CHAPTER I

INTRODUCTION

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, undesirable, unlawful and deviant 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, Mitchell & Finkelhor, 2006; Juvonen & Gross, 2008; Mitchell, Finkelhor, Wolak, Ybarra & Turner, 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. The study was carried out among college students in Chennai. The findings of the study show that a notable percentage of participants are victims of many forms of unacceptable and undesirable activity committed using a computer and other devices that are connected to the Internet.
This chapter explains the significant differences between digital crime, computer crime and cybercrime for a better understanding of these terms, which are often interchangeably used. The problem of cybercrime over a period of time, the present global scenario and cybercrime in the Indian context has also been briefly discussed in this chapter. The provisions in the Indian Penal Code, 1860 (henceforth referred to as the IPC) dealing with cybercrime and the salient features of the Information Technology Act, 2000 (henceforth referred to as the IT Act) have been methodically appraised in this chapter. In addition, both the new and the generic forms of cybercrime have been discussed along with the impact of their victimisation.

1.1 Understanding Digital Crime, Computer Crime and Cybercrime

Although the terms digital crime, computer crime and cybercrime are interchangeably used it must be noted that these terms are not one and the same. The term ‘crime’ is broadly defined as the intentional omission or commission of acts that are in violation of criminal law or the laws that are in force. Tappan (1947) defines crime as an intentional act in violation of the criminal law (statutory and case law) committed without defence or excuse and penalised by the state as a felony or misdemeanour. This definition may be used to understand any traditional form of crime that is committed in the real world. However, dealing with specific forms of crimes that are
committed using a computer either as a tool or a target is more complex and may not fit the above definition. As stated above, many terms, such as, computer crime, hi-tech crime, Internet crime, digital crime, online crime, electronic crime and computer abuse are used to denote any criminal act that involves a computer. However, all of these terms differ in usage.

The term ‘digital crime’ is broadly used to embrace crimes that are usually categorised as computer crime and cybercrime; and other crimes where a digital opportunity is possible, all of which are explained. This includes other forms of crime, such as, music and video piracy, which are caused by the growth of digital forms of representation and the use of online facilities to commit traditional crimes like drug dealing (R. Bryant & S. Bryant, 2014).

According to Newman (2009), computer crimes are crimes that involve stand-alone computers, hardware or software, or crimes that target or utilise computer data and systems to commit any illegal activity; whereas, cybercrime includes crimes that happen in cyberspace, using a computer as a tool or a target committed through the Internet. National Security Presidential Directive 54/Homeland Security Presidential Directive 23 defines cyberspace as the interdependent network of information technology infrastructures, and includes the Internet, telecommunications network, computer systems, embedded processors and controllers in critical industries. Common
usage of the term also refers to the virtual environment of information and interactions between people (US Cyberspace Policy Review, 2011). Newman was of the opinion that cybercrime is no different from any other crime. He was also of the opinion that, what makes cybercrime real is the sea of opportunities that individuals are provided with to take advantage of the technology of cyberspace. He also suggested avoiding the term ‘cyberspace’ and using a more practical term to describe the environment of opportunity – Information Technology (IT) environment, where cybercrime occurs.

A more simple description of cybercrime has been explained by Symantec Corporation (2007), which states that the term ‘cybercrime’ is used to describe a crime that involves a computer or network or hardware device. Several other authors have also defined the term cybercrime in disparate ways. However, the content of such definitions are by and large similar. Chaubey’s (2009) generalised definition of cybercrime states that it is an unlawful act when a computer is used either as a tool or a target or both. A slightly different definition was given by Kshetri (2009) who added networks to the definition and expanded the idea of unlawful act. He defines cybercrime as a criminal activity where computers or computer networks are the principal means of committing an offence or violating laws, rules and regulations. As the development of electronic devices came into the market, Baiden (2011) enhanced the definition of cybercrime and defined it as an essentially criminal
activity where computers, networks or electronic information technology devices are the source, tool, target or place of crime. Bernat and Godlove (2012) defined cybercrime as that which involves gaining illegal access to or illegal entry into a computer or illegally interfacing with another through the use of a computer.

The aforementioned definitions of cybercrime indicate that there is no universally accepted single definition. This may be due to the fact that the content of the definition would keep changing according to the change and growth in technology. However, keeping the above definitions in mind, the present research describes the term cybercrime as any unacceptable or undesirable activity that is committed using a computer and/or other devices that are connected to the Internet.

1.2 Evolution of the Computer and Related Crimes

The evolution of cybercrime takes one back to the beginning of the 19th century when the base for computers was invented. It was Charles Babbage who invented the first difference engine, a hand operated calculator in the 1820s. Later on, he invented analytical engines which had similar operations as that of a computer (Bromley, 1982). In about seven decades from 1944, when the first Electronic Numerical Integrator and Computer (ENIAC), the forerunner of modern computers was created, there are computers galore. The number of computer users continues to grow in an unexpected manner.
The science of computers has enabled one of the most extraordinary transformations of our societies in human history (Bentley, 2012). The chronological timeline of computers started from 1940 to 1949 as the first generation computers; from 1950 to 1959, the second generation computers with transistors; from 1960 to 1968, the third generation with microprocessor; from 1971 to 1978, the fourth generation computers with micro-computers; 1980s, the rise of micro-computers; 1990s, personal computers; and then 2000s saw mobile computing (Zorn, n.d.). Six decades of growth in technology was amazing and Moore’s Law states that processor speeds or the overall processing power of computers will double every two years (Moore, 2006). This is true as technology grows incredibly quickly. Moore’s Law is connected with the exponential growth of technology in the world today.

Computers came into existence and related crimes started popping up. In the beginning, particularly in the 1960s, computer crimes were known as sabotage and machines were physically damaged; and in the 1970s impersonation became notorious. In the 1990s, as the number of computers and high-speed Internet users increased, the trends in computer related crimes grew diverse. From the destruction of computer machines to cracking computer hardware, credit card fraud, identity theft, Trojan attacks, malware outbreaks, spam, denial of service, underground hacking and cyber terrorism formed part of the
crimes relating to the information technology environment (Kabay, 2008).

While analysing the trends in cybercrime over a period of ten years, from 2004 to 2014, Grabosky (2014) presented the following facts:

1. Cybercrime has become highly sophisticated in terms of the use of sophisticated technology such as Zombie computers.

2. The technology of cybercrime has also been commercialised. According to Grabosky, there are many ‘hackers for hire’ who develop hardware and software programmes.

