the public accounts neither they have the technical expertise to do so. Hence, the strength of the police should be increased. The technical expertise should be maintained.

The security is not just based on a punitive action or legal base, it should also be able to protect by generating awareness and ability to use the cyberspace securely. It is now quite convincible that the techno savvy newer generation has a good knowledge of being secured themselves however they are also a threat who can hack the accounts of targeted people proficiently. Being specific about the general public, this group is the user. This group should be aware in order to prevent committing cyber crimes or becoming victim. Since the speed of the development in other sector (health, education, etc) and cyber facilities mismatch in our country, general public should least expect the guidance from the part of government as it is coping with a lot of many other problems. So everyone must be aware of their limitation and rights while using the network.

The government of Nepal has a huge role in regulating the cyber sector of Nepal. Of course it is trying hard to provide the internet facilities to maximum population. But is it regulating the users? The present need is to address and regulate the social site uses in the country. As data shown by the MPCD the social site related crimes are in rise.

So in order to regulate this the GoN, more specifically the Ministry of Information and Communication should formulate a very pragmatic policy which will encourage the use of the internet at the same time discourage the misuse.

So, to control cyber crime in Nepal efectively, government should be serious and necessary amendments are required in existing law regarding cyber crime. There should be separate units at least in all provinces of Nepal. Effective and huge awareness programs should be conduct not only in urban area but also in rural area.

5.2 Conclusion

Cyber crime is rising day by day. It is one of the most dangerous social offenses in the world. If cyber users are careful, it can be reduced radically. Most of the cyber crime happens due to poor authenticity. So, users must have a good knowledge of strong password technique. It is more dangerous in developing countries than in developed countries due to the knowledge level of the users. The cases of cyber crime in developing and developed countries are different. Developed countries are facing cyber security issues such as data stolen, but in the developing and under-developed countries the cyber security issues related to personal issues such as misusing social media accounts. In this way, most of the cases are related with poor authenticity, so both users and service providers should be careful of using authentication. Nepal government recently announced the concept of digital signature, but it is not practically implemented till now.

Even if the government of Nepal implemented this digital signature, Nepalese resources are not secure if have not good knowledge about the authenticity security system.

In sum, increasing urbanaization, increasing access of people in information technology, criminal mind set of some people, scarcity of skilled manpower in police and insufficient legal provision are some reasons behind where from such cyber related crimes in Nepal are in increasing trend. And thus has been a subject of headache for regulatory institutions.

These types of crime causing social imbalance and disorders if not timely and adequately addresses through necessary legal arrangements will not leave society and nation unharmed.

Again, if the concerned agencies and the society itself consider it softly the repercussion will horrible as it directly hits in individual and social relation. Therefore, keeping the consequences in mind before will be more wisdom than reacting latter.

Precaution of individuals while using social networking is itself a most effective method that reduce the vulnerability. However, the state role here will be paramount to discourage such illegal and offence against the such people and legal instrument with people's active support will be the effective measure to gauge the cyber crime in Nepal.

REFERANCES

Agustina, J. R. (2012). *Exploring internet crimes and criminal behaviour* (Vol. 6). Retrieved from http://www.cyber crimejournal. com/Augustinabookreview2012julyijcc.pdf

Aryal, M. (2017). Cyber crime prevention program in Nepal. *ICT Frame,* (Security).

Bagyavati, S. (2009).*Social Engineering*. Lech J.Janczewski and Andrew M.Colarik Cyber warefare and cyber terrorism pg: 182

Bhatta, N. (2017). *Cyber warfare: How prepared is Nepal? The Himalayan*. Retrieved from https://thehimalayantimes.com/opinion/cyber-warfare-how-prepared-is-nepal/

Bhattarai, S. (2018). *Types of cyber crime in Nepal*. Gadgetbyte. Retrieved from https://www.gadgetbytenepal.com/5-cyber-crimes-nepal/

Bradley, S. (2015). *Predators on social networks.* Retrive from http://netsecurity.about.com/od/newsandeditoria2/a/socialpredators.htm

Brenner, K. (2015). *Social networking dangers exposed.* http://www.networkworld.com/news/2009/020909-slapped-in-the-facebook-social.html

Broadhurst, R. (2006). *Developments in the global law enforcement of cyber crime* (Vol. 29(3)). Australia: Australian National University. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2089650

Broadhurst, R (2013). *Cyber crime in Asia: Trends and Challenges.* 10.2139/ssrn.2118322.

