5.1 An Overview of the Present Research

The term ‘cybercrime’ is generally used to include any unlawful or deviant activity that is committed using a computer either as a tool or a target or both (Chaubey, 2009). The term is also used to include any unacceptable or undesirable, deviant or unlawful activity that is committed using a computer or other devices that are connected to the Internet. The available statistics show that there is an increase in the occurrence of cybercrime in India, but such statistics lack clarity on the different forms of cybercrime. However, previous research conducted in India and across the world show that there are diverse forms of crime being committed using a computer and other related devices that are connected to the Internet. The existing literature (Eg. Wolak et al., 2006; Juvonen & Gross, 2008; Mitchell et al., 2010) has established that, as a result of such newer forms of cybercrime, a large number of people particularly the youth are victimised. The present research attempts to find out the extent and forms of cybercrime victimisation among college students in Chennai. The study further attempts to examine the impact of such cybercrime on college students and their reporting behaviour of such victimisation.
Cybercrime victimisation is a relatively new phenomenon resulting from the advancement of technology. According to ‘Crime in India 2014’ published by the National Crime Records Bureau, the statistics on cybercrime is collected under two heads, namely, (1) offences registered under the Information Technology (IT) Act, 2000 and (2) offences registered under the Indian Penal Code, 1860 (IPC). According to the above report, cybercrime is rapidly increasing due to the extensive use of the Internet and Information Technology enabled services in the country. The report shows that about 7,201 cases of cybercrime were registered under the various provisions of the IT Act and 2,421 cases were registered under certain provisions of the IPC in 2014. From just 70 cases of cybercrime under the IT Act and 738 cases of cybercrime under the IPC registered in the year in 2002, the crime rate has grown to 7,201 and 2,421 respectively in 2014.

Several studies have been conducted on the different dimensions of cybercrime victimisation and ample research has been carried out on the characteristics of the victims of cybercrime such as age, gender, education and so on (Eg. Buzzle et al., 2006; Walker et al., 2010 and Lavanya & Prasad, 2014). To understand the factors and purposes related to the usage of the Internet in general and to find out the relationship between Internet usage and cybercrime victimisation in particular, the existing literature was reviewed and it was found that some studies have been conducted on the purpose of using the Internet and gender differences in using the Internet (Brafi & Arthur, 2011;
Cheang & Huang, 2005; Scotti et al., 2007). The relationship between victimisation and the purpose of using the Internet was also established by some studies (Yang et al., 2004; Gencer & Koc, 2012). Literature has further exhibited the other related items such as Internet addiction, (Chou et al., 2005), duration of Internet usage (Holt & Bosler, 2009), Internet behaviour (Fleming et al., 2010; Kennedy & Taylor, 2010) etc. among the youth and cybercrime victimisation. Some studies also attempted to examine the relationship between the level of knowledge in computer and cybercrime victimisation (Beran & Li, 2005; Mishna et al., 2010). Though sufficient literature is available to understand the forms of cybercrime victimisation and their extent, some authors (Eg. Reyns, 2010) have acknowledged the difficulty in estimating the extent of cybercrime victimisation due to factors such as small sample size, self-reporting surveys and so on. Despite the difficulty in estimating cybercrime victimisation, studies have established that there are several forms of cybercrime victimisation, prevalent both in India (McAfee’s Tween and Technology Report, 2013; ASSOCHAM & Mahindra SSG, 2015) and other countries (Kaspersky Lab & INTERPOL, 2014; Dell, 2015). All over the world substantial literature is available on the impact of crime on victims, but the impact of cybercrime on victims has not been extensively studied. Therefore, only a few studies were reviewed (Erdur-Baker & Kavist, 2007; Hay et al., 2010; Baker & Tanrikulu, 2010). Similarly, the
reporting behaviour of victims has been extensively researched in the field of victimology. However, dearth of literature is available on the reporting behaviour of the victims of cybercrime (Buhi et al., 2009; Afroz & Amin, 2014).

The existing statistics reveal that the extent of victimisation due to cybercrime has been on the rise over a period of time. Further studies conducted in several parts of the world have demonstrated that there are different forms of cybercrime victimisation and there are also various impacts on such victims. In India, limited research has been carried out on the problem of cybercrime and the impact of victimisation. Specifically, very few studies have been conducted on the newer forms of cybercrime, the forms of victimisation and their impact on victims. Hence, given the paucity of studies and information, it was proposed that a research study on the extent of cybercrime victimisation, the forms of cybercrime victimisation and their impact on victims be attempted. It was also suggested that the research encompasses the reporting behaviour of the victims and the response of those to whom the victimisation was reported. The outcome of the present research proved to be utilitarian in nature not only to understand the newer forms of cybercrime victimisation but also to understand the problems encountered by the victims as a result of cybercrime victimisation. Further, the outcome of the research would develop a typology of cybercrime victimisation, particularly victimisation using the Internet that could be taken into account by
the law makers while defining different forms of cybercrime which will further be useful to frame new articles in the law book. Furthermore, the findings of the present study would help the agencies of the criminal justice system to have a better understanding of the problem of cybercrime victimisation and help them effectively deal with cybercrime victimisation.