3. Though there are individual cyber criminals, due to the growth of digital technology, organisation of groups is simple and possible. Such formation of smaller groups creates greater damage in the case of botnets.

4. State sponsored cybercrime in terms of illegal cyber-attacks, particularly, on Estonia and Georgia by Russia was one of the significant trends.

The advent of wireless technology, cloud-computing, voice-over Internet Protocol and social media resulted in unlawful activities that ranges from the remote detonation of explosive devices to the transmission of fraudulent solicitations and distribution of illicit images of children (pp. 1-5).
As new technology progresses, abuse of such technology also sets in. There is a parallel growth of cyber technology and cybercrime. New technologies breed new types of cybercrime. Therefore, strategies to either reduce or alleviate cybercrime victimisation need to take into account the growth of technology as a major concern.

1.3 Cybercrime: Global Scenario

The global scenario of cybercrime is alarming as it impacts the social, political, economic and cultural aspects of citizens. The Centre for Strategic and International Studies (CSIS, 2014) estimated, that, in 2014 alone, the net loss incurred in the global economy due to cybercrime would cross US$ 400 billion and it could be a maximum of US$ 575 billion, because the cost of stolen intellectual property and cyber espionage is very difficult to estimate. Cybercrime affects companies, trade, governance, innovations, competitiveness and global economy. Below are some of the cybercrime experiences of a few countries.

The United States FBI’s Internet Crime Complaint Center (IC3, 2014) reports that in 2014, it received 2,69,422 complaints with an adjusted US$ of 800,492,073. On an average, approximately 22,000 complaints were received each month. It is an amazing to know that IC3 has so far received 3,175,611 complaints.
According to the data provided by Japan’s National Police Agency (2015), the number of reports of possible online crimes has increased to over 40 percent over the previous year. In 2014, online bank fraud cases have resulted in losses of US$ 24 million and the cost of online fraud cases in Japanese banks was US$ 13 million in the first half of that year.

The UK Office for National Statistics (2015) reported that the crime rate for England and Wales has doubled to more than 11.6 million offences in 2015. This sharp rise was attributed to the inclusion of an estimated 5.1 million online fraud incidents and 2.5 million cybercrime offences for the first time. It is also noted, that, 84 percent of the reported cybercrime involved computer viruses.

In spite of the Great Firewall, online censorship mechanism and launching of a six month programme called ‘cleaning the net’ in the first eight months of 2013, more than 20,000 Chinese based websites were hacked and more than eight million servers hijacked by Zombie and Trojan programmes that were controlled overseas (Marsh, 2014).

Symantec, a software company which works for cyber security has ranked 20 countries that faced or caused the most number of cybercrime in 2011 (Businessweek/Symantec, 2011 as cited in Enigma Software Group, 2011). It used six cybercrime activities, such as, sharing of malicious computer activity rank, malicious code rank, spam zombies rank, phishing website hosts rank, bot rank and attack
origin rank. The following figure explains in detail. India constitutes three percent of cybercrime in 2011 and is ranked among the top 20 countries.

**Figure 1.1: Top Countries in cybercrime**

(Source: Businessweek/Symantec as cited in Enigma Software group, 2011)

### 1.4 An Overview of Cybercrime in India

As stated, there is no official definition of cybercrime in the Indian context. As a result, any comprehensive statistics or data on cybercrime in India is difficult to obtain. However, the National Crime Records Bureau (an agency of the Government of India) in its official publication, Crime in India (NCRB, 2014), has included a list of offences as cybercrimes. Such offences are dealt with under the provisions of the Indian Penal Code, 1860 and the special laws such
as the IT Act, 2000, the Indian Copyright Act, 1957 and the Trade Marks Act, 1999.

The official statistics of 2014 show 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. From 70 cases of cybercrime under the IT Act and 738 cases of cybercrime under the IPC registered in the year 2002, the incidence of crime has grown to 7,201 and 2,421 respectively in 2014. Compared to the previous year 2013, there is an alarming increase of 59 percent in 2014 where 4,356 cases under the IT Act and 1,337 under certain sections of the IPC and Special and Local Laws (SLL) were registered.

The table below (Table 1.1) gives an account of the growth in cybercrime in India from 2010 onwards.

Table 1.1 Number of cases of cybercrime registered in India, 2010 - 2014

<table>
<thead>
<tr>
<th>No. of cases registered under certain sections of</th>
<th>2010</th>
<th>2011</th>
<th>2012</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Act, 2000</td>
<td>966</td>
<td>1,791</td>
<td>2,876</td>
<td>4,356</td>
<td>7,201</td>
</tr>
<tr>
<td>IPC, 1860 and SLL</td>
<td>356</td>
<td>422</td>
<td>601</td>
<td>1337</td>
<td>2,421</td>
</tr>
<tr>
<td>Total</td>
<td>1,322</td>
<td>2,213</td>
<td>3,477</td>
<td>5,693</td>
<td>9,622</td>
</tr>
</tbody>
</table>

Source: Crime in India, NCRB Reports

Furthermore, the cost of cybercrime has unexpected growth. According to the Cybercrime Survey Report 2014 of Klynveld Peat...
Marwick Goerdeler (KPMG – India, 2014), the financial sector is highly prone to cyber attacks. Rathi (2014), quoting the Delhi High Court Commission Report mentions that in the year 2013, cybercrime cost the government about Rs. 24,630 crores. The 2013 report claims that the increase in cybercrime is due to the increase of Internet usage cause many to fall prey to these new crimes.

There is consistent growth in the use of Internet world over, as it has become an integral part of people’s lives. This is true for adolescents too. The number of young people using the Internet is growing exponentially day after day. The 2015 Internet World Stats (2015) claimed that about 45 percent of the world population that is, 3,270,490,584 of the total population of 7,260,621,118 are using the Internet for various purposes with a majority of Asian Internet users located in India.

Figure 1.2: Internet users across the world

Source: Internet World Stats. Basis: 3,270,490,584 Internet users, June 2015
From the above Figure 1.2 it is evident that Asians hold a lion’s share of global Internet users. The data stated that there were 1,563,208,143 Internet users in Asia. The global index also mentioned that India topped second in the whole of Asia in the number of Internet users with 354 million users (22.6 percent of Asian users), next only to China with 674 million Internet users. However, the penetration percentage of population in India is only 28.3. This implies that the number of the Internet users in India is on the rise.

The Report of the Telecom Regulatory Authority India (TRAI) shows that there is a significant increase in the number of Internet and Broadband subscribers. The Internet subscriber base in the country as on 31st March 2014 was 251.59 million as compared to 164.81 million the previous year; while it was a mere 3.42 million in 2002 (TRAI Report, 2014). A decade and more brought in a sea of change in the number of people subscribing to the Internet and thereby proving a constant increase in the number of Internet users in India. Data from the Internet and Mobile Association of India (IAMAI) has shown that in India the Internet population has grown from 60 million in 2009 to 190 million in 2014. Mumbai has a little over 12 million Internet users followed by the national capital, Delhi with 8.1 million users and Hyderabad with 4.7 million users. Chennai and Kolkata are in fourth and fifth place with 4.5 million and 4.4 million users respectively (IAMAI & BCG Report, 2014, p. 11).
1.5 Legal Provisions dealing with Cybercrime and the Salient Features of the Information Technology Act, 2000

The Indian Penal Code of 1860 does not contain specific provisions to deal with the new forms of cybercrime. The Indian Parliament passed the Information Technology Act on 17th October 2000 inspired by the Model Law on Electronic Commerce that was adopted by the United Nations Commission on International Trade Law (UNCITRAL) at its 605th meeting on 12th June 1996. Since then, appropriate amendments were made to the IPC to provide necessary changes to the various provisions that deal with offences relating to documents and paper-based transactions. The Reserve Bank of India Act, 1934 was also amended to facilitate electronic fund transfers between financial institutions and banks. Further, the Banker’s Book Evidence Act, 1891 was amended to provide legal sanctity for the books of accounts maintained in electronic form by the banks.

The Information Technology Act, 2000 facilitates international trade and provides an alternative to the paper-based method of communication and storage of information (Rao, n.d.). The author commented that the IT Act is in line with the Model Law on Electronic Commerce that was adopted by UNCITRAL. It also contains provisions for promoting the national and regional requirements of information technology.
Basu and Jones (2002) in their article critically reviewed the IT Act and stated that the Act comprises three aspects – the first being legal recognition of electronic records and communication, in other words, the Act essentially deals with issues such as legal recognition of electronic documents, legal recognition of digital signatures, offences and contraventions and recognition of justice dispensation systems for cybercrime. Secondly, regulation of Certification Authorities (CAs) and thirdly, cyber contraventions (Network Intelligence, 2014) were included in the Act.

The IT Act is divided into 13 chapters with 94 sections. The Act includes four Schedules (Sections 91 to 94) which list the relative amendments made to the Indian Penal Code, 1860, the Indian Evidence Act, 1872, the Bankers’ Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934. The 13 chapters of the Act are as follows:

- Chapter I: Preliminary
- Chapter II: Digital Signatures
- Chapter III: Electronic Governance
- Chapter IV: Attribution, Acknowledgement and Dispatch of Electronic Records
- Chapter V: Secure Electronic Records and Secure Digital Signatures
• Chapter VI: Regulation of Certifying Authorities

• Chapter VII: Digital Signature Certificates

• Chapter VIII: Duties of Subscribers

• Chapter IX: Penalties and Adjudication

• Chapter X: The Cyber Regulation Appellate Tribunal

• Chapter XI: Offences

• Chapter XII: Network Service Providers not to be Liable in Certain Cases

• Chapter XIII: Miscellaneous

The First Schedule lists the amendments made to the IPC where 17 sections were amended. For instance, after Section 29, Section 29A was inserted to include the term ‘electronic records’. The other sections that were amended include Sections 167, 172, 173, and 192. The Second Schedule of the IT Act includes the amendments made to the Indian Evidence Act. The sections that were subjected to amendment include Sections 3, 17, 22, 34, 35, 39, 47, and 67. Interestingly, Section 3A, which defines the term ‘evidence’ was amended as follows: in the definition of ‘evidence’, for the words ‘all documents produced for the inspection of the court,’ the words ‘all documents including electronic records produced for the inspection of the court’ shall be substituted. The Third Schedule lists the amendments relating to the Bankers’ Book Evidence Act and the
amendments relating to the Reserve Bank of India Act is listed in the Fourth Schedule (IT Act, 2000).

With the exception of the preliminary sections of the IT Act, all the sections up to Section 64 deal with the various issues of electronic commerce. Various offences and punishment for such offences are dealt with under Sections 65 to 74. The various offences such as tampering with computer source documents (Section 65), hacking a computer system [Section 66(1) and (2)], publication of obscene information in electronic form (Section 67) and likewise are dealt with in detail.

Section 17(1) of the Act provides for the appointment of Controller – Controller of Certifying Authorities. Such a Controller shall perform various functions provided under Section 18. Notably, Section 69(1) entrusts the Controller with power to direct any agency of the Government to intercept any information transmitted through any computer source in order to protect the interest, sovereignty and integrity of India, or the security of the State.

Section 70(1) of the Act provides that the Government can declare any computer or computer system or computer network to be a protected system. Sub-section (3) of Section 70 provides the punishment for violation of Section 70(1). Section 71 provides the punishment for misrepresentation of or suppressing any material fact from the Controller or the certifying authority for the purpose of
obtaining any licence or digital signature certificates. There are also provisions for punishment for breach of confidentiality and privacy under Section 72 of the IT Act.

Section 73 of the Act deals with the publication of false digital signature certificates and with the punishment for such an act. Any person, who deliberately creates, publishes or makes available a digital signature certificate for any fraudulent purpose shall be imprisoned for two years including a fine up to one lakh rupees to be paid by him/her (Section 74). Provisions of this Act apply to the offences committed not only in India but also outside India irrespective of the nationality of the person who commits the offence [Section 75(1)]. The Act also provides that the provisions shall apply to an offence involving a computer, computer system or computer network in India [Section 75 (2)]. Section 76 provides for the confiscation of any computer, computer system, floppies, computer discs, tape drives or any other related accessories used or involved in the offence. Section 77 of the Act states that the penalty and confiscation under this Act shall not interfere with any other punishment provided under any other laws, which is currently in force. Although the procedures and powers to investigate offences are laid down in the Code of Criminal Procedure, Section 78 of the IT Act deals with the powers to investigate offences. This Section provides a police officer, not below the rank of Deputy Superintendent of Police to investigate any offences under the IT Act, 2000. In certain cases,
the network service providers are exempted from criminal liability, if they prove that the offence was committed without their knowledge and that they have exercised all due diligence to prevent the commissions of such offences.

Chapter XIII of the IT Act contains the miscellaneous provisions. Sections 80 to 90 have provisions, such as, power of police officers and other officers to enter and search and the like (Section 80); to consider Controller, Deputy Controller and Assistant Controller as public servants (Section 82); the power of the Central Government to give directions to any state governments, with regard to the execution of any of the provisions of this Act or any rule and regulation related to this Act in the State (Section 83); protection of action taken in good faith (Section 84); take action against offences by companies (Section 85); removal of difficulties (Section 86); power of the Central Government to make rules (Section 87); constitution of an Advisory Committee (Section 88); the power of control to make regulations (Section 89); and the power of the State Government to make rules (Section 90).

Sections 91, 92, 93 and 94 deal with amendments to the Indian Penal Code, 1860, the Indian Evidence Act, 1872, the Bankers’ Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934 respectively.
To summarise, the IT Act enables companies to file any application or any other document(s) in electronic form with the authority seal or office owned or controlled by the appropriate Government. The Act also addresses issues of security which is critical for the success of electronic transactions (Chaubey, 2009).

However, as technology grows in an unprecedented way, new forms and manifestations of cybercrime, such as, theft of Internet hours, cyber theft, cyber stalking, cyber harassment, cyber defamation, cyber fraud and misuse of credit card numbers have emerged after the IT Act, 2000 came into force as the Act did not have enough provisions to deal with such new forms of cybercrime. Therefore, the Government of India prepared the Information Technology Amendment Bill, 2006 to encompass the lacunae in the IT Act of 2000. After two years of strenuous efforts to make the Bill as effective as possible, the Bill was passed in Parliament in the last week of December 2008 and it came into force from 27th October 2009. The IT (Amendment) Act, 2008 made it possible to include new forms of cybercrime such as cyber stalking, violating the privacy of a person, cyber terrorism and the like. Altogether 13 new cyber offences were inserted and seven existing offences were substituted with new laws. The amendments focussed on issues such as data privacy and information security. Substituting the use of electronic signature with digital signature is yet another contribution of the IT (Amendment) Act, 2008. By doing so, digital signature technology is
made neutral which allows including biometric signatures. In this way, the IT (Amendment) Act, 2008 brought in many changes to the IT Act, 2000. For example, Section 43 of the IT Act, 2000 was amended in such a way to make ‘a body corporate’ (that includes a firm or sole proprietorship or other association of individuals engaged in commercial or professional activities), which possesses, deals or handles sensitive personal information and does not have adequate controls that result in wrongful loss or wrongful gain to any person, is liable to pay any damages to that person up to five crore rupees. In addition, Section 66 of the IT Act, 2000 was amended and about six sub-sections were added relating to punishments for offences that are considered cybercrimes. Section 66A of the IT (Amendment) Act specifies the punishment for sending offensive messages through communication service providers. It was struck down by the Supreme Court on 23rd March 2015 as such a law struck at the root of liberty and freedom of expression (Choudhary & Mahaputra, 2015). Section 66B of the IT (Amendment) Act, 2008 specifies the punishment for dishonestly receiving stolen computer resource(s) or communication device(s). Section 66C of the IT (Amendment) Act, 2008 included identity theft as a form of cybercrime. Accordingly, any person who dishonestly makes use of the electronic signature or password or any other unique identification feature of any person for fraudulent reasons is liable to punishment. Section 66D of the IT (Amendment) Act specifies the punishment for cheating by personation using a
computer resource. Section 66E of the IT (Amendment) Act specifies the punishment for the violation of privacy and Section 66F of the IT (Amendment) Act specifies the punishment for cyber terrorism, which is a new concept that was brought in by the Amendment of 2008.

Section 67 of the IT (Amendment) Act was also amended to entail punishment for publishing or transmitting obscene material in an electronic form with the sub-sections specifying the punishment for publishing or transmitting of material containing sexually explicit actions etc., in an electronic form [Section 67A of the IT (Amendment) Act]. The newly added sub-section 67B of the IT (Amendment) Act addresses the issue of child pornography. Through this Section, publication or transmission of material in any electronic form which depicts children engaged in sexually explicit act(s) or conduct is subject to punishment; anyone who creates, facilitates or records these acts and images is punishable with imprisonment of five years and is liable to pay a fine which may extend up to ten lakhs in the case of a first offence and seven years as well as fine of 10 lakhs for subsequent offences. Besides these amendments, the IT (Amendment) Act also introduced the Indian Computer Emergency Response Team as a national agency to operate in the area of cyber security, particularly, in collecting, analysing and disseminating cyber incidents, forecasting and alerting cyber security on issues concerning national safety [IT (Amendment) Act, 2008].
However, the Amended Act of 2008 needs to be further improved upon as it does not cover major issues that emerged after 2008, such as, spamming, privacy protection, cyber war, identity theft, data protection in Internet banking and intellectual property rights of owners’ ‘Domain name’ etc. The crimes committed through mobile phones do not find place in the Amended Act. A detailed legal regime is needed to protect the privacy of individuals (Chakraborty & Kusuman, 2014) from many such crimes.

Besides offences under the IT Act, 2000, such as, tampering with computer source documents, obscene publications and transmission in electronic form, unauthorised access, attempt to access a protected computer system, publishing false digital signature certificate and breach of confidentiality, there are offences under the Indian Penal Code, 1860, which could be filed as part of cybercrime. Through Section 91 of the IT Act, 2000, amendments were made to several sections in the IPC. For example, by adding the term ‘electronic record,’ Section 29A was added to Section 29 of the IPC. This addition enlarges the scope of adding any electronic document as evidence in addition to paper-based documents. Also, Section 167 of the IPC deals with the framing of an incorrect document with intent to cause injury to a public servant. An amendment made to that Section widens the scope of Section 167 in such a way that framing, preparing and translating any document as an electronic record that is done by a public servant to cause harm could also be charged under this Section.
Moreover, by adding the term ‘electronic record’ to Section 172 of the IPC that deals with cases of absconding to avoid service of summons or other proceedings, Section 172 of the IPC is made paperless and allows for submission of an electronic record as an authorised and legal act. Similarly, Section 173 and Section 175 of the IPC were also changed to paperless laws by adding the term ‘electronic record’ to the content.

Further, the addition of the term ‘electronic record’ to the existing Section 192 of the IPC that deals with fabricating false evidence and Section 204 of the IPC that deals with the destruction of document(s) to prevent its production as evidence provides more clarity to these sections. Both sections consider electronic record as a legal document. The addition of the term ‘electronic record’ along with the filed record and document constitutes most of the changes in Chapter XVIII of the IPC. Accordingly, Sections 463, 464, 466, 468, 470, 471 and 474 now allow the inclusion of the term ‘electronic record’ to the existing paper-based records. For example, Section 463 of IPC that includes electronic record to commit forgery and Section 464 of IPC that includes electronic record or digital signature to make, sign, seal, execute, transmit and affix a false document fall under the offences related to cybercrime (Chaubey, 2009).

The IT (Amendment) Act also brought in many changes in the IPC. In Part III of the IT (Amendment) Act, specific sections in the IPC were
amended. For example, the Section 4 of the IPC, which deals with the extension of the IPC to extra-territorial offences, after the clause (2), a new clause (3) was inserted, namely, ‘a person in any place without and beyond India committing an offence targeting a computer resource located in India was also held responsible from thenceforth.’

Similarly, Sections 40, 118, 119 and 464 of the IPC were also amended in the IT (Amendment) Act. For example, Section 40 of the IPC under clause (2), Sections 118, 119 and 120 were added. Accordingly, changes were made to Sections 118 and 119 of the IPC by substituting the phrase ‘omission or by use of encryption or any information hiding tool’ in the place of the term ‘illegal omission.’

The term ‘electronic signature’ was used to substitute of the term ‘digital signature’ in Section 464 of the IPC so that all forms of technology would fit into the frame of reference.

Needless to say, such vigorous legal efforts are certain to reduce cybercrime and its victimisation, it seems imperative to create awareness among the youth and others on the problems of cybercrime and its impact among the victims.

1.6 General Typology of Cybercrime

There have been various classifications of cybercrime in the past that include some general classifications too. There are classifications mostly on the basis of a relationship between traditional crimes and
cybercrime. One such classification was done by Chaubey (2009). He classified cybercrime mainly as traditional crimes that are committed through the Internet, for example, cheating and pornography; new crimes that are committed through the Internet, such as, hacking and spreading viruses; and new crimes that help to commit older crimes, for example, where hacking is committed to carry out cyber frauds, whereas Bernat and Godlove (2012) classify cybercrime as just new methods for committing old offences against person and property and totally new offences using computers.

The widely accepted classification is provided by Wall (2007/2010). He classified cybercrime into three kinds that emphasised the role of technology in general: computer-integrity crime, like hacking and cracking; computer-related crime, like manipulation of fee frauds using a computer network; and computer-content crime, like selling and buying pornographic materials. Rege (2008) opined that these three categories are clearly not exclusive, since crimes like identity theft are complex and could fit in all categories and others like gambling might fit both under computer-assisted and computer-content crime.

While there are authors who subscribe to the classification of cybercrime in three categories like that mentioned in the classification above, Turrini and Ghosh (2010) classify cybercrime into two major categories: those crimes that require technical
knowledge of the computer and networks (technical crimes) and those who do not (non-technical crimes). But, Tiwari and Singh (2013) classify cybercrime into four categories, namely, (i) data crimes that include data interception, data modification and data theft; (ii) network crimes that consist of network interferences and network sabotage; (iii) access crime that involves unauthorised access and virus dissemination; and (iv) related crimes that comprise of aiding and abetting cybercrime, computer related forgery, fraud and content related crimes.

There are two basic approaches followed at the international level to classify cybercrime: one is to group them under the focus on material offence of the object and the other is to consider whether computer systems or information systems form an integral part of the modus operandi of the offence. The former has been taken up in the Commonwealth of Independent States Agreement (where the offence object is the computer information) and also in the Title One of the substantive Criminal Law Chapter of the Council of Europe Cybercrime Convention (where the objects are computer data or computer systems). The latter is seen in the Titles Two, Three and Four of the same as well as in the Shanghai Cooperation Organisation Agreement and the Draft African Union Convention (Podgor, 2002).

Several authors have provided different classifications of cybercrime. However, they are neither comprehensive nor inclusive. In this
context, the UN General Assembly in its resolution 65/230 (2011) requested the Commission of Crime Prevention and Criminal Justice to form an open-ended inter-governmental expert group to undertake a comprehensive study on the problem of cybercrime and also to study the responses by the member states of the international community in the private sector to cybercrime. In its first session of the inter-governmental expert group held in Vienna in January 2011, the methodology for the study was assigned to United Nations Office on Drugs and Crime (UNODC) and the topics for the collection of data were reviewed and adopted. The study (UNODC, 2013, pp. 11-16) examined the problem of cybercrime from the perspective of academic and international organisations. The results of the study discuss the various issues relating to cybercrime, including internal connectivity and cybercrime. The study considered the definitions of cybercrime and found that certain definitions are required for core cybercrime acts. The comprehensive concept is not well suited as a legal term or act. The report stated that cybercrime itself could not be confined to a single definition since the term may include a collection of acts rather than one single act. However, the essential elements of the term cybercrime can be described by recruiting a non-exhaustive list of acts that constitute cybercrime. Further, such acts can be organised into categories based on the modus operandi of such acts and the material offence object. The report further discussed the various acts that constitute cybercrime and recommended including 14 acts that
may constitute cybercrime. Those 14 acts are further grouped into three broad categories.

Acts, such as, illegal access to a computer system, interception, acquisition or interference with a computer system or data, production, distribution or possession of a computer, misuse of tools and breach of privacy are included in the list of acts which are considered as acts against the confidentiality, integrity and availability of computer data or systems. The second category of acts is computer related acts for personal or financial gain or harm. Such acts include computer related fraud or forgery, identity offences, copyright or trademark offences or acts that cause personal harm, solicitation of children and the act of sending or controlling spam. The next category of cybercrime acts concerns the computer content such as acts involving hate speech, production, distribution or possession of child pornography and acts in support of terrorism offences (UNODC, 2013, pp. 16–17).

In general, cybercrime is classified into two major categories, namely, ‘old crimes in new cyber skin and new crimes in old cyber skin’. But the new cyber skin is unable to contain the emerging dangers of cybercrime. Wall (2007) claimed that there are ‘new crimes, no bottles.’ Whether crimes in cyber world are new or old, they are unique and peculiar in the present scenario and, the classification is done complying with the approach one takes.
1.7 Understanding Some Specific Forms of Cybercrime

Aforementioned in this Chapter are the various categories of cybercrime. Though, the existing literature and the reports/documents of the international institutions/organisations have provided various categories of cybercrime, certain specific forms of cybercrime need to be clearly outlined. The following are some of the forms of cybercrime which occur more frequently in countries like India. They are as follows:

1.7.1 Computer virus

A computer virus is a malware and insidious software programme or programme code and when introduced into a computer could attack or damage the computer data available in the computer or the networks, for example, the ‘I Love You’ virus that was widely circulated in 2000 (Cohen, 1986).

1.7.2 Phishing

It refers to any ‘sophisticated fishing’ type of attack (Dunham, 2004). Microsoft defines it as a type of online identity theft. It uses e-mail and fraudulent websites that are designed to steal your personal data or information such as credit card numbers, passwords, account data, or other information (Microsoft, 2014).
1.7.3 Internet software piracy

Software piracy is defined as the illegal copying, distribution, or use of software. Internet software piracy refers to the use of the Internet to: provide access to downloadable copies of pirated software; advertise and market pirated software that is delivered through the mail; or offer and transmit codes or other technologies to circumvent anti-copying security features (Business Software Alliance, 2009).

1.7.4 Nigerian scam

It is also known as the 419 Scam where recipients of an unsolicited e-mail are asked to provide a safe bank account for the transfer of frozen or illegal funds. It is named after its Nigerian criminal code, the ‘419’ penal law – taking money under false pretences (Kovacich, 2008).

1.7.5 Cyber defamation targeting the individual self

A failed relationship may lead either of the aggrieved individuals to spread rumours about their ex-partner to other members through his/her own posts, community walls etc. (Halder & Jaishankar, 2009).

Besides the above types of cybercrime, the following types occur more frequently among youth, particularly the student community. They are:
1.7.6 Cyber bullying

Cyber bullying involves the use of information and communication technology such as e-mail, mobile phone and pager text messaging, instant messaging, defamatory personal websites and defamatory online personal polling websites, to support deliberate, repeated and hostile behaviour by an individual or a group that is intended to harm others (Belsey, 2005).

1.7.7 Cyber pornography

Cyber pornography is the dissemination of pornographic material using the Internet as a medium. This could be in the form of pictures, text, audio and more recently, video and virtual images (Verma, 2012).

1.7.8 Cyber flirting

Offline flirting that happens in a technology orientated environment is cyber flirting. It normally happens via texts, social network sites and e-mail. In cyber flirting, an exclusive and disinhibited online, romantic and sexual relationship happens without serious intentions, giving importance to conversations (Whitty & Carr, 2003).

1.7.9 Cyber hacking

It is an act that is carried out to gain unauthorised access to a computer system. There have been incidents in the past, when this act
was not potentially breaching confidentiality but also affecting the integrity and/or availability, such as, modification of medical reports, breach of military systems or monitoring and alteration of telecommunication services (Furnelb & Warren, 1999).

1.7.10 Cyber stalking

It refers to the use of the Internet, e-mail and other electronic communication devices to stalk another person. Stalking generally involves repeatedly harassing and threatening an individual, such as following a person, appearing at a person’s home or place of business, making harassing phone calls, leaving written messages or objects, or vandalising a person’s personal property (Ashcroft, 2001).

1.7.11 Morphing

It is a technique used to alter a photograph of an individual by an unauthorised person without his consent or knowledge. Photographs posted on social networking sites are downloaded from an individual’s personal album and used for pornography or defamation. The parts of an individual’s photograph, such as, the head and face, that represent the person and the rest of the photograph is morphed. Morphing is represented in many ways. Sometimes, the changes made to an individual’s photograph may be vulgar and obscene. Sometimes, the manipulation is used to defame a person (Salimi & Mansourabadi, 2014).
It is worthwhile to mention here that these forms of cybercrime are by and large committed through social network sites.

1.8 Social Network Sites and Their Consequences

Social Network Sites (SNSs) are the web-based services where individuals are allowed to build a public or sometimes semi-public profile within a confined system and it provides a list of other users with whom they share a connection; and where individuals are allowed to view and get across their list of connections and of those made by others within the bounded system (Boyd & Ellison, 2008, p. 211). The name of such connections may vary from one site to another. In general public discourse, the terms ‘social network site’s and ‘social networking sites are interchangeably used. However, to describe the above phenomenon, the term social network sites is used. The term networking is not used in this context because networking emphasises a relationship initiation that may be between strangers. Of course, networking may be possible on these sites, though it may not be the primary practice of many of those individuals who share a connection. Also, it is not what differentiates them from other forms of computer-mediated communication (Boyd & Ellison, 2008, p. 211).

Citing Haythornthwaite (2005), Boyd and Ellison (2008) commented that SNSs become unique not because they allow individuals to meet strangers but because SNSs enable users to articulate and make visible their social networks. Such visible social networks would
result in connections between individuals that would not have otherwise been possible and such meetings frequently between ‘latent ties’ who share some offline connections are common. They further commented that on many of the large SNSs, the individuals (users) are not necessarily ‘networking’ or are they looking forward to meeting new people. Instead, users are primarily communicating with people who are already a part of their extended social networks. The articulated social network is one of the critical features of the above-discussed sites. Hence, such sites are labelled as ‘Social Network Sites’.

The traditional ways of communication have tremendously changed with the advent of SNSs. They have become a platform where people with the same likes and dislikes meet, create a personal profile, find romance, seek a new job, locate assistance, get and give product and service referrals, receive support from like-minded individuals, writing comments and making or receiving advice on career or personal issues have become easy. But the use of SNSs has not always been positive among users, particularly, the youth. The following discussion explains the problems faced by the youth and students in using SNSs.

1.8.1 Fading away of face-to-face communication

Face-to-face communication is human and personal. While dabbling in the virtual world the participant is likely to not understand,
recognise and identify the feelings of others. It might be easy for the users to remain in front of a gadget to de-friend, un-follow and dislike anyone. In real life, conflicts are part of growth. The excessive use of gadgets would cripple conflict management strategies. As the time of such use increases, users tend to form a virtual persona, leaving in its wake adverse effects. Fewer face-to-face connections are likely to create problems for users. They are posed with a higher risk of losing real friendships and maintaining good relationships. Young users are also prone to depression when they lose real friendships.