Banking Offence and Punishment Act, § 6 (2008). Retrieved from https://nrb.org.np/lgd/acts_ordinances/banking%20offence%20and%20punishment%20act.pdf

Cases of cyber crime registered in six month. (2017, February 6). *Rastriya Samachar Samiti*. Retrieved from https://thehimalayantimes.com/nepal/560-cases-cyber crime-registered

Children act, § 16 (1992). Retrieved from http://jafbase.fr/docAsie/Nepal/children-act%20%281%29.pdf

Copyright Act, § 25 (2002). Retrieved from http://www.nepalcopyright.gov.np/downloadfile/The%20Copyright%20Act_1315912777.pdf

Criminal (code) Act, § 18 (2017). Retrieved from http://www.ilo.org/dyn/natlex/natlex4.detail?p_lang=en&p_isn=106060&p_country=NPL&p_count=119&p_classification=01&p_classcount=45

Das, S., & Nayak, T. (2013). *Impact of cyber crime: Issues and challenges.* International Journal of Engineering Science & Technology, 6, 142.

Dhakal, B. (2018). *Situation of cyber crime in Nepal. ICT Frame*. Retrieved from https://ictframe.com/situation-of-cyber crimes-in-nepal-bikalpa-dhakal/

Electronic Transaction Act, Pub. L. No. 27, § 80, 36 (2008). Retrieved from http://www.lawcommission.gov.np/en/?s=2008&post_type=post

Gabrys, E. (2002). *The international dimentions of cyber crime* (Vol. 1). Retrieved from http://dx.doi.org/10.1201/1086/43322.11.4.20020901/38842.4

Ferrera G.R. (2012). *Cyber Law Text and Cases.* India, (Cengage Learning), 3rd Edition, pp. 402.

International Media Network Nepal. *"Cyber Warfare How Prepared is Nepal?*" The Himalayan Times. 5 Jan 2017. Retrieved from https://thehimalayantimes.com/opinion/cyber-warfare-how-prepared-is-nepal/

Leyden,v.(2014). *Social networkers risk losing their identities.* Retrived from http://www.theregister.co.uk/2014/10/04/social_networking_security_survey/

McQuade, S. C. (2006). *Understanding and managing cyber crime*. Boston: Pearson/Allyn and Bacon.

Panta, S.(2017). *Are Current Cyber Policies, Sufficient to Underpin Defensive and Offensive Operations to Achieve Desired Strategic Outcomes?* Higher Command and Management Course , Nepali Sainik War College.

Perils of Cyber Crime. (2018). In *Perils of Cyber Crime*. Kathmandu: Nepal Bankers' Association. Retrieved from http://nepalbankers.com.np/seminar-on-perils-of-cyber-crime/

Phulara, B. D. (2004). *Crime: Tackling cyber crime in Nepal*, In: The Nepal Digest, Newyork, volume XI, issue 1

Reyes, A. (2007). *Cyber crime investigations: Bridging the gaps between security professionals, law enforcement, and prosecutors*. Rockland, MA: Syngress Publishing.

Roka, C. B. (2017). *Cyber crime and security in Nepal: the need for two-factor authentication in social media* (vol. 5). International Journal of Interdisciplinary Stu dies. Retrieved from http://www.crossingtheborder.com.np/epaper/vol5/4.pdf

Ray, P. (2019, January 13). Trend of cyber crime in Nepal [Teliphoned].

Sapkota, j. (2019). Cyber crime trap. *Kantipur Daily*, 1. Retrieved from http://epaper.ekantipur.com/kantipur/2019-01-26/1

Sapkota, S. (2017, October 9). Nepal Police to Establish Cyber Bureau. Retrieved from https://techlekh.com/nepal-police-cyber-bureau/

Sharma, N.P. (2015). *Cyberspace and the Cyber Law.* Kathmandu: Koselee Prakasan

Sheeba, P. (2009).Safety *Issues in Orkut for Girls.* Retrived from http://article.sapub.org/10.5923.j.ijit.20120101.02.html

Subedi,P. (2015). *Cyber crime in Nepal : Assessing Nepalese legal standard for addressing current and prospective modus operandi of cyber crime in Nepal.* Master thesis, University of Oslo.

Thakuri, B. S. (2014). *Status of Cyber Security in Nepal*. MA Thesis, Tribhuban University

Willard, N. (2007). *Social networking: are cyber teens in danger?*. http://www.ivillage.co.uk/parenting/teens/teencon/articles/0,,186632_712646, 00.html

APPENDICS

Appendix 'A'

(Referred to page 7)