The present research was carried out with following specific objectives:

• To find out the extent of cybercrime victimisation among college students in Chennai.
• To find out the forms of cybercrime victimisation among college students in Chennai.
• To examine the impact of cybercrime victimisation.
• To study the reporting behaviour of students who are victims of cybercrime.

In light of the above objectives, a research was proposed, to be conducted among the population of students pursuing —under-graduate and post-graduate degrees in the various Government, aided and self-financing Arts and Science colleges affiliated to the University of Madras and situated within the city of Chennai. Data was collected from a sample size of 1,520 college students. A questionnaire was constructed for the purpose of the study and comprised several items that were used to measure each of the variables of the study.
The data collected was processed using the Statistical Package for Social Sciences (SPSS). Descriptive statistical analysis such as frequencies and percentages were used. Bi-variate and multi-variate statistical techniques were applied to test the hypothesis and examine the relationship between variables. The results thus obtained are outlined below.

5.2 Main Findings of the Study

- Of 1,520 respondents, 65 percent belong to the age group of 17 – 20 years. The percentage of respondents belonging to 25 years and above is significantly low. The results reveal an almost equal percentage of male (51.4%) and female (48.6%) respondents.
- About 32 percent of respondents are from rural areas and close to 69 percent are either from semi-urban (13.4%) or urban areas (54.7%). The results also show that a majority (62.0 %) of respondents live with their parents while about 25 percent live either in hostels or as paying guests. A minimal percentage of respondents live with their relatives (5.2), friends (4.8) and on their own (1.8).
- A vast majority of respondents (78.1%) are pursuing an undergraduate course, while 21.9 percent are post-graduate students. Among the respondents, 34.3 percent are in their first year, 38.5 percent in their second year and 27.3 percent in their third year.
• A quarter of the respondents’ monthly family income is below Rs. 10,000; about 40 percent of the respondents’ monthly family income is between Rs. 10,000 and Rs. 30,000, which implies that the majority of respondents are from middle class families. About 20 percent of the respondents’ monthly family income is between Rs. 30,000 and Rs. 50,000 and 14.8 percent of the respondents’ monthly family income is above Rs. 50,000.

• A large majority (87.5%) of respondents own either a laptop or a desktop computer at home. Interestingly, a notable percentage (27.2) own more than one computer.

• More than 75 percent of respondents share a computer with others either at home or in a hostel. The respondents also share their computer with their parents, siblings or friends. A significant percentage of them (54.1) share their computer with their siblings.

• Of the 87.5 percent of respondents who have a computer at home, 82 percent have an Internet connection.

• The various electronic devices used by respondents (N=1,249) are desktop, laptop, mobile and ipad/ipod. Of which, a majority (78.8%) of respondents access the Internet through their mobile phones and more than 57 percent use their laptop to access the Internet.

• Over 22 percent of respondents use the Internet for four hours and more every day. The percentage of respondents who use the Internet for less than one hour every day is only 35.3.
• With regard to the place where the respondents access the Internet, nearly 70 percent of them access the Internet at home and a significant percentage (42.0) access the Internet while in college.

• The respondents use the Internet for various purposes at different frequency levels (either sometimes, often or very often). It is observed that all respondents use the Internet for educational purposes, showing the constructive use of the Internet. A significantly high percentage (90.3) of respondents use the Internet for entertainment. Similarly, a very high percentage of respondents (88.4) use the Internet to download/upload pictures and videos. Findings on the level of a respondents’ computer knowledge such as installation of software, dismantling a computer, posting comments or messages, resolving Internet related issues etc., reveal that around 36 percent of respondents are tech savvy being able to create their own social networking account. Over 50 percent of respondents are capable of posting comments and messages either to a medium extent (25.9%) or to a large extent (25.1%). Nearly 50 percent of the respondents are ‘not at all’ aware of how to use a webcam. Similarly, a large percentage (56.5) of respondents could not resolve any problem related to the Internet. Overall, a large percentage of students do possess the knowledge on the various operations of the Internet and computer, however, this is only to a very small extent.
• About 12 percent of respondents were asked to meet with people who they got to know only through the social network sites (Facebook, Twitter, Whatsapp etc.) either often (6.5%) or very often (5.7%). Followed by this, around 11 percent received embarrassing posts or comments on social network sites (often 7.2% and very often 3.8%). A significant percentage of respondents (30.3) received embarrassing posts and comments and 28.1 percent (sometimes 12.9% and rarely 15.2%) respondents received a virus-infected file such as Trojan in their e-mail. The problems encountered by respondents, such as receiving virus-infected files, threatening e-mails, obscene/vulgar photographs etc. are considered as forms of victimisation both from a legal and social perspective. According to the provisions of the Information Technology Act, 2000, sending vulgar/obscene picture and videos is an offence. Hence, it may be noted that any person who receives such vulgar/obscene pictures and videos is a victim of cybercrime.