1.8.2 Diminishing privacy

Privacy is a serious concern in SNSs. Many SNSs are open in such a way that the profiles and photographs of individuals are stolen for illegal activities. For example, Facebook recently came up with a much stringent privacy policy, still it is said that it cannot identify pornographic materials. Only when someone else cries foul, then action follows suit. Most of the users are not really aware of the privacy settings in SNS. So, their pages offer full and complete access to others. According to a 2010 North-Eastern University and Max Planck Institute for Software Systems study, researchers created an algorithm to discover an individual’s personal attributes by examining the one thing that most people leave public even when all other privacy settings are in place: their friend list (Frazier, 2011). Using
this algorithm, researchers were able to infer many personal traits including educational qualification, university attended, hometown and other private data. Such algorithms steal the privacy of individuals and are rampant now. Mark Zuckerberg, the founder of Facebook, proudly announced that the privacy policy of Facebook is quite strong, but in a week’s time his own page was hacked (Curtis, 2013). Corporates steal the private information of individuals and serve up advertisements fitting the interests of users.

1.8.3 Negative health issues

A 2010 case study of Western Reserve School of Medicine showed hyper-networking (more than three hours on SNSs per day) and hyper-texting (more than 120 text messages per day) correlated with unhealthy behaviour in teens, including drinking, smoking and excess sexual activity. Hyper-networking was also associated with depression, substance abuse, poor sleep patterns, suicidal tendencies and poor academic performance. Asthma, allergies, lack of concentration, headache, dizziness, stress and tiredness are some of the negative health issues faced by hyperactive users of SNS that has been proven by previous studies (Frank, Santurri & Knight, 2010).

1.8.4 Psychological issues

Self-identity, self-esteem and self-actualisation are severed when there is hyper-networking. As a result, poor self-esteem of individuals
causes serious psychological problems. Depression sets in and stress creeps in. In 2012, Medical News Today reported a study suggesting that Facebook uses and feeds anxiety increasing a person’s feeling of inadequacy (Whiteman, 2014). Many users become addicts to SNSs looking for ‘likes’ once they post a comment or a message. It is also believed that SNSs creates narcissistic tendencies among the youth. They find it difficult to face situations, which are the outcome of too many hours spent on SNSs that result in psychological problems.

1.8.5 Problem in academics

Veen (2007) proposed the term ‘Homo Zappiens’ referring to the new generation of learners. According to him, unlike their predecessors, Homo Zappiens learn in a considerably different way. Children belonging to this generation develop – on their own and without instruction – the meta-cognitive skills necessary for enquiry-based learning, discovery-based learning, networked learning, experiential learning, collaborative learning, active learning, self-organisation and self-regulation, problem solving and making their own implicit (i.e., tacit) and explicit knowledge specific to others. Homo Zappiens believe in extensive use of growing technology. They extensively participate in SNSs. Excessive Internet use causes students to stay up late, suffer from less sleep and miss classes resulting in poor academic performance (Kirschner & Karpinski, 2010). Procrastination is yet another problem students are likely to face due to their
excessive use of the Internet. However, in general, indulging in SNSs causes problems in the academic performance of students.

1.9 Victims of Cybercrime

Cybercrime victimisation occurs when a victim stays connected on the Internet and SNSs in cyberspace. For the purpose of the research, the researcher had chosen to use the following understanding of a cybercrime victim. A cybercrime victim is one who undergoes harm or pain due to one or more unacceptable or undesirable or deviant or unlawful act or activities committed, using a computer or any other device that is connected to the Internet. It might be a one-time experience or repeated recurring activity/event.

The presupposition to any cybercrime victimisation is the use of the Internet. Among the population of the Internet users, the youth constitutes a majority. Internet usage among adolescents is increasing at a quicker pace than any other age group (Jones & Fox, 2009). Now that the Internet has its mainstay among the people, particularly among the youth, users experience both positive and negative aspects of the Internet. Positive aspects include maintaining good communication ties, entertainment and staying update on recent happenings and current information and the negative aspects include harassment and victimisation.
A few specific characteristics are associated with certain young people being at a higher risk of facing the Internet or cybercrime victimisation. Burrow-Sanchez, Call, Zheng and Drew (2011) mention a few of those characteristics in their article. According to them, those youth who turn to the Internet for solace and support that they were not able to obtain in the real world and those who desire to form intimate relationship are at high risk. Specially, the risk is higher for those who have difficulties in relationships with their peers and parents in the physical world. Those who are affected by depression and related mental disorders, people with a sense of chronic loneliness, all youth, particularly the girls who become sexually active at an early age, those who are intimately involved with older adults, are more likely to become easy victims of cybercrime. Besides these people, homosexual youth who use the Internet to solicit information on their sexual orientations might become the target of cybercrime victimisation. Those young users who participate in unsafe surfing of the Internet with certain risky behaviour such as searching for pornography, talking to unknown people online, on sex and sexual matters are most likely to become easy victims. In a fast growing world, anyone could become a victim anytime in the physical space. The same is true in cyberspace, in fact, much more seriously than in the physical space. Wolak, Finkelhor and Mitchell (2008) also confirm that students who engage in a frequent pattern of risky online behaviour are more at risk of being victimised.
The victims of cybercrime face serious harm due to various reasons. Dempsey, Sulkowski, Nichols and Storch (2009) describe why they are seriously harmful. First, there is no escape for the victim as the potential for the person to be victimised extends to the home environment via personal computers and mobile phones. Second, the offender(s) could be more volatile due to the perceived anonymity of the electronic medium. Third, the offender(s) have the opportunity to victimise a great number of users and that too in front of a large audience. And fourth, there is a limited possibility of supervision while accessing the Internet, wherein, even the parental monitoring would fail because cybercrime victimisation happens in and through private environments such as text messaging, e-mail and chat room conversations.

1.10 Impact of Cybercrime Victimisation

Business Dictionary defines impact (Online business dictionary, n.d.) as the measure of the tangible or intangible effects (consequences) of one thing or an entity’s action or influence upon another. The impact of crime and specifically the impact of cybercrime on the victims depend on various factors, such as, social, economic and demographic characteristics of the individuals. Further, the intensity of a crime depends on the number of factors as well. It does not affect all victims in the same way, since some victims have in them an ability
to cope with the impact, while others may not have the same (Wasserman & Ellis, 2007).

