1 Introduction to Cybercrime

Learning Objectives

After reading this chapter, you will able to:

- Learn what cybercrime is and appreciate the importance of cybercrime as the topic.
- Understand the different types of cybercrime.
- Understand the difference between cybercrime and cyberfraud.
- Learn about different types of cybercriminals and the motives behind them.
- Get an overview of cybercrime scenario in India as well as the overall global perspective.
- Understand the legal perspective on cybercrime including the Indian ITA 2000 and its latest amendment known as the ITA 2008.

1.1 Introduction

Almost everyone is aware of the phenomenal growth of the Internet (the statistics on Indian growth for Internet and mobile usage are indicated through links provided in Ref. #26, Additional Useful Web References, Further Reading). Given the unrestricted number of free websites, the Internet has undeniably opened a new way of exploitation known as cybercrime. These activities involve the use of computers, the Internet, cyberspace (see Box 1.1) and the worldwide web (WWW). Interestingly, cybercrime is *not* a new phenomena; the first recorded cybercrime took place in the year 1820. It is one of the most talked about topics in the recent years. Figure 1.1, based on a 2008 survey in Australia, shows the cybercrime trend. Also refer to Appendix L.

While the worldwide scenario on cybercrime looks bleak, the situation in India is not any better. Indian corporate and government sites have been attacked or defaced more than 780 times between February 2000 and December 2002. There are also stories/news of other attacks; for example, according to a story posted on 3 December 2009, a total of 3,286 Indian websites were hacked in 5 months – between January and June 2009 (see Ref. #2, Articles and Research Papers, Further Reading).

Similar data for later years is presented in Tables 1.1–1.4; the data in those tables show statistics related to various cybercrimes and cases registered under cybercrimes by motives and suspects in States and Union Territories (UTs).

1.2 Cybercrime: Definition and Origins of the Word

With the backdrop of information in the previous section and the statistics presented in Tables 1.1 and 1.2, let us understand the origins of the term *cybercrime*. Reaching consensus on a definition of computer

Box 1.1 Cyberspace, Cybersquatting, Cyberpunk, Cyberwarfare and Cyberterrorism

Cyberspace

This is a term coined by William Gibson, a science fiction writer, in his Sci-fi novel Neuromancer (published in 1984) – he suggested it as a "consensual hallucination." According to his vision about near-future computer network (as at the time when he coined the term in 1984), "cyberspace" is where users mentally travel through matrices of data. Conceptually, "cyberspace" is the "nebulous place" where humans interact over computer networks. The term "cyberspace" is now used to describe the Internet and other computer networks. In terms of computer science, "cyberspace" is a worldwide network of computer networks that uses the Transmission Control Protocol/Internet Protocol (TCP/IP) for communication to facilitate transmission and exchange of data. A common factor in almost all definitions of cyberspace is the sense of place that they convey – cyberspace is most definitely a place where you chat, explore, research and play.

Cybersquatting

The term is derived from "squatting" which is the act of occupying an abandoned/unoccupied space/building that the squatter does not own, rent or otherwise have permission to use. Cybersquatting, however, is a bit different in that the domain names that are being squatted are (sometimes but not always) being paid for by the cybersquatters through the registration process. Cybersquatters usually ask for prices far greater than those at which they purchased it. Some cybersquatters put up derogatory or defamatory remarks about the person or company the domain is meant to represent in an effort to encourage the subject to buy the domain from them. This term is explained here because, in a way, it relates to cybercrime given the intent of cybersquatting. Cybersquatting is the act of registering a popular Internet address, usually a company name, with the intent of selling it to its rightful owner. From an affected individual's point of view, cybersquatting means registering, selling or using a domain name with the intent of profiting from the goodwill of someone else's trademark. In this nature, it can be considered to be a type of cybercrime. Cybersquatting is the practice of buying "domain names" that have existing businesses names. In other words, cybersquatting involves the pre-emptive registration of trademarks by third parties as domain names. It is done with the intent to sell those "domain names" to earn profit. Comparing cybersquatting to online extortion, Senator Spencer Abraham, a Michigan Republican, introduced to Congress the Anti-Cybersquatting Consumer Protection Act. This bill, if enacted, would make cybersquatting illegal. Violators would be charged a fine of up to $300,000. The World Intellectual Property Organization (WIPO) has also outlined anti-cybersquatting tactics, which have been endorsed by Internet Corporation for Assigned Names and Numbers (ICANN). Ironically enough, someone recently registered www.wipo.com in order to sell it back to WIPO for several thousand dollars. Even though legislation has not been enacted, almost all cybersquatting court-case decisions are against cybersquatters. We can see that the topic of "domain name disputes" is closely connected with cybersquatting, because domain name disputes arise largely from the practice of cybersquatting. Such disputes happen because cybersquatters exploit the first-come, first-served nature of the domain name registration system to register names of trademarks, famous people or businesses with which they have no connection. Since registration of domain names is relatively simple, cybersquatters can register numerous examples of such names as domain names. As the holders of these registrations, cybersquatters often then put the domain names up for auction, or offer them for sale directly to the company or person involved, at prices far beyond the cost of registration. Alternatively, they can keep the registration and use the name of the person or business associated with that domain name to attract business for their own sites.

In India, "cybersquatting" is considered to be an "Intellectual Property Right" (IPR) evil (see Ref. #29, Additional Useful Web References, Further Reading). In India, "cybersquatting" is seen to interfere with the "Uniform Dispute Resolution Policy" (a contractual obligation to which all domain name registrants are presently subjected to). It also affects the rights of Indians who have to face charges of "Squatting" in respect of international generic domain names such as dot com, dot org, etc. The terms "trademark" and "intellectual property" are explained in Chapter 10.

Box 1.1 Cyberspace, Cybersquatting, . . . (*Continued*)

Cyberpunk and Cyberwarfare

According to science fiction literature, the words "cyber" and "punk" emphasize the two basic aspects of cyberpunk: "technology" and "individualism." The term "cyberpunk" could mean something like "anarchy via machines" or "machine/computer rebel movement." This word first appeared as the title of a short story "*Cyberpunk*" by Bruce Bethke, published in science fiction stories magazine, AMAZING, Vol. 57, No. 4, November 1983. It is quite interesting to note that the word was coined in the early spring of 1980, and applied to the "bizarre, hard-edged, high-tech" science fiction emerging in the 1980s. The story is about a bunch of teenage hackers/crackers. The idea behind calling it "cyberpunk" was to invent a new term that will express the juxtaposition of punk attitudes and high technology. For the terms "hackers," "crackers" and others, readers may like to refer to specific pages of the source mentioned at the end of this box. Also refer to Chapter 10.

Cyberwarfare, for many people, means information warriors unleashing vicious attacks against an unsuspecting opponent's computer networks, wreaking havoc and paralyzing nations. This perception seems to be correct as the terms cyberwarfare and cyberterrorism have got historical connection in the context of attacks against infrastructure. The term "information infrastructure" refers to information resources, including communication systems that support an industry, institution or population. Cyberattacks are often presented as threat to military forces and the Internet has major implications for espionage and warfare. Information warfare (see Ref. #9, Books, Further Reading) covers a range of activities of which cyberattacks may be the least important.

Cyberterrorism

This term was coined in 1997 by Barry Collin, a senior research fellow at the Institute for Security and Intelligence in California. Cyberterrorism seems to be a controversial term. Some authors choose a very narrow definition, relating to deployments, by known terrorist organizations, of disruption attacks against information systems for the primary purpose of creating alarm and panic. However, this narrow definition makes it difficult to identify any instances of cyberterrorism. There is a broad definition stated by Kevin G. Coleman of the Technolytics Institute:

> *The premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives or to intimidate any person in furtherance of such objectives.*

There is a lot of misinterpretation in the definition of cyberterrorism, the term consisting of familiar word "cyber" and less familiar word "terrorism." Although "*cyber*" is the term we can understand (see Section 1.2), the term *terrorism* is difficult to define. The ambiguity in the definition brings in vagueness in action, as D. Denning pointed in her work saying that "'an E-Mail bomb' may be considered as 'hacktivism' by some and 'cyberterrorism' by others" (for terms such as "activism," "hacktivism" and "cyberterrorism", see Ref #13, Additional Web References, Further Reading). There is a degree of understanding of the meanings of cyberterrorism, either from the popular media, other secondary sources or personal experience; however, the specialists use different definitions. "Cyberterrorism", as well as other contemporary "terrorisms" appear as a mixture of words terrorism and a meaning of an area of application. Barry Collin defined cyberterrorism as the convergence of cybernetics and terrorism. In the same year, Mark Pollitt, special agent for the FBI, offers a working definition:

> *Cyberterrorism is the premeditated, politically motivated attack against information, computer systems, computer programs and data which result in violence against noncombatant targets by sub national groups or clandestine agents.*

We can also define cyberterrorism as: *Use of information technology and means by terrorist groups and agents.* Refer to Chapter 10.

Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices* (Box 11.2, p. 170 and Box 38.12, p. 926), Wiley India.

Box 1.1 Cyberspace, Cybersquatting, . . . (*Continued*)

Cyberpunk and Cyberwarfare

According to science fiction literature, the words "cyber" and "punk" emphasize the two basic aspects of cyberpunk: "technology" and "individualism." The term "cyberpunk" could mean something like "anarchy via machines" or "machine/computer rebel movement." This word first appeared as the title of a short story "*Cyberpunk*" by Bruce Bethke, published in science fiction stories magazine, *AMAZING*, Vol. 57, No. 4, November 1983. It is quite interesting to note that the word was coined in the early spring of 1980, and applied to the "bizarre, hard-edged, high-tech" science fiction emerging in the 1980s. The story is about a bunch of teenage hackers/crackers. The idea behind calling it "cyberpunk" was to invent a new term that will express the juxtaposition of punk attitudes and high technology. For the terms "hackers," "crackers" and others, readers may like to refer to specific pages of the source mentioned at the end of this box. Also refer to Chapter 10.

Cyberwarfare, for many people, means information warriors unleashing vicious attacks against an unsuspecting opponent's computer networks, wreaking havoc and paralyzing nations. This perception seems to be correct as the terms cyberwarfare and cyberterrorism have got historical connection in the context of attacks against infrastructure. The term "information infrastructure" refers to information resources, including communication systems that support an industry, institution or population. Cyberattacks are often presented as threat to military forces and the Internet has major implications for espionage and warfare. Information warfare (see Ref. #9, Books, Further Reading) covers a range of activities of which cyberattacks may be the least important.

Cyberterrorism

This term was coined in 1997 by Barry Collin, a senior research fellow at the Institute for Security and Intelligence in California. Cyberterrorism seems to be a controversial term. Some authors choose a very narrow definition, relating to deployments, by known terrorist organizations, of disruption attacks against information systems for the primary purpose of creating alarm and panic. However, this narrow definition makes it difficult to identify any instances of cyberterrorism. There is a broad definition stated by Kevin G. Coleman of the Technolytics Institute:

> *The premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives or to intimidate any person in furtherance of such objectives.*

There is a lot of misinterpretation in the definition of cyberterrorism, the term consisting of familiar word "cyber" and less familiar word "terrorism." Although "*cyber*" is the term we can understand (see Section 1.2), the term *terrorism* is difficult to define. The ambiguity in the definition brings in vagueness in action, as D. Denning pointed in her work saying that "'an E-Mail bomb' may be considered as 'hacktivism' by some and 'cyberterrorism' by others" (for terms such as "activism," "hacktivism" and "cyberterrorism", see Ref #13, Additional Web References, Further Reading). There is a degree of understanding of the meanings of cyberterrorism, either from the popular media, other secondary sources or personal experience; however, the specialists use different definitions. "Cyberterrorism", as well as other contemporary "terrorisms" appear as a mixture of words terrorism and a meaning of an area of application. Barry Collin defined cyberterrorism as the convergence of cybernetics and terrorism. In the same year, Mark Pollitt, special agent for the FBI, offers a working definition:

> *Cyberterrorism is the premeditated, politically motivated attack against information, computer systems, computer programs and data which result in violence against noncombatant targets by sub national groups or clandestine agents.*

We can also define cyberterrorism as: *Use of information technology and means by terrorist groups and agents.* Refer to Chapter 10.

Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices* (Box 11.2, p. 170 and Box 38.12, p. 926), Wiley India.

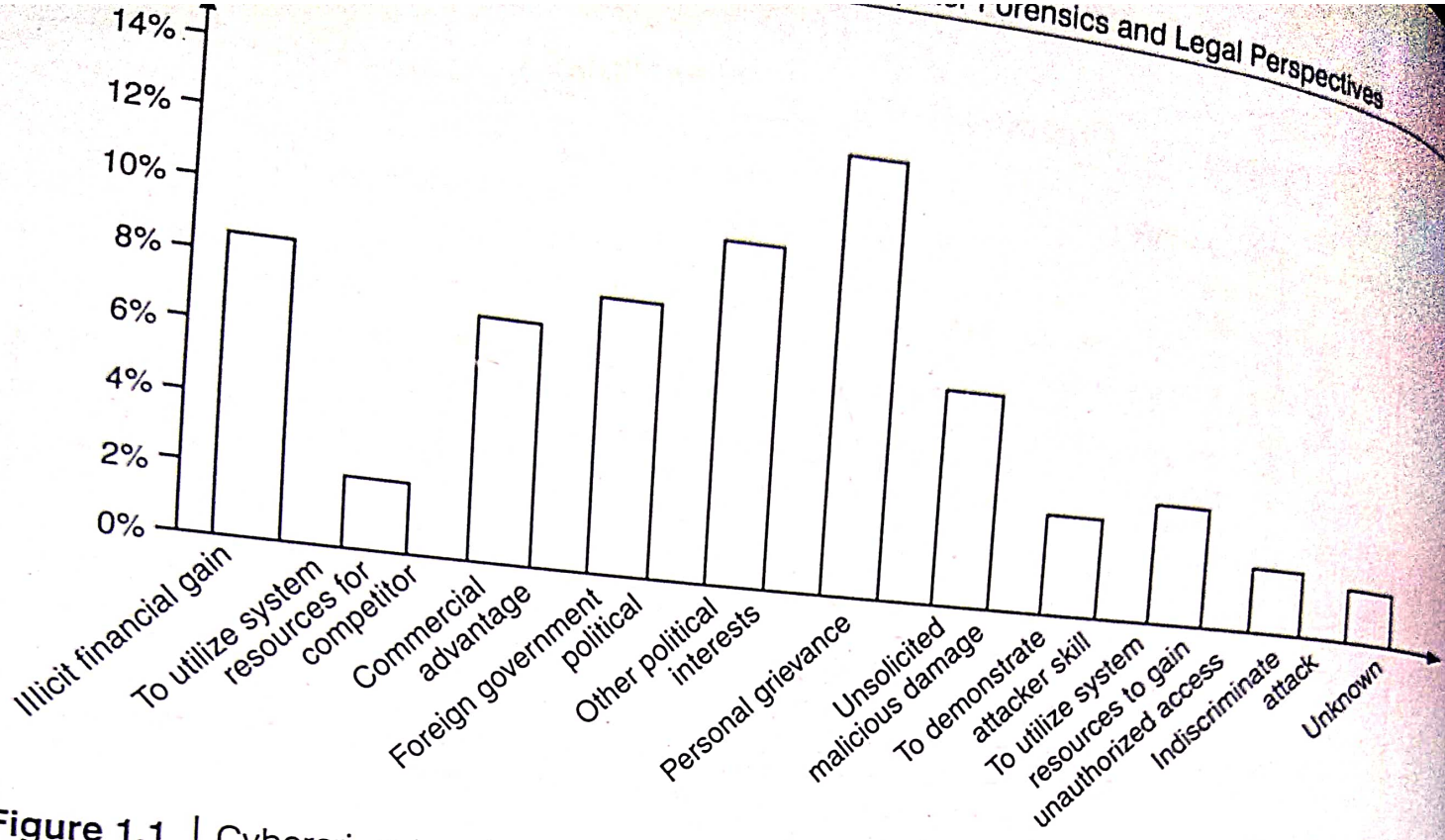

Figure 1.1 Cybercrime trend.
Source: 2008 Pacific Islands Computer Crime and Security Survey. Adapted from *Cybercrime: Threats, Challenges* presentation by Wipul Jayawickrama at the Computer Security Week 2008 in Brisbane, Australia (reproduced with permission).

crime is difficult. One definition that is advocated is, "*a crime conducted in which a computer was directly and significantly instrumental.*" This definition is not universally accepted. It, however, initiates further discussion to narrow the scope of the definition for "cybercrime": for example, we can propose the following alternative definitions of computer crime:

1. Any illegal act where a special knowledge of computer technology is essential for its perpetration, investigation or prosecution.
2. Any traditional crime that has acquired a new dimension or order of magnitude through the aid of a computer, and abuses that have come into being because of computers.
3. Any financial dishonesty that takes place in a computer environment.
4. Any threats to the computer itself, such as theft of hardware or software, sabotage and demands for ransom.

Here is yet another definition: "*cybercrime (computer crime) is any illegal behavior, directed by means of electronic operations, that targets the security of computer systems and the data processed by them.*" Note that in a wider sense, "computer-related crime" can be any illegal behavior committed by means of, or in relation to, a computer system or network; however, this is not cybercrime.

Statute and treaty law both refer to "cybercrime." The term "cybercrime" relates to a number of other terms that may sometimes be used interchangeably to describe crimes committed using computers. *Computer-related crime, Computer crime, Internet crime, E-crime, High-tech crime,* etc. are the other synonymous terms. Cybercrime specifically can be defined in a number of ways; a few definitions are:

1. A crime committed using a computer and the Internet to steal a person's identity (identity theft) or sell contraband or stalk victims or disrupt operations with malevolent programs. Refer to Chapter 5.

Table 1.1 | Cybercrimes/cases registered and persons arrested under IT Act during 2004–2007

Sr. No.	Crime Heads	Cases Registered				% Variation in 2007 over 2006	Persons Arrested				% Variation in 2007 over 2006
		2004	2005	2006	2007		2004	2005	2006	2007	
1	Tampering computer source documents	2	10	10	11	10.0	0	10	8	2	–75
2	Hacking with computer system										
	(i) Loss/damage to computer resource/utility	14	33	25	20	–20.0	31	27	34	25	–26.5
	(ii) Hacking	12	41	34	46	35.3	1	14	29	23	–20.7
3	Obscene publication/transmission in electronic form	34	88	69	99	43.5	21	125	81	86	6.2
4	Failure										
	(i) Of compliance/orders of Certifying Authority	0	1	0	2	—	0	0	0	1	—
	(ii) To assist in decrypting the information intercepted by government agency	0	0	0	2	—	0	0	0	0	—
5	Unauthorized access/attempt to access to protected computer system	0	0	0	4	—	0	0	0	0	—
6	Obtaining licence or digital signature certificate by misrepresentation/suppression of fact	0	0	0	11	—	0	0	0	11	—
7	Publishing false digital signature certificate	0	0	0	0	—	0	0	0	0	—
8	Fraud digital signature certificate	0	1	1	3	200.0	0	3	0	3	—
9	Breach of confidentiality/privacy	6	3	3	9	200.0	7	13	2	3	50.0
10	Other	0	0	0	0	—	0	0	0	0	—
	Total	**68**	**177**	**142**	**207**	**45.8**	**60**	**192**	**154**	**154**	**0.0**

Source: http://www.nasscom.org/download/Cybercrimes in India 2003.pdf (28 February 2009).

Table 1.2 | Cybercrimes/cases registered and persons arrested during 2004–2007

Sr. No.	Crime Heads	Cases Registered				% Variation in 2007 over 2006	Persons Arrested				% Variation in 2007 over 2006
		2004	2005	2006	2007		2004	2005	2006	2007	
1	Offences by/ against public servant	0	0	0	0	—	0	0	0	0	—
2	False electronic evidence	0	0	0	0	—	0	0	0	0	—
3	Destruction of electronic evidence	77	48	160	217	35.6	81	71	194	264	36.1
4	Forgery	173	186	90	73	-18.9	181	215	121	85	-29.8
5	Criminal breach of trust/ fraud										
6	Counterfeiting						8	0	7	23	228.6
	(i) Property/ mark	12	0	13	8	-38.5					
	(ii) Tampering	7	9	0	5	—	16	0	0	8	—
	(iii) Currency/ stamps	10	59	48	36	-25.0	43	82	89	49	-44.9
7	**Total**	**279**	**302**	**311**	**339**	**9.0**	**329**	**368**	**411**	**429**	**4.4**

Source: http://www.nasscom.org/download/Cybercrimes in India 2003.pdf (28 February 2009).

2. Crimes completed either on or with a computer.
3. Any illegal activity done through the Internet or on the computer.
4. All criminal activities done using the medium of computers, the Internet, cyberspace and the WWW.

According to one information security glossary,[1] cybercrime is any criminal activity which uses network access to commit a criminal act. Opportunities for the exploitation due to weaknesses in information security are multiplying because of the exponential growth of Internet connection (see Ref. #26, Additional Useful Web References, Further Reading). Cybercrime may be internal or external, with the former easier to perpetrate. The term "cybercrime" has evolved over the past few years since the adoption of Internet connection on a global scale with hundreds of millions of users. *Cybercrime* refers to the act of performing a criminal act using cyberspace as the communications vehicle (the term "cyberspace" is explained in Box 1.1). Some people argue that a cybercrime is not a crime as it is a crime against software and not against a person or property. However, while the legal systems around the world scramble to introduce laws to combat cybercriminals (refer to Section 1.5), two types of attack are prevalent:

1. **Techno-crime:** A premeditated act against a system or systems, with the intent to copy, steal, prevent access, corrupt or otherwise deface or damage parts of or the complete computer system. The 24 × 7 connection to the Internet makes this type of cybercrime a real possibility to engineer from anywhere in the world, leaving few, if any, "finger prints."