• With regard to the impact of cybercrime victimisation, around 52.0 percent of respondents feared secondary victimisation and a similar percentage (50.0) of respondents who faced cybercrime victimisation either feared that others would come to know about their victimisation or developed a sense of sadness and felt hurt for having experienced such a situation.

• Of the cumulative percentage of the impact of cybercrime victimisation on respondents, 15.6 percent developed a sense of
sadness and felt hurt [either very often (6.7%) or often (8.9%)] and 36.8 percent felt sad or emotionally vulnerable [sometimes (15.0%) or rarely (22.14%)]. A minor proportion (12.0%) of respondents developed addictions such as consuming alcohol as a result of cybercrime victimisation.

- Alarmingly, out of those who were victimised (N=926), only 1.6 percent reported their victimisation to the police. A high percentage (47.2) of them talked about it to their friends and their parents (19.8%). Unfortunately, nearly one-third (29.4%) of respondents did not report their victimisation to anyone.

- A vast majority of respondents (73.0%) did not report the incident, as they did not consider it a serious issue, while a significant percentage (42.7) did not report the incident, as they thought that such an experience of victimisation is a personal matter. Nearly 20 percent of respondents were not allowed to report their victimisation either by their parents or friends.

- With regard to the type of responses from persons to whom the respondents reported their victimisation, nearly 45.0 percent received support and a closely similar number (44.0%) of respondents were advised to stay away from the Internet by the people to whom they reported their victimisation. Only around 8 percent of them took legal action against their offender.
5.3 Conclusions

On the basis of the findings of the present research, the researcher has drawn the following conclusions. It may be noted that the conclusions are substantiated with the findings, which are in turn the results of the analysis of data using appropriate statistical tools.

- Various forms of cybercrime victimisation of varying degrees are prevalent among college students in city of Chennai. The respondents reported to have experienced four types of cybercrime victimisation, namely, cyber harassment, cyber stalking, cyber hacking and cyber sexual victimisation. Of all these forms, cyber stalking is the most predominant form of cybercrime victimisation. It can also be concluded that each form of cybercrime victimisation has either influenced or is influenced by other forms as they are positively correlated.

- The findings have also clearly demonstrated that the impact of cybercrime victimisation has taken different dimensions. It is evident beyond a doubt that over half of the victims reported that they were afraid that others would get to know about their victimisation and almost the same percentage of respondents were afraid that such an experience would recur. It can be concluded that cyber stalking contributed more to the impact of cybercrime victimisation followed by cyber sexual victimisation and cyber hacking.
• In light of the findings relating to the reporting behaviour of the victims of cybercrime victimisation, it may be inferred that the victims neither had faith and confidence in the criminal justice system (particularly the police) nor did they want to get legally involved. Further, irrespective of the levels of victimisation, the victims did not prefer to report their victimisation to the police.

• It can be concluded that there is a significant association between the age, gender, current place of stay and monthly family income of respondents and the extent of cybercrime victimisation. Statistically, there is a significant association between gender, current place of stay and monthly family income and the forms of cybercrime victimisation.

• The findings have explicitly shown that there is a significant association between the number of computers at home, number of hours connected to the Internet per day, place of the Internet usage, computer (desktop/laptop) at home and Internet connection at home and cybercrime victimisation. From the findings it can be concluded that there is a broad spectrum of purposes of Internet usage among college students; the Internet usage for the purpose of education tops the list. The findings have shown a positive correlation between the respondents’ knowledge of computers/Internet and their cybercrime victimisation.

• Based on the findings of the present study, the researcher feels it is appropriate to conclude that the victims of cybercrime need to
be provided support and counselling assistance through victim assistance centres. Such centres could be established at educational institutions and at Non-governmental organisations with the legal and financial support of the Government.

- As expressed by the victims of cybercrime, the findings have emphasised that the agencies of the criminal justice system, particularly the police should be equipped with new and updated cyber forensic tools. The agencies concerned should also be provided with suitable and modern administrative and physical infrastructure along with technically competent human resources.

To sum up, the researcher earnestly feels that the outcome of this research would indubitably enrich the existing literature in the field of cybercrime and cybercrime victimisation. It may not be an exaggeration to state that the outcome has created a new typology of cybercrime victimisation in the Indian context. Such a typology is expected to considerably enable the law makers to redefine the concept of cybercrime and to provide appropriate sections in the existing law or to create new laws. The researcher also feels that the agencies of criminal justice system and the academic institutions would deem this study as a significant piece of research which would guide them to effectively handle cybercrime victimisation among the youth, particularly the college students.