A victim of any crime undergoes serious physical, psychological, emotional, financial and social pain. Such pain would create short-term and long-term trauma among the victims. Short-term trauma occurs during or immediately after the crime and lasts for about three months (Kilpatrick, Saunders & Amick-McMullen, 1989). This time frame for short-term versus long-term trauma is based on several reports showing that most crime victims achieve considerable recovery sometime between one and three months after the crime (Wasserman & Ellis, 2007, pp. 1–6). During this time, the victim predominantly experiences physiological effects such as anxiety, rapid heart rate, hyperventilation, muscle tension, headache, fatigue and stomach disorder. Psychologically, the victim undergoes fear, resentment, humiliation and anger against the offender and the criminal justice system. Echeburúa, Corral and Amor (2003) opine that the impact of a crime on a victim includes negative feelings, such as, humiliation, shame, guilt or anger, anxiety, constant worry due to trauma, with a tendency to encourage flashbacks, depression, progressive loss of personal confidence as a consequence of the feelings of helplessness and despair, decrease in self-esteem, loss of interest and concentration with regard to activities previously enjoyed, changes in the system of values, especially confidence in others and the belief in a just world, hostility, aggressiveness, drug
and alcohol use, modification of relationships (emotional dependence and isolation), increase in vulnerability, with fear of living in a dangerous world and loss of control over one’s own life, drastic changes in lifestyle, with fear of going to the usual places, urgent need to change their place of residence, alterations in pattern and amount of sleep and sexual dysfunction. Wasserman and Ellis, (2007) identified some more impacts such as increased risk of alcohol or other drug use, isolation, suicidal tendencies, persistent avoidance of things associated with the traumatic event and post-traumatic stress disorder to emotional disorder that a victim undergoes (pp. 1–6).

Financially, it burdens the victims in many ways such as paying for the medical bills, taking care of the victims, expenses on therapies, loss of wages and relocation expenses and so on. And, social impact would include effects on work and life, on relationships in the family and society and social exclusion (Langton & Truman, 2014).

Studies conducted on the impact of cybercrime such as of those by Finkelhor, Mitchell and Wolak (2000), Beran and Li (2005), Hay, Meldrum and Mann (2010), Schenk & Fremouw (2012), Staude-Muller, Hansen and Voss (2012) that has elaborately been discussed in the chapter on review of literature, prove that the victims of cybercrime face a similar impact of the crime committed on them.
1.11 Need and Significance of the Study

The existing official statistics published by the Government of India reveals that the extent of victimisation due to cybercrime is on the rise in the last few years. Further studies conducted in several parts of the world have demonstrated that there are different forms of cybercrime victimisation. But in India, limited research has been carried out on the problem of cybercrime and its victimisation. Specifically in India, not many studies have been conducted on the newer forms of cybercrime, forms of victimisation and their impact on the victims. Hence, the present research was undertaken to find out the extent of cybercrime victimisation, the forms of cybercrime victimisation and their impact on the victims. An attempt was also made to understand the reporting behaviour of the victims and the response of those to whom it was reported. The outcome of the present research has proved to be useful not only to understand the newer forms of cybercrime victimisation but also to understand the problems encountered by the victims as a result of their victimisation. Further, the outcome of research would help to develop a typology of cybercrime victimisation, particularly victimisation using the Internet, which could be taken into account by the lawmakers while defining different forms of cybercrime which will be useful to create new provisions in the existing law or to enact an exclusive law to deal with various forms of cybercrime. 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 which would help them to effectively deal with cybercrime victimisation.

1.12 Statement of the Problem

The present research is aimed at discovering the extent of cybercrime victimisation among college students in Chennai. The research has attempted to find out the various forms of cybercrime victimisation faced by college students in Chennai. The study also examined the impact of the problems of cybercrime and the reporting behaviour of victims.

1.13 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.

1.14 Scope

The term cybercrime is generic and includes several forms of offences committed in cyberspace. In the present research, the term cybercrime
is used to denote any unacceptable or undesirable, deviant or unlawful activity committed using a computer or any other device that is connected to the Internet. The study was carried out among students pursuing both under-graduate and post-graduate programmes in colleges in Chennai. This research was conducted among students who are Internet users. The scope of the research is restricted to victimisation faced by students who have access to e-mail and/or social network sites such as Facebook, Twitter, and Whatsapp etc. The scope of the study does not include cybercrime victimisation which involves financial loss.

1.15 Operational Definitions

• **Social Network Sites (SNSs)**

Web-based services that allow constructing a public or semi-public profile within a bounded system, articulate a list of other users with whom a profile holder shares a connection and views and traverse their list of connections and those made by others within the system.

• **Cybercrime**

Any unacceptable or undesirable or deviant or unlawful activity committed, using a computer or any other device that is connected to the Internet.
• **Cybercrime Victimisation**

A state of being victimised by any unacceptable or undesirable or deviant or unlawful activity committed, using a computer or any other device that are connected to the Internet.

• **Cyber Harassment**

Any unacceptable or undesirable or deviant or unlawful activity like bullying and harassment committed, using a computer or any other device that are connected to the Internet.

• **Cyber Stalking**

Any unacceptable or undesirable or deviant or unlawful activity like stalking and related activities, committed using a computer or any other devices that are connected to the Internet.

• **Cyber Hacking**

Any unacceptable or undesirable or deviant or unlawful activity such as stealing passwords or personal information, hacking the mailbox of individuals, committed using a computer or any other device that is connected to the Internet.

• **Cyber Sexual Victimisation**

A state of being victimised by any unacceptable or undesirable or deviant or unlawful activity such as sharing or posting pornographic pictures/videos, sharing child-pornography, being
forced to browse obscene websites, committed using a computer or any other device that is connected to the Internet.

- **Impact**

Impact is defined as the measure of the tangible or intangible effects (consequences) of one thing or entity’s action or influence upon another. Here, impact is defined as the changes that are brought into life of respondents due to cybercrime victimisation.

- **Reporting Behaviour**

Behaviour of a victim in reporting the problem or situation or crime faced by them to someone.

The aforesaid narrative provides an overview of the issue of both cybercrime and cybercrime victimisation. Attempts have been made to comprehensively and explicitly define the broad concepts such as cybercrime, cybercrime victimisation, SNSs, impact and so on. The chapter has also thrown light on both national and international legal instruments to handle or deal with cybercrime. The issues pertaining to the victims of cybercrime and the consequences on them have also been highlighted in this chapter. Sufficient justification has been arrived at to undertake a research on cybercrime and its extent and forms of cybercrime victimisation among the youth. The relevant literature has been reviewed and presented in Chapter II.