Table 1.3 | 2005 Cases under cybercrime – part A

Cases registered under cybercrimes by motives and suspects during 2005 [(States and Union Territories (UTs)]

Sr. No.	State/UT	Motives								
		Revenge/ Settling Scores	Greed/ Money	Extortion	Cause Disrepute	Prank/ Satisfaction of Gaining Control	Fraud/Illegal Gain	EveTeasing/ Harassment	Others	Total
	States									
1	Andhra Pradesh	0	0	0	0	3	18	3	58	82
2	Arunachal Pradesh	0	0	0	0	0	0	0	0	0
3	Assam	0	0	0	0	0	0	0	1	1
4	Bihar	0	0	0	0	0	0	0	0	0
5	Chhattisgarh	0	4	0	0	0	1	0	41	46
6	Goa	0	0	0	0	0	0	1	2	3
7	Gujarat	0	2	0	1	0	1	0	151	155
8	Haryana	0	0	0	0	0	1	2	6	9
9	Himachal Pradesh	0	0	0	0	0	0	0	0	0
10	Jammu & Kashmir	0	0	0	0	0	0	0	0	0
11	Jharkhand	0	0	0	0	0	0	0	0	0
12	Karnataka	4	4	0	3	0	16	10	1	38
13	Kerala	0	0	0	0	0	0	0	0	0
14	Madhya Pradesh	0	0	0	0	0	0	0	0	0
15	Maharashtra	2	4	0	2	1	7	11	0	27
16	Manipur	0	0	0	0	0	0	0	0	0
17	Meghalaya	0	0	0	0	0	0	0	0	0
18	Mizoram	0	0	0	0	0	0	0	0	0
19	Nagaland	0	0	0	0	0	0	0	0	0
20	Orissa	0	0	0	0	0	2	0	4	6
21	Punjab	0	0	0	1	0	7	0	42	50
22	Rajasthan	0	0	0	0	0	0	0	18	18
23	Sikkim	0	0	0	0	0	0	0	0	0

(Continued)

Table 1.3 | *(Continued)*

Sr. No.	State/UT	Motives								
		Revenge/ Settling Scores	*Greed/ Money*	*Extortion*	*Cause Disrepute*	*Prank/ Satisfaction of Gaining Control*	*Fraud/Illegal Gain*	*Eve Teasing/ Harassment*	*Others*	*Total*
24	Tamil Nadu	0	0	2	10	0	—	9	0	22
25	Tripura	0	0	0	0	0	0	0	0	0
26	Uttar Pradesh	0	1	0	0	0	1	0	2	4
27	Uttaranchal	0	0	0	0	0	0	0	0	0
28	West Bengal	0	0	0	0	0	0	0	0	0
	Total (States)	**6**	**15**	**2**	**17**	**4**	**55**	**36**	**326**	**461**
	Union Territories									
29	A & N Islands	0	0	0	0	0	0	0	0	0
30	Chandigarh	0	1	0	0	0	0	0	1	2
31	D & N Haveli	0	0	0	0	0	0	0	0	0
32	Daman & Diu	0	0	0	0	0	0	0	0	0
33	Delhi	0	0	0	0	0	2	1	15	18
34	Lakshadweep	0	0	0	0	0	0	0	0	0
35	Pondicherry	0	0	0	0	0	0	0	0	0
	Total (UTs)	**0**	**1**	**0**	**0**	**0**	**2**	**1**	**16**	**20**
	Total (All India)	**6**	**16**	**2**	**17**	**4**	**57**	**37**	**342**	**481**
	Cities									
36	Agra	0	0	0	0	0	0	1	0	1
37	Ahmedabad	0	2	0	1	0	1	0	5	9
38	Allahabad	0	0	0	0	0	0	0	0	0
39	Amritsar	0	0	0	0	0	0	0	0	0
40	Asansol	0	0	0	0	0	0	0	0	0
41	Bangalore	4	4	0	3	0	16	10	1	38
42	Bhopal	0	0	0	0	0	0	0	0	0
43	Chennai	0	0	2	10	0	0	8	0	20
44	Coimbatore	0	0	0	0	0	0	0	0	0

Table 1.3 | *(Continued)*

Sr. No.	State/UT	Motives								
		Revenge/ Settling Scores	*Greed/ Money*	*Extortion*	*Cause Disrepute*	*Prank/ Satisfaction of Gaining Control*	*Fraud/Illegal Gain*	*Eve Teasing/ Harassment*	*Others*	*Total*
45	Delhi (City)	0	0	0	0	0	2	1	15	18
46	Dhanbad	0	0	0	0	0	0	0	0	0
47	Faridabad	0	0	0	0	0	0	0	3	3
48	Hyderabad	0	0	0	0	0	0	0	0	0
49	Indore	0	0	0	0	0	0	0	0	0
50	Jabalpur	0	0	0	0	0	0	0	0	0
51	Jaipur	0	0	0	0	0	0	0	0	0
52	Jamshedpur	0	0	0	0	0	0	0	0	0
53	Kanpur	0	0	0	0	0	0	0	0	0
54	Kochi	0	0	0	0	0	0	0	0	0
55	Kolkata	0	0	0	0	0	0	0	0	0
56	Lucknow	0	0	0	0	0	0	0	0	0
57	Ludhiana	0	0	0	0	0	0	0	0	0
58	Madurai	0	0	0	0	0	0	0	0	0
59	Meerut	0	0	0	0	0	0	0	0	0
60	Mumbai	0	5	0	0	0	0	1	2	8
61	Nagpur	0	0	0	0	0	1	2	0	3
62	Nasik	0	0	0	0	0	0	0	0	0
63	Patna	0	0	0	0	0	0	0	0	0
64	Pune	0	0	0	1	0	4	3	1	9
65	Rajkot	0	0	0	0	0	0	0	0	0
66	Surat	0	0	0	0	0	0	0	146	146
67	Vadodara	0	0	0	0	0	0	0	0	0
68	Varanasi	0	0	0	0	0	0	0	0	0
69	Vijayawada	0	0	0	0	0	2	0	0	2
70	Vishakhapatnam	0	0	0	0	0	0	0	0	0
	Total (Cities)	**4**	**11**	**2**	**15**	**0**	**26**	**26**	**173**	**257**

Source: http://ncrb.nic.in/crime2005/cii-2005/Table%2018.8.pdf (1 March 2009).

Table 1.4 | 2005 Cases under cybercrime – part B

Sr. No.	State/UT	Suspects						
		Foreign National /Group	Disgruntled Employee/ Employees	Cracker/ Student/ Professional Learners	Business Competitor	Neighbors/ Friends and Relatives	Others	Total
	States							
1	Andhra Pradesh	0	0	3	11	8	60	82
2	Arunachal Pradesh	0	0	0	0	0	0	0
3	Assam	0	0	0	0	0	1	1
4	Bihar	0	0	0	0	0	0	0
5	Chhattisgarh	0	0	20	0	0	26	46
6	Goa	0	0	0	0	0	3	3
7	Gujarat	0	2	2	1	0	150	155
8	Haryana	0	0	0	2	1	6	6
9	Himachal Pradesh	0	0	0	0	0	0	0
10	Jammu & Kashmir	0	0	0	0	0	0	0
11	Jharkhand	0	0	0	0	0	0	0
12	Karnataka	4	13	1	0	7	13	38
13	Kerala	0	0	0	0	0	0	0
14	Madhya Pradesh	0	0	0	0	0	0	0
15	Maharashtra	0	2	0	0	5	20	27
16	Manipur	0	0	0	0	0	0	0
17	Meghalaya	0	0	0	0	0	0	0
18	Mizoram	0	0	0	0	0	0	0
19	Nagaland	0	0	0	0	0	0	0
20	Orissa	0	0	0	2	0	4	6
21	Punjab	0	8	6	1	0	35	50
22	Rajasthan	0	0	11	0	0	7	18
23	Sikkim	0	0	0	0	0	0	0
24	Tamil Nadu	0	15	1	0	3	3	22
25	Tripura	0	0	0	0	0	0	0
26	Uttar Pradesh	0	0	2	0	0	2	4
27	Uttaranchal	0	0	0	0	0	0	0
28	West Bengal	0	0	0	0	0	0	0
	Total (States)	**4**	**40**	**46**	**17**	**24**	**330**	**458**

(Continued)

Table 1.4 | (*Continued*)

Sr. No.	State/UT	Suspects						
		Foreign National /Group	Disgruntled Employee/ Employees	Cracker/ Student/ Professional Learners	Business Competitor	Neighbors/ Friends and Relatives	Others	Total
	Union Territories							
29	A & N Islands	0	0	0	0	0	0	0
30	Chandigarh	0	0	1	0	0	1	2
31	D & N Haveli	0	0	0	0	0	0	0
32	Daman & Diu	0	0	0	0	0	0	0
33	Delhi	0	2	0	0	0	16	18
34	Lakshadweep	0	0	0	0	0	0	0
35	Pondicherry	0	0	0	0	0	0	0
	Total (UTs)	**0**	**2**	**1**	**0**	**0**	**17**	**20**
	Total (All India)	**4**	**42**	**47**	**17**	**24**	**347**	**478**
	Cities							
36	Agra	0	0	0	0	0	1	1
37	Ahmedabad	0	2	2	1	0	4	9
38	Allahabad	0	0	0	0	0	0	0
39	Amritsar	0	0	0	0	0	0	0
40	Asansol	0	0	0	0	0	0	0
41	Bangalore	4	13	1	0	7	13	38
42	Bhopal	0	0	0	0	0	0	0
43	Chennai	0	14	0	0	3	3	20
44	Coimbatore	0	0	0	0	0	0	0
45	Delhi (City)	0	2	0	0	0	16	18
46	Dhanbad	0	0	0	0	0	0	0
47	Faridabad	0	0	0	0	0	3	3
48	Hyderabad	0	0	0	0	0	0	0
49	Indore	0	0	0	0	0	0	0
50	Jabalpur	0	0	0	0	0	0	0
51	Jaipur	0	0	0	0	0	0	0
52	Jamshedpur	0	0	0	0	0	0	0
53	Kanpur	0	0	0	0	0	0	0
54	Kochi	0	0	0	0	0	0	0
55	Kolkata	0	0	0	0	0	0	0
56	Lucknow	0	0	0	0	0	0	0
57	Ludhiana	0	0	0	0	0	0	0
58	Madurai	0	0	0	0	0	0	0
59	Meerut	0	0	0	0	0	0	0
60	Mumbai	0	0	0	0	0	8	8

(*Continued*)

Table 1.4 | (Continued)

Sr. No.	State/UT	Suspects						
		Foreign National /Group	Disgruntled Employee/ Employees	Cracker/ Student/ Professional Learners	Business Competitor	Neighbors/ Friends and Relatives	Others	Total
61	Nagpur	0	0	0	0	2	1	3
62	Nasik	0	0	0	0	0	0	0
63	Patna	0	0	0	0	0	0	0
64	Pune	0	0	0	0	1	8	9
65	Rajkot	0	0	0	0	0	0	0
66	Surat	0	0	0	0	0	146	146
67	Vadodara	0	0	0	0	0	0	0
68	Varanasi	0	0	0	0	0	0	0
69	Vijayawada	0	0	0	2	0	0	2
70	Vishakhapatnam	0	0	0	0	0	0	0
	Total (Cities)	**4**	**31**	**3**	**3**	**13**	**203**	**257**

Source: http://ncrb.nic.in/crime2005/cii-2005/Table%2018.8.pdf (1 March 2009).

2. **Techno-vandalism:** These acts of "brainless" defacement of websites and/or other activities, such as copying files and publicizing their contents publicly, are usually opportunistic in nature. Tight internal security, allied to strong technical safeguards, should prevent the vast majority of such incidents.

There is a very thin line between the two terms "computer crime" and "computer fraud"; both are punishable (see Tables 1.1–1.4). Cybercrimes (harmful acts committed from or against a computer or network) differ from most terrestrial crimes in four ways: (a) how to commit them is easier to learn, (b) they require few resources relative to the potential damage caused, (c) they can be committed in a jurisdiction without being physically present in it and (d) they are often not clearly illegal.

The term cybercrime has some stigma attached and is notorious due to the word "terrorism" or "terrorist" attached with it, that is, cyberterrorism (see explanation of the term in Box 1.1). Cyberterrorism is defined as "*any person, group or organization who, with* ***terrorist intent****, utilizes accesses or aids in accessing a computer or computer network or electronic system or electronic device by any available means, and thereby knowingly engages in or attempts to engage in a terrorist act commits the offence of cyberterrorism.*" Cybercrime, especially through the Internet, has grown in number as the use of computer has become central to commerce, entertainment and government.

The term *cyber* has some interesting synonyms: fake, replicated, pretend, imitation, virtual, computer-generated. Cyber means combining forms relating to Information Technology, the Internet and Virtual Reality. This term owes its origin to the word "cybernetics" which deals with information and its use; furthermore, cybernetics is the science that overlaps the fields of neurophysiology, information theory, computing machinery and automation.[2] However, beyond this, there does not seem to be any further connection to the term "cybernetics" as per other sources searched.[3–5] According to Wikipedia,[6] cybernetics is the interdisciplinary study of the structure of regulatory systems. It is closely related to control theory and systems theory.

People are curious to know how cybercrimes are planned and how they actually take place (explained in Chapter 2). Worldwide, including India, cyberterrorists usually use computer as a tool, target or both for