Number of Internet users in the Asia Region 2018

Country	Population (2018 Est.)	Internet Users 2018	Penetration (% Population)	Facebook 31-Dec-2017
Afganistan	36,373,176	6,003,183	16.5 %	3,200,000
Bangladesh	166,368,149	88,687,000	53.3 %	28,000,000
Bhutan	817,054	370,423	45.3 %	350,000
Brunei	434,076	410,836	94.6 %	350,000
Cambodia	16,245,729	8,005,551	49.3 %	6,300,000
China	1,415,045,928	802,000,000	56.7 %	1,800,000
Hong Kong	7,428,887	6,461,894	87.0 %	5,200,000
India	1,354,051,854	462,124,989	34.1 %	251,000,000
Indonesia	266,794,980	143,260,000	53.7 %	130,000,000
Japan	127,185,332	118,626,672	93.3 %	71,000,000
Korea (N)	25,610,672	20,000	0.0 %	14,000
Korea (S)	51,164,435	47,353,649	92.6 %	43,000,000
Macao	632,418	512,352	81.0 %	380,000
Malaysia	32,042,458	25,084,255	78.3 %	22,000,000
Maldives	444,259	340,000	76.5 %	320,000
Mongolia	3,121,772	2,000,000	64.1 %	1,900,000

Myanmar	53,855,735	18,000,000	33.4 %	16,000,000
Nepal	29,624,035	16,190,000	54.7 %	8,700,000
Pakistan	200,813,818	44,608,065	22.2 %	32,000,000
Philippines	106,512,074	67,000,000	62.9 %	62,000,000
Singapore	5,791,901	4,839,204	83.6 %	4,300,000
Sri Lanka	20,950,041	6,710,160	32.0 %	5,500,000
Tajikistan	9,107,211	3,013,256	33.1 %	170,000
Thailand	69,183,173	57,000,000	82.4 %	46,000,000
Vietnam	96,491,146	64,000,000	66.3 %	50,000,000

Source: Internet World Stats, http://www.internetworldstats.com/stats.htm

Appendix 'B'

(Referred to page 29)

1. Questionnaire for Security Personnel

Name (Optional):

Profession/Post:

Office/Address:

Contact No:

Mail ID (if):

Q. 1. What is the current status of Cyber crime in Nepal?

Ans:

Q. 2. Which type of cyber crime that has frequently happened in Nepal?

Ans:

Q.3 What are the difficulties to investigate the cyber crime?

Ans:

Q.4 Are you satisfied with the rules/regulations of Nepal to prevent cyber crime?

Ans: a. satisfactory b. unsatisfactory c. Need to amendment

Because….

Q. 5. What are the common types of cyber crime of Nepal ?

Ans:

Q. 6. What are the activities taken by Nepal Police to control cyber crime?

Ans:

Q. 7. Are you satisfied with the activities of Nepal Police to control cyber crime?

Ans:

Q. 6. Have you observed any impacts (Social, Economy) of cyber crime? If so what are they?

Ans:

Q. 7. Do you think existing laws and mechanisms are adequate to control cyber crime in Nepal?

Ans:

Q. 8. What are the areas you think government / Police needs to improve to control cyber crime?

Ans:

Q. 9. What short of programs should be needed to make aware to people about cyber crime?

Ans:

Q.10. Are there any coordination mechanism within the concerned stakeholders to control cyber crime?

Ans:

Q.11 Do Nepal Police have sufficient resource or mechanism to control cyber crime ?

Ans:

Q.12 Are there any awareness programs developed by the government of Nepal ?

Ans:

Q.13 What are the special program conducted by Nepal Police to control cyber crime in Nepal ?

Ans:

Q.14 Any other things that you want to add?

Ans:

Appendix 'C'

(Referred to page 30)

2. Questionnaire for Victims of Cyber crime

Name (Optional):

Age: 26

Gender:

Address:

Contact No:

Mail ID (if):

Q. 1. What is your profession?

Ans:

Q. 2. How have you been victimized?

Ans:

Q. 3. Did you have any idea or knowledge about cyber crime before you were victimized?

Ans:

Q. 4. What actions did you take after you were victimized?

Ans:

Q. 5. Do you felt any negative impact in your life?

Ans:

Q. 6. Did you have any idea that makes you to report to police or you need to seek advice by other person?

Ans:

Q. 7. How Nepal police responded and acted on your report ?

Ans:

Q.8. At last anything you want to add?

Ans:

Appendix 'D'

(Referred to page 30)

2. Questionnaire for Students

Name (Optional):

Age:

Gender:

Address:

Contact No:

Mail ID (if):

Q.1 Do you have internet access in your mobile?

Ans: (Yes) (No) (Sometime)

Q.2 If you use internet, which type of site you frequently use?

Ans:

Q.3 Have you been ever victimized from someone through social media?

Ans:

Q.4 Do you have any idea about cyber crime?

Ans:

Q.5 Do you have any idea how to safe from cyber crime? If yes, how?

Ans:

Q.6 If someone sent to you friend request in your face book account, could you verified it? If yes, how you verify it?

Ans:

Q.7 Have you got any education / training from your college or from any other organization?

Ans:

Q.8 Do you have any idea that your unsafe behavior in social media may fall you in trouble? If yes, how do you protect yourself?

Ans:

Q.9 Anything you want to add about cyber crime?

Ans: